KİŞİSEL VERİLERİN KORUNMASI, MUHAFAZASI VE PAYLAŞIMI

Adnan Coşkun DOĞAN
Maliye Uzmanı

Ankara
Nisan 2015

İÇİNDEKİLER

KISALTMALAR

Avrupa Adalet Divanı	AAD
Avrupa Birliği	AB
Avrupa Birliği Temel Haklar Şartı	ABTHŞ
Avrupa İnsan Hakları Sözleşmesi	AİHS
Avrupa Konseyi	AK
Avrupa Kömür Çelik Topluluğu	AKÇT
Avrupa Veri Koruma Denetçisi	EDPS
Birleşmiş Milletler	BM
Ekonomik İşbirliği ve Kalkınma Teşkilatı	OECD
Kişisel Verilerin Korunması Kanun Tasarısı	KVKKT
Mali Eylem Görev Gücü	FATF
Mali İstihbarat Birimleri	FIU
Mali Eylem Görev Gücü	FATF
Mutabakat Muhtırası	MoU
Sermaye Piyasası Kurulları Uluslararası Organizasyonu	UICI-IOSCO
Uluslararası Sigorta Denetçileri Birliği	IAIS

GİRİŞ

Sözlükte "veri", Bir araştırmanın, bir tartışmanın, bir muhakemenin temeli olan ana öge, muta, done[1] olarak tanımlanmıştır. Kişisel veri ise ulusal ve uluslararası pek çok hukuksal düzenlemede belirtildiği gibi, belirli ya da belirlenebilir nitelikteki bir kişiye ilişkin her türlü bilgidir. Bu durumda kişisel veriyi, kişisel olmayan verilerden ayırabilmek için temelde iki ölçütten yararlanıldığı söylenebilir. Buna göre, kişisel veriden söz edebilmek için verinin,

- bir kişiye ilişkin,
- bu kişinin de belirli ya da belirlenebilir nitelikte,

olması gerekir.

Bu doğrultuda bilgi, "anlamlı bir biçime sokularak, kullanıcısına güncel ve olası kararların alınmasında yardımcı olan veri"[2] olarak tanımlanmaktadır.

Verilerin korunması, temelde verilerin değil de bu verilerin ilişkili olduğu kişi ve kurumların korunmasını hedef alır. Verilerin korunması kişileri onlar hakkındaki bilgilerin bilgisayarla ya da elle işlenmesinden doğacak zararlardan koruma amacına yönelmiş ve kişisel verilerin korunmasına ilişkin ilkelerde somutlaşmış bir dizi yasal ya da yasal olmayan önlemi ifade eder.

Veriyi bulunduran ya da işleyenler açısından hukuki sorumluluk doğurma ihtimalinin daha yüksek olması nedeniyle kişisel verilerin korunması olgusunun genel manada kullanılan verilerin korunması olgusuna nazaran daha ön plana çıktığı söylenebilir. Bu bağlamda kişisel verilerin korunmasının ulusal ve uluslararası durumu hakkında değerlendirme yapılmasının daha faydalı olacağı açıktır.

Veri ile ilgili değerlendirme ve işleme faaliyetleri hakkında sorumluluğun doğabilmesi için verinin ilk olarak kaydedilmiş olması gerekmektedir. Bu bağlamda kaydedilmiş verilerin saklanması ve işleme amacının sona ermesini müteakip, kanunlarda belirtilen istisnai haller dışında, imha edilmesine ilişkin genel anlayışın da ortaya konulmasında fayda olacaktır.

Kayıtların tutulması ve kişisel verilerin korunmasının yanı sıra verilerin uluslararası işbirliği çerçevesinde paylaşımı da önemli bir husus olarak karşımıza çıkmaktadır. bu enstrümanlara ilişkin olarak uluslararası alanda gerçekleştirilmiş

[1] http://www.tdk.gov.tr/index.php?option=com_bts&arama=kelime&guid=TDK.GTS.5512b1dca74d95.20250379

[2] Faruk ÇUBUKÇU, Bilgisayar Terimleri Sözlüğü, V Yayınları, Ankara 1987, s.24.

anlaşmalarda yer alan hususlara da suç gelirlerinin aklanması ve terörün finansmanı ile mücadele bağlamında değinilmesi faydalı olacaktır.

İşbu Raporda, kayıt tutulmasına, kişisel verilerin korunmasına ve veri paylaşımı hususunda uluslararası işbirliğine ilişkin dünya çapında çok çeşitli düzenlemeler yapılmış olmakla birlikte, bu hususta genel bir çerçeve çizilebilmesini sağlamak adına Birleşmiş Milletler (BM); Ekonomik İşbirliği ve Kalkınma Teşkilatı (OECD); Avrupa Konseyi (AK) ve Avrupa Birliği (AB) kapsamında yapılmış düzenlemelere değinilecektir. Suç gelirlerinin aklanması ile mücadele bağlamında Mali Eylem Görev Gücü (FATF) temel prensiplerinde değinilen hususlara, Basel Komitesi'nin etkin bankacılık denetimine ilişkin uygulamalarına; Uluslararası Sigorta Denetçileri Birliğinin (IAIS) uygulamalarına; Sermaye Piyasası Kurulları Uluslararası Organizasyonu (UICI-IOSCO) uygulamalarına değinilecektir.

1. KİŞİSEL VERİLERİN KORUNMASI KONUSUNDAKİ ULUSLARARASI KAYNAKLARI

Kişisel verilerin korunması hususu, çeşitli hukuki metinler kapsamında ele alınmıştır. Bu metinlerden en önemlileri BM, OECD, Avrupa Konseyi ve Avrupa Birliği çatısı altında kaleme alınmıştır.

1.1. BİRLEŞMİŞ MİLLETLER KAPSAMINDA VERİ KORUMAYA İLİŞKİN YAPILMIŞ DÜZENLEMELER

BM II. Dünya Savaşı sonrasında uluslararası barışın devamı ve güvenliğin sağlanması, sürdürülebilir kalkınmanın desteklenmesi ve insan haklarının güvence altına alınması amacıyla Türkiye dahil 51 ülke tarafından 24 Ekim 1945 tarihinde kurulmuş ve günümüzde üye sayısı 192'ye ulaşmış bir örgüttür.

Birleşmiş Milletler İnsan Hakları Evrensel Bildirisi, hukuki açıdan bağlayıcı bir nitelik taşımasa da uluslararası düzeyde birtakım ideallere hizmet etmesi dolayısı ile uluslararası arenada siyasi ve moral açıdan etkiye sahiptir. Bildirinin 12nci maddesinde, özel yaşamın gizliliği hakkı düzenlenmiştir. 12. madde hükmü şöyledir:

"Hiç kimse, özel yaşamına, ailesine, konutuna ya da haberleşmesine yönelik keyfi müdahalelere ya da onur ve şöhretine yönelik saldırılara maruz bırakılmayacaktır. Herkesin, bu tür müdahale ya da saldırılara karşı yasa ile korunma hakkı vardır".

BM İnsan Hakları Komitesi 16. Genel Yorumu ile 17. maddenin kapsamına açıklık getirmiştir. Buna göre:

"Tüm insanların toplum içerisinde yaşamalarının sonucu olarak, özel hayatın gizliliğinin korunması kaçınılmaz şekilde görecelidir. Ancak, Sözleşme'den anlaşıldığı üzere yetkili kamu otoriteleri, bilinmesi toplumun çıkarlarının korunması açısından gerekli olan, bireyin özel hayatıyla ilgili bir bilgiyi öğrenme talebinde bulunabilmelidir. ... Kamu otoritelerinin, özel kişi ve kurumların bilgisayarlarda, veri bankalarında veya benzeri cihazlarda kişisel bilgileri toplaması veya saklaması hukuki düzenlemeye tabi olmalıdır. Devletler, bir kimsenin özel hayatına dair bilgilerin hukuken bu bilgilere sahip olma ve kullanma yetkisine sahip olmayanların eline geçmesini ve bu bilgilerin Sözleşme'nin amaçlarına aykırılık teşkil edecek şekilde kullanılmasını engellemek için etkili tedbirler almalıdır. Özel hayatın gizliliğinin en etkili şekilde korunabilmesi için, her birey kişisel dosyalarda veya veri tabanlarında kendisiyle ilgili bilgiler saklanmışsa bu bilgilerin ne tür bilgiler olduğunu ve ne amaçla saklandığını öğrenme hakkına sahiptir. Ayrıca, her birey hangi kamu otoritelerinin, özel kişilerin veya

kurumların bu dosyaları kontrol altında tuttuğunu veya tutabileceğini öğrenebilmelidir. Söz konusu dosyaların, yanlış kişisel bilgilere yer vermesi halinde veya bu bilgilerin hukuka aykırı şekilde toplanması veya kullanılması halinde her birey düzeltme veya bilgilerin ortadan kaldırılmasını talep etme hakkına sahiptir"

Görüldüğü gibi İnsan Hakları Komitesi, 17 nci madde ekseninde geliştirdiği yorum ile kişisel verilerin korunmasını özel yaşamın gizliliği hakkı içerisinde gördüğünü açıkça ortaya koymuştur. Komite'nin 17nci madde hükmünü değerlendirirken kişisel verilerin korunmasına ilişkin ulusal ve uluslararası düzenlemeleri dikkate aldığı görülmektedir.

BM, kişisel verilerin korunmasına ilişkin belli bir standart çalışmayı ortaya koymak maksadı ile 45/95 sayılı Bilgisayara Geçirilmiş Kişisel Veri Dosyalarına İlişkin Rehber İlkeler (Guidelines for the Regulation of Computerized Personal Data Files) adıyla kılavuz bir belge yayınlamıştır. On maddeden oluşan ve üye devletlerin veri korunması alanında asgari bir standarda kavuşmasını amaçlayan bu ilkelerin uygulanması üye ülkelerin inisiyatifine bırakılmıştır. Bahsi geçen Rehber İlkeler'de yer alan temel esaslara ve kısa açıklamalarına aşağıda yer verilmiştir.

- Yasallık ve dürüstlük: Kişisel veriler kanuna aykırı ve dürüst olmayan yollarla toplanmamalı ve toplanış amacına ve temel haklar ve özgürlüklerle ilgili ilkelere aykırı olarak kullanılmamalıdır.
- Doğruluk: Toplanan verilerin doğruluğu kontrol edilmeli ve doğru ve eksiksiz olarak saklanmasını ve güncelliğini sağlamak için saklandığı süre zarfında düzenli olarak kontrol edilmelidir.
- Amacın belirli ve haklı olması: Kişisel verilerin hangi haklı amaçla toplandığı başlangıçta kesin olarak belirlenmeli ve bu amaç bütün ilgililere açık olarak bildirilmelidir.
- İlgili kişilerin erişme hakkı: Kişisel veri ile ilgili kişi kimliğini kanıtlamak koşulu ile kendisi hakkında toplanan bilgilerin ne gibi bir işleme tabi tutulduğunu öğrenebilmeli ve bunların bir anlaşılabilir biçimdeki bir örneğini aşırı bir masraf ve zaman kaybı olmadan elde edebilmelidir.
- Ayrımcılıktan kaçınma: Kişinin etnik kökeni, ırkı, cinsel yaşamı, dini veya felsefi inançları gibi duyarlıklı konularla ilgili bilgiler ancak yasanın izin verdiği haklı ve gerekli durumlarda toplanmalıdır.

- İstisna koyma yetkisi: Görevli makamlara, milli güvenliği, kamu düzenini, halk sağlığını, genel ahlakı korumak veya diğer kişilerin hak ve özgürlüklerine zarar vermemek amacıyla yasallık ve dürüstlük, doğruluk, amacın belirli ve haklı olması, ilgili kişilerin erişme hakkı ilkeleri ile ilgili önlemlerden ayrılma yetkisi tanınabilir. Ancak bu yetkinin kapsamı ve sınırları kanunda açıkça belirlenmelidir. Ayrımcılıktan kaçınma ilkesine getirilecek istisnanın her durumda temel hak ve özgürlüklere aykırı olmaması gerekir.
- Güvenlik: Kişisel verilerin toplanması, saklanması ve işlenmesi ile görevli bütün kurum ve kişiler, bu verilerin doğal afetler, kazalar ve insanların işleyecekleri hata, kusur ve suçların yaratacağı tehlikelere karşı korunması için her türlü önlemi almalıdır.
- Denetim ve yaptırım: Kişisel verilerin korunması ile ilgili düzenlemelerde öngörülen ilke ve kuralların uygulanması ve önlemlerin alınması ve gerekli denetimlerin yapılması sorumluluğu tarafsız, yetkin ve adil bir makama verilmelidir.
- Sınır ötesi veri transferi: Kişisel verilerin saklanmakta olduğu ülkeden başka bir ülkeye aktarılması için öncelikle her iki ülkenin ulusal mevzuatlarının bu aktarmaya izin vermesi gerekir. Ayrıca, bu veriler için verinin gönderileceği ülkenin bu veri için sağladığı korumanın verinin bulunduğu ülkede sağlanan korumadan daha aşağı düzeyde olmaması da gerekir.
- Uygulama Alanı: Mevcut ilkeler kamusal ve özel sektör için bilgisayar aracılığıyla işlenen kişisel verileri kapsamakla birlikte, manuel olarak işlenen kişisel verilerde isteğe bağlı olarak dahil edilebilir. Tüzel kişilere ait verilerin gerçek şahıslara ilişkin kişisel verileri içermesi durumunda, isteğe bağlı olarak bu verilerde kişisel veri kapsamına dahil edilebilir

BM'nin Rehber İlkeleri, kişisel verilerin korunmasına ilişkin ilkelerin uygulamasını denetleyecek yetkili ve bağımsız bir veri koruma organının kurulmasını öngören ilk uluslararası hukuk belgesidir. Ancak bu öncü rolüne karşın metnin, AK Sözleşmesi ve OECD Veri Koruma İlkelerine göre çok daha sınırlı bir etkisi olmuştur. Bu durumun nedenlerinden biri olarak ilkelerin hukuksal açıdan bağlayıcı olmaması, yalnızca tavsiye niteliğinde bulunması düşünülebilir. OECD Veri Koruma İlkelerinin de aynı şekilde bağlayıcılığının bulunmamasına karşın, bu alandaki ilk uluslararası düzenleme olması dolayısıyla daha geniş bir etki yarattığı söylenebilir.

1.2. AVRUPA KONSEYİ KAPSAMINDA VERİ KORUMAYA İLİŞKİN YAPILMIŞ DÜZENLEMELER

AK, II. Dünya Savaşı sonrasında Avrupa'da meydana gelen parçalanmışlığın ve savaşın ortaya çıkardığı çatışma atmosferinin yok edilerek barışın tesis edilmesi amacıyla başlatılan çalışmaların neticesinde 5 Mayıs 1949 tarihinde kurulmuştur. Konsey Türkiye'nin de üyelerinin arasında yer aldığı hükümetler arası bir örgüttür. AK tarafından yapılan çalışmaların neticesinde ortaya çıkan sözleşmeler, daha çok ulusal yasal düzenlemelerin birbirleriyle ve Konsey standartları ile uyumlu hale gelmesi için yapılan çalışmalardır.

AK, Bakanlar Komitesi, Parlamenterler Meclisi ve Sekreterlikten oluşmaktadır. AK işleyişi, 47 üye hükümeti temsil eden Bakanlar Komitesi ile 47 milli parlamentoyu temsil eden Parlamenterler Meclisi'nin ortak çalışmalarına dayanmaktadır. Üye hükümetler Konsey çalışmalarını, örgütün karar organı olan Bakanlar Komitesi aracılığıyla doğrudan yönlendirmektedir. AK tarafından alınan kararlar sözleşmeler ve tavsiye kararları ile şekillenerek somut hale gelmektedir. Konsey uygulamalarında temel araç sözleşmelerdir. Sözleşmelerin bağlayıcılığı vardır. Tavsiyeler bağlayıcı nitelikte olmasa dahi, Statü'nün 15/b maddesine göre Bakanlar Komitesi üye devletlerden tavsiyelerin uygulanma şekli hakkında bilgi talep edebilir.

AK tarafından kişisel verilerin korunması ile ilgili 1981 tarihli ve 108 Sayılı Sözleşme düzenlenmiş olduğu gibi kişisel verilerin işlenmesi ile ilgili olarak veya 108 sayılı Sözleşmeyi güncellemek amacıyla ihtiyaca binaen birçok karar almıştır. Bu kararlar aşağıda yer almaktadır.

1995, 4 sayılı tavsiye kararı	Telekomünikasyon ve özellikle telefon hizmetlerinde kişisel verilerin korunması
1997, 5 sayılı tavsiye kararı	Tıbbi verilerin korunması
1997, 18 sayılı tavsiye kararı	İstatistik amaçlı toplanan ve işlenen kişisel verilerin korunması
1999, 5 sayılı tavsiye kararı	İnternet üzerinde gizliliğin korunması
2002, 9 sayılı tavsiye kararı	Sigorta amaçlı toplanan ve işlenen kişisel verilerin korunması
2010, 13 sayılı tavsiye kararı	Profil bilgisi içindeki kişisel verilerin otomatik işleme karşısında korunması
2012, 3 sayılı tavsiye kararı	Arama motorları ile ilgili insan haklarının korunması
2012, 4 sayılı tavsiye kararı	Sosyal ağ hizmetleri ile ilgili insan haklarının korunması

Kişisel verilerin korunması bağlamında AK tarafından yapılan en önemli çalışma 1981 yılında kabul edilen 108 Sayılı Kişisel Nitelikteki Verilerin Otomatik İşleme Tabi Tutulması Karşısında Şahısların Korunmasına Dair Sözleşme'dir. Bu sözleşmenin en önemli tarafı, kişisel verilerin korunması konusunda hukuksal bağlayıcılığı olan ilk uluslararası belge olmasıdır. Türkiye tarafından da imzalanmış olan sözleşme, ülkemizde henüz onaylanmamıştır.

AK tarafından kabul edilen Sözleşmeler, konusuna göre sınıflandırıldığında, iki durum söz konusudur, birincisi Avrupa"da standart bir kurallar bütünü oluşturulmasına katkı sağlayacak anlaşmalar, ikincisi ise üye ülkeler arasında işbirliğine katkı sağlayacak anlaşmalar şeklindedir. Standardize olmuş kuralları belirleyen 108 Sayılı Sözleşme birinci kategoride yer almaktadır.

108 sayılı Sözleşme, AK üyesi olmayan devletlerin de imzasına açıktır. Bu nedenle, yalnızca üye devletler için değil, Sözleşme'ye taraf olan üçüncü ülkeler için de konuya ilişkin bir çerçeve sunmaktadır. Nitekim Sözleşmenin 23ncü maddesinde AK Bakanlar Komitesinin maddede belirtilen şartların sağlanması durumunda üye olmayan her devleti bu sözleşmeye katılmaya davet edebileceğini belirtmektedir. Diğer taraftan Sözleşme, halen kişisel verilerin korunması alanında bağlayıcı olan tek uluslararası metindir.

Sözleşmenin amacı, taraf devletlerde her gerçek kişinin temel hak ve özgürlüklerini ve özellikle kişisel bilgilerinin otomatik bilgi işleme tabi tutulması karşısında özel yaşamın gizliliği haklarını, kısacası kişisel verilerinin korunmasını güvence altına almaktır.

AK Sözleşmesi'nin koruma kapsamında hem kamusal hem de özel sektör tarafından işlenen veriler bulunmaktadır. Bununla birlikte yalnızca otomatik yolla işlenen veriler için güvence öngörüldüğünden, elle işlenen veriler kapsam dışında kalmaktadır. Ancak bunu mutlak bir dışlama olarak düşünmemek gerekir. Nitekim Sözleşme'ye göre "otomatik işleme"den söz edebilmek için sürecin tamamının otomatik olması gerekmemektedir. Kısmen otomatik işlenen veriler de güvenceden yararlanmaktadır. Bu, Sözleşme'nin uygulama alanını oldukça genişletmektedir.

Sözleşmede belirlenen temel ilkeler şöyle sıralanabilir:

- Verilerin belirli bir nitelikte olması (madde 5): Buna göre otomatik olarak işlenecek kişisel verilerin meşru ve yasal yoldan elde edilmesi ve işlenmesi; belirli ve meşru amaçlar için tutulması ve bunlarla bağdaşmayan amaçlar için kullanılmaması; bu amaçlar için yalnızca ilgili ve gerektiği kadar verinin

saklanması; doğru ve gerektiğinde güncel olması; ilgili kişinin kimliğini belirtecek şekilde amaç için gerekli olandan uzun süre saklanmaması, kısaca "kaliteli" olması gerekir.

- Veri güvenliği (madde 7): Verilere yetkisiz erişimin, bunların değiştirilmesinin ya da ortadan kaldırılmasının önlenmesi için veri güvenliği sağlanmalıdır.
- İlgili kişinin bilgi alma, verilere ulaşma ve gerektiğinde onları düzeltme hakkı (madde 8): İlgili kişinin kendisine ilişkin otomatik olarak işlenmiş veriler hakkında bilgi alma, eğer bu veriler hukuka aykırı bir şekilde işlenmişse onları sildirtme, yanlış verileri düzeltme, eğer bu taleplerine uyulmazsa hukuksal yollara başvuru hakkı bulunmaktadır.

Sözleşmede bu hakların kullanımına bazı sınırlamalar getirildiği görülmektedir. Ancak burada sınırlamaların sınırlarına da yer verilmiştir. Buna göre, sınırlamalar ancak,

- Yasa ile devletin ya da kamunun güvenliği,
- Devletin ekonomik çıkarlarının korunması,
- Suçlarla mücadele veya ilgili kişinin ya da başkalarının hak ve özgürlüklerinin korunması,

amaçlarıyla ve eğer demokratik bir toplumda gerekli ise yapılabilir.

Sözleşme, taraf devletler arasında kişisel verilerin serbest aktarımını öngörmektedir. Buna göre taraf devletler arasında özel yaşamın gizliliğinin korunması gerekçesiyle, veri aktarımı yasaklanamaz ya da özel bir izne tabi tutulamaz. Ancak bu kurala iki durumda istisna getirilmiştir:

- Belirli veri kategorileri için özel bir koruma getirilmiş olması ve aktarımın yapılacağı Sözleşmeci devlette buna "eşdeğer" korumanın bulunmaması,
- Aktarımın, Sözleşme'nin tarafı olmayan üçüncü bir devlet aracılığıyla yapılacak olması.

Sözleşme ile bu metinde yer alan hükümleri yorumlamaktan ve uygulamaları geliştirmekten sorumlu bir Danışma Komitesi de oluşturulmuştur. Danışma Komitesi, 108 numaralı Sözleşme'ye ek 181 sayılı Ek Protokolü kabul etmiştir. Bu Protokol ile Sözleşme'deki önemli bir eksiklik giderilmeye çalışılmış ve veri işleme etkinliklerini denetleyecek bağımsız bir organ öngörülmüştür. Bu organ, niteliği bakımından AB'nin 95/46/AT sayılı Yönergesi'nde yer alan nitelikler ile paralellik göstermektedir. Ek Protokol 1 Temmuz 2004'te yürürlüğe girmiştir. Protokolün 3 üncü maddesinde,

Protokolün kabul edilebilmesi için ön koşul olarak 108 sayılı sözleşmenin imzalanmış ve yürürlüğe girmiş olması şartı bulunmaktadır. Türkiye bu protokolü 8 Kasım 2001 tarihinde imzalamış olmasına rağmen henüz onaylayamamış ve yürürlüğe sokamamıştır.

Protokol'de ayrıca Sözleşme'nin üçüncü ülkelere veri aktarımına ilişkin hükümler de yer almaktadır. Yine AB Yönergesine benzer bir şekilde Protokol ile "yeterli" düzeyde veri koruma sağlamayan üçüncü ülkelere kişisel verilerin aktarımı yasaklanmaktadır.

Protokol iki ana bölümden oluşmaktadır. Birinci bölümde denetim otoritelerinden ikinci bölümde ise sözleşmeye taraf olmayan üçüncü ülkelere yönelik sınır aşan veri trafiğinden bahsedilmiştir. Birinci bölümde, taraf ülkelere kişisel verilerin korunmasında etkin görev alacak bağımsız hareket eden kişisel verilerin korunması otoritelerinin kurulması gerekliliğinden bahsedilmiştir. Bu otoritelerin görevlerini yerine getirirken tam bir bağımsızlık içinde hareket etmeleri gerektiği ve bireylerden gelecek şikayetleri soruşturabilecek şekilde yetkilendirilmiş olmaları gerektiği belirtilmiştir. Gerektiği durumlarda adli makamlara başvur yapılabilmesini veya adli makamlar nezdinde itiraz edebilmesini sağlayacak mekanizmaların bulunması gerektiği ifade edilmiştir.

Yasalaşmayı bekleyen Kişisel Verilerin Korunması Kanun Tasarısı (KVKKT) içerisinde Türkiye için tasarlanmış tüzel kişiliği olan, bağımsız hareket edebilen, kendi özel bütçesi olan Kişisel Verileri Koruma Kurumu'nun kurulması için düzenleme yapılmıştır.

Protokolün ikinci bölümde sözleşmeye taraf olmayan üçüncü ülkelere sınır aşan veri trafiğinden bahsedilmektedir. Sınır aşan veri paylaşımında sözleşmeye taraf olmayan ülkelerde yeterli seviyede veri korumanın söz konusu olup olmadığına bakılarak paylaşımda bulunulabileceği, aksi takdirde bireyin kişisel verilerinin paylaşılmayacağı ifade edilmiştir. Bu transferin; veri sahibi bireyin özel bir yararının olması, kamu yararı ya da meşru bir yararın bulunması ve güvenlik tedbirleri için ülkelerarası anlaşmalar söz konusu ise, kişisel veriler üçüncü ülkelere veya milletlerarası organizasyonlara gönderilebileceği belirtilmektedir. Bu durumda yeterli seviyede veri korumanın olması yani uygunluğun olması şartının aranmayacağı ifade edilmiştir. Bu istisnalar ile sınır aşan veri trafiğinin net çizgiler çekilerek engellenmesinin önüne geçilmiş olmaktadır.

1.3. AVRUPA İNSAN HAKLARI SÖZLEŞMESİ KAPSAMINDA VERİ KORUMAYA İLİŞKİN YAPILMIŞ DÜZENLEMELER

5 Mayıs 1949'da 10 Avrupa ülkesinin bir araya gelmesiyle oluşturulan Avrupa Konseyi, insan hakları ve özgürlüklerinin devletlerce korunmasına ve geliştirilmesine vurgu yaparak insan haklarına saygı yükümlülüğünü üyelik koşulu olarak belirtmiştir. Avrupa Konseyi'nin bu anlamda ilk adımı 4 Kasım 1950'de Roma'da imzalanan ve 3 Eylül 1953'te yürürlüğe giren İnsan Hakları ve Özgürlüklerinin Korunmasına İlişkin Avrupa Sözleşmesi (AİHS)'dir. Sözleşme. İnsan haklarının korunmasını ve geliştirilmesini amaç edinir. AİHS hazırlık aşamasında Avrupa'daki demokratik rejimlerin devam ettirilmesi açısından gerekli olan asgari hak ve özgürlükleri güvenceye alarak işe başlamış, zamanla insan hakları listesini genişletmiştir. AİHS ekonomik, sosyal ve kültürel haklardan çok sivil ve politik hakların korunmasına öncelik vermiştir. Bu sözleşmeyi sosyal ve ekonomik hakları içeren "Avrupa Sosyal Şartı" izlemiştir. Türkiye 10 Mart 1954'te sözleşmeyi onaylamış, 28 Ocak 1987'de de bireysel başvuru hakkını tanımıştır. Mahkemenin zorunlu yargı yetkisini ise 28 Ocak 1990'da kabul etmiştir. AİHS, 45 Avrupa Konseyi üyesi devletin 44'ü tarafından onaylanmıştır.

Avrupa İnsan Hakları Sözleşmesi'nde kişisel verilerin korunmasının bağımsız bir hak alanı olarak yer almamaktadır. Ancak Sözleşme'nin 8 inci maddesinde özel yaşamın gizliliği hakkı düzenlenmiştir. Buna göre,

"1. Herkes özel ve aile yaşamına, konutuna ve haberleşmesine saygı gösterilmesi hakkına sahiptir.

2. Bu hakkın kullanılmasına bir kamu otoritesinin müdahalesi, ancak ulusal güvenlik, kamu emniyeti, ülkenin ekonomik refahı, dirlik ve düzenin korunması, suç işlenmesinin önlenmesi, sağlığın veya ahlakın veya başkalarının hak ve özgürlüklerinin korunması için, demokratik bir toplumda gerekli olan ölçüde ve yasayla öngörülmüş olmak koşuluyla söz konusu olabilir".

Avrupa İnsan Hakları Mahkemesi'nin verdiği pek çok kararında bazı temel ilkeleri Sözleşme'nin 8'inci maddesi kapsamında değerlendirdiğini görülmektedir. Buna göre:

- Bireylere ilişkin kişisel bilgilerin resmi makamlarca toplanarak arşivlenmesi[3],
- Toplanan verilerin toplanma amacı dışında kullanılması[4],

[3]Amann İsvçre'ye karşı, b.n. 27798/95; k.t. 16 Şubat 2000;
Rotaru Romanya'ya karşı, b.n. 28341/95, k.t. 4 Mayıs 200.

- Kişisel verilerin gerektiğinden uzun süre tutulması[5],

  gibi konular Mahkeme'nin çeşitli kararlarında 8/1 hükmü kapsamında değerlendirilmiştir.

  AİHS 8/2 hükmü uyarınca özel ve aile yaşamına müdahale,
- Burada sınırlı sayımla belirtilmiş amaçlardan bir ya da bir kaçına yönelik;
- Yasada öngörülmüş,
- Aynı zamanda demokratik toplum için gerekli ve öngörülen amaç ile orantılı olması,

  durumlarda meşrudur.

Sınırlı sayımla belirlenen ve özel ve aile yaşamına saygı hakkına istisna getiren meşru amaçlar şunlardır:

- Ulusal güvenlik,
- Kamu güvenliği,
- Ülkenin ekonomik refahı,
- Dirlik ve düzenin korunması,
- Suç işlenmesinin önlenmesi,
- Sağlığın veya ahlakın veya başkalarının haklarının korunması.

Görüldüğü gibi meşru amaçlar oldukça geniş bir şekilde belirlenmiştir. O kadar ki herhangi bir müdahalenin burada belirlenen meşru amaçları karşılayamaması oldukça zordur.

Mahkeme içtihadında yer alan "gerekli" deyimi "zorlayıcı toplumsal gereksinim"(pressing social need) ve yöneldiği amaç ile "orantılılık" olarak anlaşılmak durumundadır. Mahkeme, bunun belirlenmesinde üye devletlere bir "takdir marjı" tanımıştır. Bu gerekliliğin saptanmasında Mahkeme'nin yetkisi ikincil niteliktedir. Mahkemeye göre "ülke ve toplum gerçekleriyle dolaysız ve devamlı temasta olan ulusal merciler" ilk olarak bu değerlendirmeyi yapar. Ancak bu takdir yetkisi sınırsız olmayıp Sözleşme organlarının denetimine tabidir.

[4]Leander, İsviçre'ye karşı, b.n. 9248/81, k.t. 26 Mart 1987

[5]S. ve Marper, Birleşik Krallığa karşı, b.n. 30562/04, 30566/04, k.t. 4 Aralık 2008.

1.4. EKONOMİK İŞBİRLİĞİ VE KALKINMA TEŞKİLATI (OECD) KAPSAMINDA VERİ KORUMAYA İLİŞKİN YAPILMIŞ DÜZENLEMELER

OECD, 14 Aralık 1960 tarihinde imzalanan Paris Sözleşmesi"ne dayanılarak kurulmuş ve 30 Eylül 1961"de resmen işlerlik kazanmıştır. OECD'nin amacı, üye ülkelerin benzer sorunlara ortak çözüm üretebilecekleri, deneyimlerini paylaşabilecekleri ve uluslararası standartlar geliştirebilecekleri bir ortam sağlamaktır.

OECD bünyesinde kişisel verilerin korunması ile ilgili olarak yürütülen çalışmalar neticesinde 23 Eylül 1980 tarihinde uluslararası bir temel teşkil edecek şekilde, bağlayıcı olmayan ilkeleri içeren, "Mahremiyetin Korunması ve Kişisel Verilerin Sınır Ötesi Akışına İlişkin Rehber İlkeler" kabul edilmiştir.

1980 yılında yayınlanmış olan OECD Rehber İlkeleri'nde yer alan 2 nci bölüm "Ulusal Uygulama Temel İlkeleri" başlığı altında toplanmış ilkelerden oluşmaktadır. Bu bölümde yer alan 8 ilke, kişisel veri işleme faaliyetlerinde dikkate alınması gereken temel hususları ortaya koymuştur. Bu ilkelere ve konuya ilişkin kısa açıklamalara aşağıda yer verilmiştir.

1- Sınırlı Bilgi Toplama: Kişisel verilerin toplanmasında belirli sınırlamalar olmalıdır. Hukuka uygun sebepler ve araçlarla veri toplanırken, veri sahibi (öznesi) toplama konusunda bilgilendirilmeli ve bilinçli rızası alınmalıdır.

2- Veri Kalitesi: Kişisel veriler, kullanılacakları amaç ile ilgili olmak şartıyla mümkün olduğunca doğru, tam ve güncel olmalıdır.

3- Amaca Özgülük: Kişisel verilerin toplanma amacı belirlenmeli ve bu veriler sadece belirlenen amaç için kullanılmalıdır. Kullanım amacı, verinin toplandığı zamandan sonraki bir tarihte değişiyorsa veya yeni amaca uygun olarak veri işleme faaliyetinin veri sahibine zarar verme ihtimali varsa, veri sahibi kişi bilgilendirilmelidir.

4- Kullanım Sınırlaması: Toplanan veriler, "amaca özgülük" prensibi ile belirlenen amaçlar dışında yayılamaz, bulundurulamaz veya başka amaçlarla kullanılamaz. Kullanım sınırlamasının istisnaları; veri sahibinin bilinçli rızası ve kanuna dayalı yetkidir.

5- Güvenlik Önlemleri: Toplanan veriler, potansiyel tehlikelere karşı (kayıp, yetkisiz erişim, zarar verme, değiştirme, kullanma, açıklama) makul güvenlik tedbirleri ile korunmalıdır.

6- Açıklık (Aleniyet) İlkesi: Kişisel verilerle ilgili gelişmeler, uygulama ve politikalar hakkında genel bir açıklık ilkesi bulunmalı; kişilere kendileriyle ilgili veri

barındıran kurum ve kuruluşların bu gizlilik politikalarına kolaylıkla erişebilme hakkı sağlanmalıdır.

7- Bireyin Katılımı (Rıza): Veri öznesinin rızası olmaksızın veriler erişilebilir hale getirilmemeli ve açıklanmamalıdır. Bununla birlikte veri sahibinin;
   a) Veri kontrolörünün kendisi ile ilgili veriye sahip olup olmadığı hakkında bilgi alma hakkı olmalıdır.
   b) Kendisiyle ilgili veri konusunda kontrolör ile makul bir süre içinde, ölçülü bir ücret mukabilinde, makul bir şekilde, açık ve anlaşılabilir araçlarla irtibata geçme hakkı sağlanmalıdır.
   c) Yukarıdaki (a) ve (b) bentlerinde yazılı gerekçelerle yapılan bir başvuru reddedilmişse buna karşı itiraz etme hakkı olmalıdır.
   d) İtiraz kabul edilirse verinin silinmesi, değiştirilmesi veya düzeltilmesini isteme hakkı temin edilmelidir.

8- Hesap Verebilirlik: Veri öznelerinin veri toplayıcılarına karşı yukarıdaki ilkeler çerçevesinde hesap sorabilmeleri mümkün olmalıdır.

şeklinde sıralanabilir.

1.5. AVRUPA BİRLİĞİ KAPSAMINDA VERİ KORUMAYA İLİŞKİN YAPILMIŞ DÜZENLEMELER

AB'nin bugünkü yapısına kavuşmasını sağlayan süreç,18 Nisan 1951'da 6 ülkenin (Almanya, Fransa, İtalya, Belçika, Hollanda ve Lüksemburg) Paris Antlaşması'nı imzalaması ve Avrupa Kömür Çelik Topluluğu'nun (AKÇT) kurması ile ivme kazanmıştır. 7 Şubat 1992 tarihinde imzalanan Maastricht Anlaşması ile AB'nin bugünkü yapısının temelleri atılmıştır.

AB, yasama, yürütme ve yargı erkleriyle tam olarak bir devlet yapılanmasına sahip olmamakla birlikte, diğer ulusüstü örgütlere kıyasla, üye devletlerce topluluklara daha geniş yetkiler devredilmiştir. Bu kapsamda, AB'ye dahil olan ülkeler, anayasalarında gerekli düzenlemeler yaparak Topluluk organlarına yetki devri yapmışlardır.

Uluslararası hukukta kurallar devletler tarafından bazı durumlarda sınırlı olarak örgütler tarafından konulurken AB hukukunda, kurucu antlaşmalar yanında kurallar AB organları tarafından konulmaktadır. Uluslararası hukuk, devletleri ve örgütleri muhatap alırken, AB hukukunda iç hukuk, kişileri ve bireylerde muhatap almaktadır.

Diğer bir deyiş ile gerçek ve tüzel kişiler ile devletler içinde bağlayıcılık söz konusudur. AB'de Avrupa Adalet Divanı (AAD) gibi yaptırımları uygulayacak bir yargı erkinin olması da AB'yi diğer ulusüstü örgütlerden ayırmaktadır

Topluluk hukukunun kaynakları; birincil kaynaklar olan anayasal antlaşmalar, ikincil kaynaklar olan Topluluk organlarının tasarrufları, AAD tarafından tanınan hukukun genel ilkeleri, AAD'ın kararları, üye olmayan devletlerle yapılan uluslararası antlaşmalar ve yazılı olmayan topluluk hukuku kurallarıdır.

Birincil kaynaklar olan anayasal antlaşmalar; topluluğun kuruluş, işleyiş ve organlarına ilişkin temel kuralların yer aldığı mevzuattır. Bunlar bir nevi topluluğun temel ve dayanak yasal altyapısını oluşturan düzenlemelerdir. Kurucu antlaşmalar ve bu antlaşmalar üzerinde değişiklik yapan antlaşmalar, antlaşmaları tamamlayan ek ve protokollerle birlikte Birliğe yeni üye olan ülkelerle yapılan katılma antlaşmaları da bu kapsamdadır.

İkincil kaynaklar AB Kurumları'nın kendilerine tanınmış yetkileri kullanırken gerçekleştirdikleri işlemler sonucunda aldıkları kararlardır. Bunlar AB'nin İşleyişine İlişkin Antlaşma'nın 288 inci maddesinde düzenlenmişlerdir. Madde, Birliğin işlemlerini tüzükler, yönergeler (direktifler), kararlar, tavsiye kararları ve görüşler olarak sıralamaktadır. Tüzükler doğrudan üye ülkelerin iç hukukunda yürürlüğe girer ve bağlayıcıdırlar. Yönergeler, bağlayıcıdır ve iç hukuka aktarılması üyelere bırakılmıştır, uygulanma şekli üyelerin kendisine bırakılmıştır. Kararlar yöneltildiği devlet, birey veya şirket için bağlayıcı olmakla birlikte iç hukuka aktarılma zorunlulukları yoktur.

İkincil kaynakların, birincil kaynaklarda çizilen sınırlar dışına çıkmayacak kararları içermesi gerekmektedir. Kişisel verilerin korunmasında temel düzenleme olan "Kişisel Verilerin İşlenmesi ve Bu Verilerin Serbest Dolaşımına İlişkin 95/46 Sayılı Avrupa Parlamentosu ve Konseyi Yönergesi" ikincil kaynaklara önemli bir örnektir.

AAD"ın kararları özel kişileri, tüzel kişileri ve devletleri doğrudan bağlayıcı nitelik taşımaktadır. Divan kararları ulusal yasalarla çeliştiği takdirde dahi doğrudan uygulanmaktadır.

AB nezdinde hukuki açıdan bağlayıcı niteliği olan Avrupa Birliği Temel Haklar Şartı'nda (ABTHŞ) yer alan, kişisel verilerin korunması hakkı başta özel hayatın gizliliği kapsamında belli seviyede korunmaktayken tam olarak temel hak ve özgürlükler kapsamında değerlendirilmemiştir. ABTHŞ'nin "Özgürlükler" başlıklı 2 nci

bölümünün 8 nci maddesinde, kişisel verilerin korunması hakkı başlı başına bir hak olarak düzenlenmiştir.

Topluluğu kuran antlaşmalarda topluluk organlarına üye olmayan devletlerle ve uluslararası örgütlerle antlaşma yapma yetkisi verilmiştir. Bu şekilde yapılan antlaşmalar üye devletler açısından bağlayıcı nitelik taşımaktadır. Bu anlaşmalar, ekonomik olarak karşılıklı ilişkileri düzenleyen herhangi bir ürünle ilgili olabileceği gibi sosyal ve siyasi şartları içeren düzenlemeleri de konu alabilen çok geniş çaplı olabilmektedir. ABD ile AB arasında imzalanan Safe Harbor Antlaşması, üye olmayan devletlerle topluluk organları arasında yapılan antlaşmaya bir örnektir.

1.5.1. 95/46/AT Sayılı Kişisel Verilerin Korunması Yönergesi

AB bünyesinde yapılan kişisel verilerin korunmasına ilişkin en önemli metinlerden biri "Kişisel Verilerin İşlenmesi Ve Bu Türdeki Verilerin Serbest Dolaşımı Bağlamında Bireylerin Korunmasına İlişkin 24 Ekim 1995 tarihli ve 95/46/AT sayılı Avrupa Parlamentosu ve Konseyi Yönergesi'dir.

Yönerge'nin 1 nci maddesi, kişisel verilerin korunmasının temel bir insan hakkı olduğunu açıkça ortaya koymaktadır. Bu hükme göre,

"Üye Devletler, gerçek kişilerin temel hak ve özgürlüklerini ve özellikle kişisel verilerin işlenmesi ile ilgili özel yaşamın gizliliği hakkını koruyacaktır".

Avrupa Adalet Divanı'da Yönerge'nin yalnızca iç pazarı geliştirme amacına yönelmediğini, temel hedeflerinden bir diğerinin insan haklarını korumak olduğunu teyit etmiştir. Bu bağlamda Yönergenin hem ekonomi hem de hukuk alanında önemli etkilerinin olduğu söylenebilir.

Görüldüğü gibi Yönerge ile özellikle önleyici bir korumanın sağlanması hedeflenmektedir. Veri Koruma Yönergesi'nin uygulama alanı birkaç açıdan sınırlandırılmıştır. Buna göre Yönerge, tamamı ya da bir bölümü otomatik olarak işlenen kişisel verilere ve otomatik olmayan yollarla işlenen verilerden bir dosyalama sistemine kaydedilenler veya kaydedilebilecek olanlar için uygulanır. Biraz karmaşık şekilde dile getirilmiş olsa da bu hükümden veri işleme usulünden bağımsız olarak neredeyse bütün kişisel verilerin korunması istendiği çıkarılabilir. Nitekim günümüzde kişisel veriler, başta bilgisayarlar aracılığıyla olmak üzere, büyük oranda otomatik yollarla işlenmektedir. Arşivdeki dosyaların ise pek çok yerde hızla elektronik ortama aktarıldığı görülmektedir.

Yönerge'nin uygulama alanı, verileri işleyen kişiye ve işleme amacına ilişkin olarak da bazı konularda sınırlandırılmıştır. İlk olarak AB'nin üçüncü sütununda yer alan ve topluluk hukukunun alanına girmeyen,

- Kamu güvenliği,
- Savunma,
- Devlet güvenliği,
- Ceza hukuku,

alanlarında devletin etkinliklerinde Yönerge hükümleri uygulanmayacaktır.

Yönerge'nin 3/2 maddesi hükmü bu sınırı açıkça belirlemiştir. Buna göre, metinde yer alan hükümler, Avrupa Birliği Kurucu Antlaşması'nın V nci ve VI ncı Başlıkları altında düzenlenen konular gibi topluluk hukukunun dışında bulunan alanlarda ve her halükarda,

- Genel asayişte,
- Savunmada,
- Devletin güvenliğinde,
- Devletin ceza hukukuna ilişkin etkinliklerde,

kişisel verilerin işlenmesinde uygulanamaz.

AB Andlaşması'nın V nci Başlığı "Ortak Dış Politika ve Güvenlik Politikasına İlişkin Hükümler"i içermektedir. VI ncı Başlık altında ise "Adli Konularda Polis ve Adli İşbirliğine İlişkin Hükümler" düzenlenmiştir. Oldukça önemli olan bu alanlarda Yönerge'nin zorlayıcılığı bulunmamaktadır.

İkinci bir istisna, gerçek kişilerce tamamen kişisel ya da ailevi etkinlikler çerçevesinde yapılan veri işlemelere Yönerge'nin uygulanamayacak olmasıdır. Buna göre örneğin bir adres defteri, ticari ya da profesyonel amaçla değil, tamamen kişisel amaçlarla tutulmuşsa Yönerge'nin uygulama alanı dışında kalmaktadır.

AAD'nın Yönerge'nin uygulama alanına ilişkin Lindqvist kararında, İnternet ortamında bulunan kişisel veriler açısından Yönerge'nin uygulama alanına ilişkin genel kuralı belirlenmiştir. Buna göre Divan, kişilerin adları ve telefon numaraları gibi bilgilerin bir İnternet sitesinde yayınlanmasının, başka bir etkinliğe gerek görülmeksizin, "verilerin otomatik yolla işlenmesi" anlamına geleceğine hükmetmiştir.

1.5.1.1. 95/46/AT Sayılı Kişisel Verilerin Korunması Yönergesi Kapsamında Üçüncü Ülkelere Veri Aktarılması

Veri Koruma Yönergesi "aktarım"a ilişkin bir tanım geliştirmemiştir. Bu husus, hangi durumların veri aktarımı olarak değerlendirileceğini saptamayı güçleştirici bir unsur olarak karşımıza çıkmaktadır.

Üçüncü ülkelere kişisel verilerin aktarımına ilişkin kurallar, AB Kişisel Verilerin Korunması Yönergesi'nin 25 ve 26 ncı maddeleri hükümlerinde düzenlenmiştir. Yönerge uyarınca, kural olarak, üçüncü ülkelere veri aktarımı ancak bu ülkelerde kişisel verilerin "yeterli düzeyde" korunması durumunda olanaklıdır.

1.5.1.1.1. Yeterli Düzeyde Koruma Koşulu

Daha önce de belirttiğimiz üzere kişisel verilerin "yeterli" düzeyde korunduğu ülkelere veri aktarımının gerçekleşmesinin olanaklı bulunmaktadır. Ancak "yeterli" düzeyin ne olduğunun saptanması pek de kolay değildir. Yönerge'ye göre, bir veri aktarımında ya da veri aktarımı grubunda, koruma düzeyinin yeterliliği bütün koşullar göz önüne alınarak değerlendirilecektir. Bu bağlamda,

- Verinin niteliği,
- İşlemenin (ya da işlemelerin) amacı ve süresi, çıkış yeri ülkesi ve varacağı ülke,
- Üçüncü ülkede geçerli genel ve sektörel hukuk kuralları,
- Bu ülkede uyulan mesleki kurallar ve uygulanan güvenlik önlemleri özellikle dikkate alınacaktır.

"Yeterli" düzeyin ne olduğu saptanırken, yalnızca ilgili hukukta konuya ilişkin olarak belirlenmiş kurallara değil, bu kuralların işlerliğini sağlamak için oluşturulmuş sistemin de dikkate alınması gerekmektedir. Veri aktarımının gerçekleşmesi istenilen üçüncü ülkede verilerin yeterli düzeyde korunup korunmadığının saptanmasında hem üye devletlerin hem de Komisyon'un üzerine düşen çeşitli görevler bulunmaktadır. Yapılan inceleme sonucunda yeterli düzeyde korumanın sağlanmadığı fark edilirse Komisyon'un ve üye devletlerin birbirlerini durumdan haberdar etme yükümlülükleri bulunmaktadır.

1.5.1.1.2. İstisnalar

Verilerin Korunması Yönergesi'ne göre eğer verilerin aktarılacağı ülkede yeterli düzeyde koruma yoksa aktarımın yapılabilmesi ancak istisnai bazı durumlarda söz konusu olabilir. Buna göre, aşağıdaki durumlarda söz konusu yasaktan muafiyet tanınmıştır.

- İlgili kişinin aktarım için açık rızasının bulunması[6]: Yalnızca rızanın varlığı bu koşulun karşılanması için yeterli değildir. Ayrıca rızanın açık ve ilgili kişinin isteği konusunda şüphe bırakmayacak nitelikte; özgürce verilmesi ve ilgili kişinin bilgilendirilmiş olması gerekir.
- Aktarımın bir sözleşmenin ifası veya ilgilinin talebi ile sözleşme öncesi bir ilişkinin yürütülmesi için gerekli olması[7]: oldukça geniş kapsamlı bu istisna "gereklilik" ölçütü ile sınırlandırılmıştır. Gereklilik testinde, veri öznesi ile sözleşme arasında yakın ve gerçek bir bağ bulunması aranmaktadır.
- Aktarımın ilgili kişinin çıkarlarının korunması doğrultusunda, veri kontrolörü ve üçüncü bir kişi arasında yapılan bir sözleşmenin sonuçlandırılması ve uygulanması için gerekli olması[8]: Bir önceki istisnada olduğu gibi burada da aktarımın "gereklilik"i koşulu öne çıkmaktadır.
- Aktarımın önemi bir kamusal çıkarın korunması; hukuksal taleplerin tesisi, ileri sürülmesi ve korunması için gerekli veya yasa gereği zorunlu olması[9]: Buradaki "kamusal çıkar" ölçütünün dar yorumlanması gerekmektedir. Aksi takdirde istisnanın sınırları özü ile bağdaşmayacak oranda genişleyebilir. Veri Koruma Yönergesi'nin Başlangıç Bölümü'nde bu duruma örnek olarak vergi veya gümrük kurumları arasında veya sosyal güvenlik konularında yetkili birimler arasında uluslararası veri aktarımı gösterilmiştir.
- Aktarımın ilgili kişinin yaşamsal bir çıkarının korunması için gerekli olması[10]: Bu istisna, ilgili kişinin sağlığına ilişkin acil bir durumda, tıbbi yardım alması için verilerin aktarılmasının gerekli olması halinde söz konusu olmaktadır.
- Aktarımın herkese (ya da ilgisini kanıtlayan herkese) açık olan kamu sicillerinden yapılması ve veri koruma mevzuatının aradığı şartları taşıması[11]:

[6]Veri Koruma Yönergesi, m. 26/1,a.
[7]Veri Koruma Yönergesi n. 26/1,b.
[8]Veri Koruma Yönergesi, m. 26/1,c.
[9]Veri Koruma Yönergesi, m. 26/1,d.
[10]Veri Koruma Yönergesi, m. 26/1,e.
[11]Veri Koruma Yönergesi, m. 26/1,f.

Bu istisna, mantıksal temelini kayıtların herkese açık olmasında bulur. Eğer ilgili ülkede meşru çıkarı olan herkes bu bilgilere ulaşabiliyorsa, üçüncü ülkelerde bulunan kişilerin de onlara ulaşmasında bir engel bulunmamalıdır. Ancak bu, verilerin veya veri kategorilerinin tamamının aktarılabileceği şeklinde yorumlanmamalıdır. Aktarım meşru çıkarı olanların talebi üzerine ya da bu kişiler alıcı konumunda ise söz konusu olacaktır.

1.5.1.1.3. Bağışıklık Sözleşmeleri (Safe Harbor)

2000 yılında ABD ile AB arasında veri aktarımına yönelik farklı yaklaşımları bir uzlaşıda birleştirmek veri aktarımını temin etmek maksadı ile bir anlaşma yapılmıştır. "Bağışıklık Sözleşmesi" (Safe Harbor) olarak adlandırılan bu anlaşma, ABD ve AB arasında kabul edilen bir dizi veri koruma ilkesinden oluşmaktadır. Bu anlaşma, Amerikan Ticaret Bakanlığı yardımıyla yürütülecek bir program öngörmektedir.

Safe Harbor kapsamda kabul edilen ilkeler uyarınca, Amerikan ticari şirketlerinden, antlaşmada belirtilen ilkelere bağlı olacaklarını belirterek, yeterli düzey koruma sağlayanlar, AB tarafından sanki bu ilkeyi gerçekleştirmiş bir ülkede işlem yapıyormuş gibi değerlendirileceklerdir. Böylece Bağışıklık Sözleşmesi kapsamında olan şirketlerle AB arasında veri aktarımı gerçekleştirilebilecektir. Şirketlerin gerekliliklere uygun hareket etmeleri ise Amerikan yönetimi tarafından sağlanacaktır.

Safe Harbor temel olarak verilerin işlenmesine ilişkin yedi ilkeyi içermektedir. Bunlar,

- Bildirim,
- Seçim,
- Aktarım,
- Güvenlik,
- Doğruluk,
- Erişim,
- Uygulama,

olarak sıralanabilir.

Safe Harbor uyarınca özel nitelikli (hassas kişisel veriler) söz konusu olduğunda, özel bazı gerekliliklerde öngörülmüştür. Bu durumda eğer bu türdeki veri toplandığı sırada belirtilen amaçtan başka nedenlerle kullanılacaksa yada üçüncü kişiye aktarılacaksa şirketin mutlaka rızayı "opt-in" alması gerekir.

Safe Harbor uyarınca veri koruma otoritesi öngörülmemiştir. Ayrıca bu ilkelere bağlılığını açıklamak Amerikan şirketleri açısından bir zorunluluk da değildir. Ancak şirketlerin bağışıklık sözleşmesine katılımı tamamen gönüllük esasına dayansa da sözleşmeyi ihlal etmelerini engelleyecek bir sistem bulunmaktadır[12].

1.5.2. AB Kurumları Ve Yapılarının Kişisel Verileri İşlemesi Ve Bu Verilerin Serbest Dolaşımı Hususunda Kişilerin Korunması Hakkında Tüzük

Topluluk kurum ve organları tarafından kişisel verilerin işlenmesi sırasında gerçek kişilerin korunması 18 Aralık 2000 tarihli 45/2001/AT sayılı bir tüzük ile sağlanmıştır. Kısaca AT Organlarında Verilerin Korunması Tüzüğü olarak adlandırılabilecek bu metin, Avrupa Parlamentosu, AB Konseyi, Avrupa Komisyonu, Avrupa Adalet Divanı ve Sayıştayı ile Topluluk hukuku çerçevesinde yaratılmış diğer organ ve kurumları bünyesinde kişisel verilerin işlenmesinde uyulacak esasları saptamaktadır. Yönergede belirlenen temel ilkeler kısaca şöyle özetlenebilir:

- Verinin kaynağını bilme hakkı,
- Yanlış verileri düzeltme hakkı,
- Hukuk dışı işlemelere karşı başvuru hakkı,
- Doğrudan pazarlama gibi bazı konularda verilerin kullanılmasına izin vermeme hakkı.

  Tüzüğün 4 üncü maddesi kapsamına giren kişisel verilerin,
- Adil ve hukuka uygun bir şekilde işlenmesi,
- Belirli, açık ve yasal amaçlarla toplanması gerektiği; bu amaçlar dışında işlenmemesi gerektiği,
- Toplanan verinin tarihi, istatistiki ve bilimsel amaçlarla daha fazla işlenmesi durumunda, amaç dışı kullanımın engellenmesi için veri güvenliğinin sağlanması gerektiği,
- Yeterli, uygun ve toplama/daha fazla işleme amacını aşmayan nitelikte olması gerektiği,
- Doğru, gerektiğinde güncel, her aşamada doğru olmayan ve yanlış bilginin silinmesini ve düzeltilmesini sağlayacak adımların oluşturulması gerektiği,
- Verinin toplanma ve daha fazla işlenme amacı dışında kullanımını engelleyecek şekilde öznesinin belirlenmesini sağlayacak formda tutulmasının

[12] http://www.export.gov/safeharbor/

gerektiği. Verinin uzun süreli olarak tarihi istatistiki ve bilimsel amaçla tutulmasının gerekmesi alinde anonimleştirilmesinin gerektiği; anonimleştirmenin mümkün olmadığı durumlarda veri öznelerinin şifrelenmesi gerektiği,

Belirtilmektedir.

Tüzüğün 7 nci maddesine göre Tüzük kapsamında olan kişisel verilerin Birlik kuruluş ve yapılarına aktarılması,

- Alıcının yetki alanında olup yasal olarak görevleri yerine getirmesi ile ilgili olduğunda,
- Alıcı ve kontrolörün aktarımın yasal olduğuna dair sorumluluğu üstlendiklerinde,

mümkün olmaktadır. Ayrıca, verinin aktarım sebebi ile sınırlı bir şekilde kişisel veriyi işleyebilecektir.

Tüzüğün 8 nci maddesine göre, 95/46/AT sayılı Direktif kapsamında olup ta Birliğin kurum ve yapıları arasında olmayan alıcılara kişisel verilerin aktarılması, kişisel verinin,

- Kamu çıkarları ile ilgili veya kamu otoritesinin uygulamaları ile ilgili görevlerin yürütülmesi ile ilgili olduğunun alıcı tarafından kanıtlanması,
- Veri transferinin gerekliliğinin alıcı tarafından kanıtlanması ve veri öznesinin yasal çıkarlarının ön yargılı olduğunu var saymak için neden bulunmaması,

durumlarında mümkündür.

Tüzüğün 9/1 inci maddesine göre, Hem Birliğin kurum ve yapıları arasında olmayan hem de 95/46/AT sayılı Direktif kapsamında bulunmayan alıcılara kişisel verilerin aktarılması,

- Alıcının ülkesinde veya alıcı uluslararası organizasyonda yeterli derecede koruma tedbirlerinin alınmış olması,
- Veri transferinin sadece kontrolörün yetkisinde uygulanan görevlerde gerçekleştirilmesi,

durumlarında mümkündür.

Tüzüğün 9/2 inci maddesine göre, üçüncü ülke veya uluslararası organizasyonun sağlayacağı korumanın yeterli olup olmadığının değerlendirilmesi,

- Verinin doğası,
- İşlem veya işlemlerin amaç ve süresi,

- Alıcı üçüncü ülke veya alıcı uluslararası organizasyon,
- Hukuk kuralları,
- Profesyonel kurallar ve güvenlik tedbirleri,

  Dikkate alınmak sureti ile karar verilmesi gereken bir husustur.

  Tüzüğün 9/6 inci maddesine göre, Tüzüğün 9/1 ve 9/2. maddelerinde belirtilen durumlara istisna olarak, Komisyon kurum veya yapıları,
- Verisi aktarılacak kişinin açık rızası,
- Verisi aktarılacak kişi ile kontrolör arasındaki bir kontratın uygulanmasında ya da bu kişinin kontrat öncesi işlemlerin yapılmasını teminen aktarım isteğinin olması,
- Kontrolör ve üçüncü tarafın, verisi aktarılacak kişinin menfaatine sonuçlar doğuracak bir kontratın uygulanması ve sonuçlanması maksadı ile,
- Önemli kamu yararı temelinde yasal olarak gerekmesi, yasal iddiaların oluşturulması; uygulanması ve savunulması için gerekliyse,
- Verisi aktarılacak kişinin hayati çıkarlarının korunması maksadıyla,
- Birlik hukuku gereğince kamuya yönelik bilgi veren, genel anlamda kamunun bilgi edinmesine açık sicillerden; belli bir olay ile ilgili olarak konsültasyonun yerine getirilmesi hususunda kişisel çıkarını kanıtlayan kişilere,

  veri aktarımı gerçekleştirilebilmektedir.

Tüzüğün 9/7 inci maddesinde belirtildiğine göre, 9 uncu maddenin birinci paragrafında belirtilen anlamda yeterli seviyede koruma sağlayamayan, ancak mahremiyetin korunması; temel haklar; bireylerin özgürlükleri ve bununla bağlantılı hakların uygulanması hususlarının sözleşme hükümleri ile güvence altına alındığının kontrolör tarafından karara bağlanması halinde Avrupa Veri Koruma Denetçisi tarafından üçüncü ülkeye veya uluslararası organizasyona kişisel verilerin/veri setlerinin aktarılmasına onay verebilir.

Tüzüğün 20/1 inci maddesinde belirtildiği üzere, Birlik kurumları ve yapıları, “veri kalitesi” başlıklı 4/1 maddesin, “veri öznesinden temin edilen bilgiler” başlıklı 11 inci maddesi; “veri öznesi dışındaki kaynaklardan temin edilen bilgiler”başlıklı 12/1 maddesi, Veri Öznesinin Hakları başlıklı 5 inci Bölümde yer alan “erişim hakkı” başlıklı 13 üncü maddesi; “onaylama” başlıklı 14 üncü maddesi; “bloklama” başlıklı 15 inci maddesi; “silme “ başlıklı 16 ncı maddesi ve “üçüncü tarafların

bilgilendirilmesi” başlıklı 17 nci maddesi ile “veri alışverişi ve faturalandırması” başlıklı 37/1 maddelerinin uygulanmasına aşağıdaki gerekçelerle sınırlama getirebileceklerdir:

- Cezayı gerektiren suçların önlenmesi, soruşturulması, araştırılması, kovuşturulması,
- Para, bütçe ve vergi konuları ile ilgili olarak üye devletin ya da Avrupa Topluluklarının önemli ekonomik ve mali çıkarlarının olması,
- Veri öznesinin korunması, diğer kişilerin hak ve özgürlüklerinin korunması,
- Ulusal güvenlik, kamu güvenliği veya üye devletin savunması,
- İlk iki maddede belirtilen hususlar ile ilgili olarak, resmi otoritelerin izleme, denetim, düzenleyici işlemleri.

Tüzüğün 20/2 inci maddesinde belirtildiği üzere, 13 ila 16 madde hükümlerin uygulanması, verilerin sadece bilimsel araştırma veya yalnızca istatistik oluşturulmasına kadar geçecek makul sürede kişisel formda saklanması, veri öznesinin mahremiyetinin ihlal edilmesi riskinin bulunmaması ve kontrolörün yeterli yasal güvence sağlaması durumunda; verinin yaptırım uygulanması veya kişiler hakkında karar verilmesi maksadı ile kullanılmaması şartıyla mümkündür.

2. KİŞİSEL VERİLERİN KORUNMASI HUKUKUNUN TEMEL İLKELERİ

Kişisel verilerin korunmasına ilişkin temel ilkeler bu hususta belli bir standardın ortaya konulabilmesinde olumlu katkı yapan unsurlardandır. Söz konusu ilkelerden Raporumuzu ilgilendirenlere aşağıda yer verilmiştir.

2.1. KİŞİSEL VERİLERİN NİTELİĞİNE İLİŞKİN İLKELER

"Verilerin kaliteli olması ilkesi" olarak da ifade edilebilecek bu gerekliliğin içeriği, 95/46/AT sayılı Yönerge'nin 6 ncı maddesinde beş ayrı fıkrada belirlenmiştir. Buna göre kişisel veriler,

- Hukuka ve dürüstlük kurallarına uygun işlenmeli,
- Belirli, açık ve meşru amaçlar için toplanmalı,
- Toplanma ve daha sonrasında işlenme amaçlarına uygun, ilgili bulunmalı ve aşırı olmamalı,
- Doğru ve eğer gerekli ise güncel olarak tutulmalı,
- Amacın gerektirdiğinden daha uzun bir süre tutulmamalıdır.

2.1.1. Hukuka Ve Dürüstlük Kurallarına Uygun İşleme

Hukuka uygun olma gerekliliği kendi kendini açıklar niteliktedir. Bu gereklilik, kişisel verilerin işlenmesinde yasalarla ve diğer hukuksal düzenlemelerle getirilen ilkelere uygun hareket edilmesi zorunluluğunu ifade eder. AB Yönergesi'nde işleme oldukça geniş bir şekilde tanımlanmıştır. Buna göre:

"'kişisel verinin işlenmesi' ('isleme') toplama, kaydetme, düzenleme, saklama, uyarlama veya değiştirme, geri alma, danışma, kullanma, ileti ile açığa çıkarma, yayma veya başka şekilde oluşturma, sıraya koyma ve ya birleştirme, engelleme, silme veya yok etme gibi otomatik olan veya olmayan araçlarla, kişisel veri üzerinde uygulanan her türden işlem veya işlem dizisi anlamına gelir"[13].

AK Sözleşmesi'nde de işleme bütün bu süreçleri kapsar şekilde tanımlanmıştır[14]. Dürüstlük kuralına uygun olma ilkesi ile veri denetçilerinin, veri işlemedeki hedeflerine ulaşmaya çalışırken, ilgili kişilerin çıkarlarını ve makul beklentilerini dikkate almaları gerektiğinin ifade edildiği söylenebilir. Bu, işlemenin

[13] AB Yönergesi m. 2/b.

[14] AK Sözleşmesi'ne göre otomatik işleme *"bütünüyle ya da bir bölümü otomatik şekilde olmak üzere: şu işlemleri kapsar: verilerin depolanması, bu verilerin üzerinde mantıksal ya da aritmetik işlemlerin uygulanması, bunların değiştirilmesi, silinmesi, düzeltilmesi veya yayınlanması"* Bkz. AK Sözleşmesi m. 2/c.

ilgili kişi için şeffaf olması ve veri koruma görevlisinin bilgilendirme ve uyarı yükümlülüklerine uygun hareket etmesi gerekliliğini de kapsar.

2.1.2. Belirli, Açık ve Meşru Amaçlar İçin Toplanma

Kişisel verilerin işlenme sürecinin tamamında belirli, açık ve meşru amaçlar doğrultusunda hareket edilmelidir. Bir başka anlatımla, verilerin hem toplanma, hem de daha sonraki bütün işlenmelerinde bu ilkeye uyulmalıdır. Bütün temel veri koruma düzenlemelerinde kabul edilen bu ilkenin üç parçadan oluştuğu görülmektedir:

- Verilerin toplanma amacının belirli ve açık olması;
- Verilerin toplanma amacının meşru olması;
- Verilerin daha sonra işlenme amaçlarının, toplanma amacı ile uyumlu olması.

Verilerin toplanma amacının belirli ve açık olması, her şeyden önce bu konuya ilişkin hukuksal düzenlemelerde belirsiz ifadelerden kaçınılmasını gerektirir. Ayrıca verilerin anonimleştirilmeden yalnızca depolanmak üzere, bir başka anlatımla olası kullanımdan hareketle tutulması da bu ilkeye aykırılık oluşturur.

Verilerin toplanmasının meşru olabilmesi için yasal bir temele dayanması, bütün yasal gereklilikler ile uyum içinde olması ve verilerin işlenmesinden kaynaklanan çıkar ile dengeli olması gerekir.

AB Veri Koruma Yönergesi'nde veri işlemeyi meşru kılan ölçütler belirlenmiştir[15]. Bu ölçütler,

- İlgili kişinin rızasının bulunması[16];
- İlgili kişinin taraf olduğu bir sözleşmenin ifa edilmesi ya da ilgili kişinin bir sözleşmenin tarafı olmadan önceki istemleri dolayısıyla işlemenin gerekli olması[17]: Bir servis sağlayıcının sunduğu hizmeti yerine getirebilmesi için veri öznesinin ad, telefon numarası, e-posta adresi gibi bilgilerini sağlaması burada örnek olarak gösterilebilir;
- Denetçinin tabi olduğu yasal bir yükümlülüğe uymak için işlemenin gerekli olması[18]: Bu hükümde söz konusu olan yalnızca vergi,

[15] AB Yönergesi, m.7.
[16] AB Yönergesi m. 7/a.
[17] AB Yönergesi m. 7/b.
[18] AB Yönergesi m. 7/c.

- Sosyal sigorta ya da mahkemeye delil sunma gibi yasal yükümlülüklerdir. Bu nedenle sözleşmeden kaynaklı yükümlülüklerin bu kapsamda değerlendirilmemesi gerekecektir.
- İlgili kişinin yaşamsal çıkarlarının korunması için işlemenin gerekli olması[19]: Bu istisna ancak ilgili kişinin yaşamı için elzem bir çıkarının korunması söz konusu ise uygulanabilir[20].
- İşlemenin kamu yararının bulunduğu bir hizmetin gerçekleştirilmesi ya da denetçinin veya verinin açıklandığı üçüncü kişinin resmi bir yetkisini kullanması için gerekli olması[21]: Burada geçen "kamu yararı" deyimi geniş yorumlamayı olanaklı kılan niteliği dolayısıyla istisnanın sınırlarının belirsizleşmesine neden olabilmektedir.
- Yönerge'nin 1/1 hükmü uyarınca ilgili kişinin temel hak ve özgürlüklerinden kaynaklı çıkarlarının baskın olduğu durumlar hariç, denetçi veya verinin açıklandığı üçüncü kişinin meşru çıkarlarından kaynaklanan amaçlar için gerekli olması[22]: Bu hüküm ile ilgili kişinin çıkarları ile veri denetçisinin çıkarları arasında bir denge öngörüldüğü söylenebilir. AB Yönergesi'nde "meşru çıkar" ın ne olduğu tanımlanmamıştır. Ancak Yönerge'nin Başlangıç bölümünde "şirketlerin ve diğer organların meşru olağan etkinlikleri" ifadesi yer almaktadır[23]. Bu bağlamda "meşru çıkarlar"ın "meşru ticari çıkarlar" olarak algılanması olanaklıdır.

2.1.3. Verilerin Daha Sonra İşlenme Amaçlarının Toplanma Amacı İle Uyumlu Olması

Kişisel verilerin korunmasına yönelik AB Yönergesi bu noktada bir istisna tanımıştır. İlgili hüküm uyarınca "üye devletlerin uygun önlemleri alması koşuluyla, tarihsel, istatistiksel ve bilimsel amaçlarla sonradan işlemelerin uygunsuz olduğu düşünülmeyecektir"[24]. Bu varsayım ile Yönerge'yi hazırlayanların, tarihsel, bilimsel ve istatistiksel amaçlarla yapılan araştırmalar ile belirtilen ilke arasında yaşanabilecek çatışmaya bir ölçüde de olsa çözüm bulmayı amaçladıkları söylenebilir. Ancak

[19]AB Yönergesi m. 7/d.
[20]AB Yönergesi, baş. par. 31.
[21]AB Yönergesi m. 7/e.
[22]AB Yönergesi m. 7/f.
[23]AB Yönergesi baş. 30.
[24]AB Veri Koruma Yönergesi, m. 1/b, 2. cümle.

burada üye devletlerin uygun önlemleri almasının bir zorunluluk olduğunu belirtmek gerekir.

2.1.4. Toplanma ve Sonrasında İşlenme Amaçlarına Uygun, İlgili Bulunma, Aşırı Olmama

095/46/AT sayılı Yönerge'nin 6/1,c hükmü uyarınca kişisel veriler, "toplanma ve/veya bunu izleyen işleme amaçları açısından yeterli ve onlarla ilgili olacak veaşırı olmayacaktır". 108 sayılı AK Sözleşmesi'nde ise bu ilkenin, AB Yönergesi ile hemen hemen aynı ifadelerle yer aldığı görülür. Ancak her iki hüküm arasında dikkat çekilmesi gereken bir farklılık da bulunur. Sözleşme'nin 5/c hükmüne göre otomatik yollarla işlenen kişisel veriler "saklanma amacı için yeterli, onunla ilgili olacak ve aşırı olmayacaktır". 108 sayılı AK Sözleşmesi'nde ise yalnızca otomatik işlenen verilerin korunmasına hasredilmiştir. Buradaki farklılık AB Yönergesi'nde ölçüt, "toplama ve/veya daha sonra işleme amaçları" ile bağlantısı açısından geliştirilirken, AK Sözleşmesi'nde "saklanma amacı" dikkate alınarak belirlenmesidir.

Burada anonimleştirme konusun kısaca açıklık getirmekte fayda vardır. Tam anlamıyla anonim olan verilerin gerçek kişilerle ilişkisi koptuğu, yani belirlenebilir bir birey ile arasında bir bağ kurmak olanaklı bulunmadığı için bunlar, kişisel veri olarak değerlendirilemezler. Dolayısıyla anonim veriler, kişisel verilerin korunması mevzuatının dışında yer alır. Buna karşın, takma adların birey ile bağlantısı bulunduğu için bunlar, halen veri koruma hukukunun konusu olmayı sürdürür.

2.1.5. Doğru Ve Eğer Gerekli İse Güncel Olarak Tutulma

AB Yönergesi'nin 6/1,d, Avrupa Konseyi Sözleşmesi'nin 5/d maddesinde bu ilke hüküm altına alınmıştır. Her iki metinde de kişisel verilerin "doğru ve gereken durumlarda güncel olması" gerektiğinden söz edilmektedir. Ancak kişisel verilerin korunmasına ilişkin her metinde ilkenin bu şekilde ifade edilmediği de belirtilmelidir. OECD Rehber İlkeleri'nin 8 inci maddesinde "doğruluk" ve "güncellik"in yanında, kişisel verilerin "tamlığı"na da (completeness) da bir zorunluluk olarak yer verilmiştir. Bu noktada AB Yönergesi'nin 6/1,d hükmünün alınmasında fayda vardır. Burada kişisel verilerin, "doğru ve eğer gerekli ise güncel olarak tutulması" zorunluluğunun hemen ardından ikinci bir gereklilik daha belirlenmiştir: buna göre üye devletlerde

“toplanma amaçları veya sonradan işleme için yanlış veya eksik verinin silinmesi veya düzeltilmesi için makul olan bütün adımlar atılacaktır”[25].

2.1.6. Amacı Gerektirdiğinde Daha Uzun Süre Tutulmama

Kişisel verilerin gerektiğinden uzun süre tutulmaması gerekir. AB Veri Koruma Yönergesi’nin 6/1,e hükmü uyarınca, ilgili kişinin teşhis edilmesine olanak tanıyacak şekilde, kişisel verilerin toplandığı veya daha sonra işlendiği amaçlar için gerekli olandan daha uzun süre tutulmaması gerekir. Kişisel verilerin amaç açısından gereksiz duruma gelmesi birkaç olasılıkta söz konusu olabilir:

- Kişisel verilerin işlenmesi ile hedeflenen amaç ortadan kalkabilir,
- Amaca ulaşmak için kişisel verinin işlenmesinin gereksiz olduğu anlaşılabilir,
- Amaca ulaşıldığı için artık kişisel verinin tutulması gerekliliği ortadan kalkabilir.

Avrupa sisteminde, kişisel verilerin korunması bağlamında, verilere artık gereksinim duyulmadığı noktada iki yoldan biri tercih edilmek durumundadır: kişisel veriler,

- Ortadan kaldırılmaktadır,
- Anonimleştirilerek saklanmaktadır.

Bunun yanında AB Yönergesi, üye devletlerin uygun güvenceleri sağlamaları kaydıyla bilimsel, tarihi ve istatistikî amaçlarla verilerin daha uzun süre saklanmasını da olanaklı kılmıştır[26].

2.2. İLGİLİ KİŞİ KATILIMI VE DENETİMİNE YÖNELİK İLKELER

Kişisel verilerin korunması hukuku kapsamında, ilgili kişiye, sürece çeşitli aşamalarda müdahale etme olanağı tanıyan bazı haklar verilmiştir. Kişisel verilere erişim hakkı, verilerin düzeltilmesini isteme hakkı ve bazı durumlarda veri işlemeye itiraz hakkı bu kapsamda sayılabilir.

OECD Rehber İlkelerinin 13 üncü paragrafında bireyin katılımına yönelik ilkeler topluca düzenlenmiştir. Ancak genel olarak bakıldığında diğer metinlerde ilgili kişinin katılımı ve denetimine yönelik ilkelerin tek bir başlık altında toplanmadığı, çeşitli hükümlerin içine serpiştirildiği görülmektedir.

[25] AB Yönergesi m. 6/1,d.
[26] AB Yönergesi, m. 6/1,e.

Kişinin verilerinin işlenmesi hakkında bilgilendirilmesi özellikle iki açıdan önemlidir. Birincisi, kişinin haklarını gerçek anlamda kullanabilmesi için kişisel verilerinin işlenmesi hakkında bilgi sahibi olması gerekir. İkincisi ise bu ilke özellikle kamusal organların ellerinde tuttukları kişisel veriler düşünüldüğünde idarenin şeffaflığının da önemli bir gereğidir. Veri denetçisinin ilgili kişiyi bilgilendirme yükümlülüğü AB Yönergesi'nin 10 ve 11 inci maddelerinde düzenlenmiştir. Diğer uluslararası metinlerde ise bu ilkenin AB Yönergesi'ndeki gibi açık ve kapsamlı bir şekilde düzenlenmediği görülmektedir.AK Sözleşmesi'nin 8 inci maddesinde, OECD Rehber İlkeleri'nin 12 nci paragrafında, BM Rehber İlkeleri içerisinde 3 üncü ilkede dolaylı olarak ilgili kişinin bilgilendirilmesine değinildiği söylenebilir. Ulusal düzenlemelerin bir bölümünde ise verilerin doğrudan ilgili kişiden elde edildiği durumlarda AB Yönergesi'nin 10 uncu maddesine benzer yükümlülüklerin getirildiği görülmektedir.

Kişisel verilerin ilgili kişiden alınmadığı, başka kaynaklardan elde edildiği durumlarda da ilgili kişinin bu kapsamda bilgilendirilmesi, eğer ilgili kişiden elde edilen bilgiler üçüncü kişiyle paylaşılmışsa bu konuda da haberdar edilmesi gerekir. Ancak bu kurala karşın, eğer bu bilgilerin sağlanması olanaksız ise, oransız bir çaba gerektiriyor ise ya da işlem açıkça yasadan kaynaklanıyorsa bu bilgilerin sağlanması gerekmeyecektir[27]

Pek çok metinde ilgili kişinin başka kişi ve kurumların elinde bulunan kişisel verilere ulaşma hakkı kabul edilmiştir. Ancak özellikle AB Yönergesi'ndeki düzenleme dikkat çekicidir. Nitekim benzer hükümler, AK Sözleşmesi[28], OECD Rehber İlkeleri[29] ve BM Rehber İlkeleri'nde [30] bulunsa da Yönerge'deki düzenleme daha geniş kapsamlıdır. AİHM de kişinin bilgilerine erişim hakkını Sözleşme'nin 8 inci maddesinin güvence alanı kapsamında görmektedir.

Belirtilen hükümde kişiye yalnızca kendisine ilişkin verilere ulaşma hakkı tanınmamış, bunun yanında verilerin nasıl kullanıldığı, işleme amaçları, verinin kaynağı ve alıcıları gibi başka bilgilerin alınmasına da olanak verilmiştir[31].

---

[27]Bkz. AB Yönergesi, m. 11;

[28]AK Sözleşmesi m. 8.

[29]OECD Rehber İlkeleri par. 13-14.

[30]BM Rehber İlkeleri 4. İlke.

[31]AB Yönergesi'nin 12. maddesi şu hükmü içermektedir:

"Üye devletler her ilgili kişinin veri denetçisinden şunları edinmesini sağlar:

(a) makul aralıkları sınırlama ve aşırı gecikme ve masraf olmaksızın:

- kendisine ilişkin verilerin işlenip işlenmediğinin teyidi ve an azından işlemenin amacını (belirten)

95/46/AT sayılı Yönerge'nin 12/b hükmü uyarınca ilgili kişinin Yönerge'nin hükümlerine uygun olmayan, özellikle de eksik ve yanlış olan verileri düzeltme hakkı bulunmaktadır. İlgili kişinin verilerinin düzeltilmesini, silinmesini veya engellenmesini sağlama hakkı, bilgilere erişim hakkının bir uzantısıdır.

2.3. İLGİLİNİN DİĞER HAKLARI

Örneğin AB Yönergesi'nde ilgili kişiye belirli durumlarda veri işlemeye itiraz hakkı[32] ve otomatik bireysel kararların konusu olmama hakkı[33] tanınmıştır.

2.4. İLGİLİNİN RIZASI

Bu bağlamda "rıza" ilgili kişinin kendisiyle ilgili veriler üzerinde denetimini sağlamasının önemli bir aracı ve "bilgilerin geleceğini belirleme" düşüncesinin bir yansımasıdır. Diğer taraftan, kişisel verilerin korunmasına ilişkin düzenlemelerden bir bölümünde bireyin rıza vermesi koşulu yer almadığı gibi, AB Yönergesi gibi başka metinlerde verilerin işlenmesinin tek meşru koşulu olarak değerlendirilmemiş, yalnızca veri işlemeyi meşru kılan durumlar içerisinde sayılmıştır.

AB Yönergesi'nde rıza, kişinin kendisiyle ilgili verilerin işlenmesini kabul ettiğini gösteren, belirli ve aydınlatılmış özgür iradesinin her türlü işareti [34] olarak tanımlanmıştır. Hassas kişisel verilerin söz konusu olduğu durumlarda ise ayrıca rızanın "açık" olması da gerekmektedir.

2.5. ÖZEL KATEGORİDEKİ (HASSAS) KİŞİSEL VERİLERİN NİTELİKLİ KORUNMASI

Bu ilke, ilgili kişi açısından "hassas" sayılan bazı veri türlerinin işlenmesini diğerlerine göre daha sıkı bir denetim altına alma düşüncesine dayanır. AB

---

bilgi, ilgili veri kategorileri ve verinin açıklandığı alıcılar ya da alıcı kategorileri;
- işlenmekte olan verinin kaynağına ilişkin her türlü bilginin anlaşılır bir şekilde iletilmesi;
- en azından m. 15/1'de düzenlenen otomatikleştirilmiş kararlar durumunda, kendisine ilişkin verinin her tür otomatik işlenmesinin temelini içeren bilgi;
(b) özellikle verinin yapısının eksik veya yanlış olmasından dolayı, işlenmesi bu Yönerge'nin hükümlerine göre uygun olmayan verinin düzeltilmesi, silinmesi veya engellenmesine uygun olarak;
(c) olanaksız olduğunun kanıtlanması veya oransız bir çaba gerektirmesi durumları hariç olmak üzere, (b) fıkrasına uygun olarak her tür düzeltme, silme veya engellemenin verinin açıklandığı üçüncü kişilere bildirilmesi".

[32] AB Yönergesi m. 14.
[33] AB Yönergesi m. 15.
[34] AB Yönergesi m.2/h.

Yönergesi[35], AK Sözleşmesi[36], BM Rehber İlkeleri[37] hassas verilere özel koruma öngörmüştür.

AB Yönergesi'nin 8 inci maddesine göre özel kategorideki kişisel verilerini işlenmesi kural olarak yasaktır. Bunlar ilgili kişinin,

- Irksal veya etnik kökenini,
- Siyasal görüşünü,
- Dinsel ya da felsefi inancını,
- Sendika üyeliğini,
- Sağlık ya da cinsel yaşamını[38]

belirli eden verilerdir.

Bunun yanında kişilerin ceza mahkumiyetine ilişkin veriler de her durumda korumadan yararlanırken, idari ve adli mahkumiyetlere ilişkin verilerin bu kapsamda sayılıp sayılmayacağı üye devletin takdirine bırakılmıştır[39]

Ulusal hukuk sistemleri açısından düşündüğümüzde bu noktada elbette önemli olan veri koruma otoritesinin ve nihai olarak da mahkemenin yorumudur. Hassas kişisel verilerin bazı ek güvencelerle korunmasındaki temel mantık, bu türdeki verilerin, ayrımcılık başta olmak üzere, diğer verilere göre ilgili kişi açısından daha ciddi zararlar ortaya çıkarabilmesidir.

Bazı veri kategorilerinin özel olarak korunması gerekliliğini kabul ettiğimizde başka bazı soruların da yanıtlanması gerekecektir. Birincisi AB Veri Koruma Yönergesi'nde ve bu ayrımı benimseyen diğer metinlerde hassas kişisel veriler, sınırlı sayım esasına göre belirlenmiştir. Yönerge'nin 8/2 hükmü hassas kişisel verilerin işlenebileceği durumları belirlemiştir. Buna göre bu türdeki verilerin işlenmesine izin verilebilecek özel koşullar şöyledir:

- İlgili kişinin açık rızası bulunuyorsa[40],
- Veri işleme, veri koruma görevlisinin iş hukukundan kaynaklanan özel hak ve yükümlülüklerini yerine getirmesi için zorunluysa[41],

[35]AB Yönergesi m. 8.
[36]AK Sözleşmesi m. 6.
[37]BM Rehber İlkeleri 5. İlke.
[38] İlk beş kategori 8. maddenin 1. fıkrasında hüküm altına alınmış ve bunların işlenmesinin kural olarak yasak olduğu belirlenmiştir. Bu kuralın istisnaları ise Yönerge'nin 8/2 hükmünde yer alır.
[39]Yönergenin 8/5 inci maddesi.
[40]AB Yönergesi 8/2,a maddesi.
[41]AB Yönergesi 8/2, b maddesi.

- Veri öznesinin ya da diğer bir kişinin yaşamsal çıkarlarının korunması için gerekliyse[42],
- İşlemenin ilgili kişi tarafından kamuya açıklanan verilere ilişkin ya da hakların kurulması, kullanılması ve korunması için gerekli olması[43],
- Kar amacı gütmeyen bir kurum tarafından yasal etkinliklerini yerine getirebilmesi için işlemenin gerekli olması[44],
- Veri işlemenin önleyici hekimlik, tıbbi teşhis, tıbbi yardım veya bakım veya sağlık hizmetlerinin idari olarak yürütülmesi için gerekli olması ve bu verilerin ya sağlık personeli veya sağlık personeli gibi sır saklama yükümlülüğüne tabi kişiler tarafından işlenmesi[45]

2.6. VERİ GÜVENLİĞİ

Veri güvenliği ilkesi kişisel verilerin korunması hukukunun ayrılmaz bir parçasıdır. Bu ilke veri denetçilerinin kişisel verilerin kazara ortadan kaldırılmasını, bunlara yetkisiz erişimi, değiştirilmelerini, silinmelerini ve yayınlanmalarını engelleyecek önlemleri almalarını gerektirir.

Kişisel verilerin korunması ile veri güvenliği eş anlamlı değildir. İlkinde amaç, bireylerin korunması iken, ikincisinde verilerin korunması hedeflenmektedir. Ancak bunlar kişisel nitelikte olduğunda veri güvenliği kişisel verilerin korunmasının bir aracı haline gelmektedir. Verilere yetkisiz erişim ve bunların yetkisiz kullanımının önüne geçilmesinde kurum ve kuruluşların da çıkarı bulunur.

Veri güvenliği ilkesi konuya ilişkin metinlerin tamamında yer alır. 108 sayılı AK Sözleşmesinin 7 nci maddesi uyarınca "Yetkisiz erişim, değiştirme veya yayımlamayanında kazara veya yetkisiz tahribe karşı otomatik veri dosyalarında yer alan kişisel verilerin korunması için uygun güvenlik önlemleri alınacaktır". Hükümde yer alan "uygun güvenlik önlemleri" ifadesini, somut olaydaki verinin tutulma amacı, taşıdığı riskin şiddeti gibi konuları dikkate alarak yorumlamak gerekir. BM Rehber İlkelerinde ise: "Hem kazara kayıp veya tahrip gibi doğal tehlikelere karşı, hem de yetkisiz erişim, verilerin dolandırıcılık amacıyla kötüye kullanımı gibi insan kaynaklı

[42] AB Yönergesi 8/2,c maddesi.
[43] AB Yönergesi 8/2,e maddesi.
[44] AB Yönergesi, 8/2, d maddesi.
[45] AB Yönergesi 8/3 maddesi.

tehlikelere ya da bilgisayar virüslerinin bulaşmasına karşı dosyaları koruyacak uygun önlemler alınmalıdır" ifadesi yer alır[46]

OECD Rehber İlkelerinde: "Kayıp veya yetkisiz erişim, tahrip, kullanım, değiştirilme ya da yayımlamaya karşı" kişisel verilerin "makul güvencelerle" korunması gerektiğine işaret edilmiştir[47].

AB Veri Koruma Yönergesi'nde ise şu düzenleme yer alır: "Üye Devletler Denetçinin,

- Kişisel verilerin kazara veya hukuka aykırı tahribine veya kazara kaybolmasına,
- Değiştirilmesine,
- Yetkisiz yayımı veya erişimine,

özellikle işlemin bir şebeke ağı üzerinden nakli yoluyla yapılması durumunda ve hukuka aykırı diğer hukuka aykırı işleme biçimlerinden korunması için gerekli teknik ve örgütsel önlemleri almasını sağlayacaklardır"[48].

Bu önlemlerin hem ilgili sistem kurulurken, hem de daha sonra verileri işlenirken alınmalıdır[49]. Bu sırada teknik olanaklar ve uygulama masrafları göz önünde tutularak işlemeden kaynaklı riske ve korunan verinin niteliğine uygun düzeyde güvenlik sağlanmalıdır[50]. Bunun yanında belirtilen hükümlere uygun olarak alınan önlemlerin belgelendirilmesi de gerekir[51].

Veri güvenliğine yönelik yukarıda işaret edilen önlemler, birkaç açıdan değerlendirilebilir. Öncelikle konu, tehdidin kaynağı açısından irdelenmelidir. BM Rehber İlkelerinin ilgili hükmünde de açıkça belirtildiği gibi tehlike kazara oluşabileceği gibi, bir ya da daha fazla kişiden de kaynaklanabilir. Her iki durumda da teknik önlemler alınmalıdır. Veriler, kazara kaybolmalarına ya da değiştirilmelerine karşı yedeklenmeli, bilgisayar virüslerinden korunmayı sağlayacak bir sistem kurulmalıdır. İnsan kaynaklı tehlikelere karşı da dışarıdan gelebilecek müdahalelerin önlenmesi için bilgisayar sistemlerine güvenlik duvarları kurulması yararlı olacaktır.

Bunun yanında, böylesine bir müdahalenin verileri işleyenlerden kaynaklanabileceği de göz ardı edilmemelidir. Verileri işleyenlerin olanaklı olan en az

[46]BM Rehber İlkeleri, par. 7 maddesi.
[47]OECD Rehber İlkeleri, par. 11.
[48]AB Veri Koruma Yönergesi,17/1 maddesi.
[49]AB Veri Koruma Yönergesi, baş. Par. 46.
[50]AB Veri Koruma Yönergesi, 17/1 maddesi., 2. cümle; baş. par. 46.
[51]AB Veri Koruma Yönergesi, 17/4 maddesi.

miktarda veriye ulaşmasının sağlanması ve bu kişilerin etkinliklerinin uygun araçlarla denetimi olumlu sonuçlar sağlayabilir.

2.7. İSTİSNALAR VE SINIRLAMALAR

Kişisel verilerin korunması hakkı, sınırsız bir hak alanı değildir. Yukarıda incelenen temel ilkelere belirli durumlarda istisna getirilmesi olanaklıdır. Bu, her şeyden önce buradaki temel hakkın göreceli yapısından kaynaklanır. Kişisel verilerin korunmasına temel oluşturan hakkın, diğer hak ve özgürlüklerle ayrıca bireysel ya da kolektif olarak başkalarının hak ve özgürlükleriyle dengeli olması gerekir. Nitekim kişisel verilerin korunmasına hâkim olan temel ilkelere yönelik sınırlama ve istisnalar konuya ilişkin bütün belgelerde yer alır.

AB sistemi açısından baktığımızda özellikle 95/46/AT sayılı Yönerge'yi dikkate almak gerekir. Yönerge'nin 9 ve 13 üncü maddelerinde yukarıda değerlendirilen ilkelerin sınırlandırılmasına ilişkin hükümler yer almaktadır. "Kişisel verilerin işlenmesi ve düşünceyi açıklama özgürlüğü" kenar başlıklı 9 uncu madde uyarınca kişisel verilerin işlenmesi yalnızca gazetecilik amacıyla veya sanatsal ya da edebi açıklamalar için söz konusu olduğunda özel yaşamın gizliliği hakkı ile düşünceyi açıklama özgürlüğüne hakim olan ilkelerin dengelenmesini gerektiren durumlarda sınırlandırılabilir ve istisnalar getirilebilir. AB Yönergesi'nin 13 üncü maddesinde ise "istisnalar ve sınırlamalar" başlığı altında bu konu düzenlenmiştir. Buna göre, bazı durumlarda verinin niteliğine ilişkin ilkelere, ilgili kişinin bilgilendirilme hakkına, erişim hakkına, işleme eyleminin kamuya ilan edilmesine sınırlandırma getirilebilir. Ancak bunun şu konuların korunması için mutlaka zorunlu bulunması gerekir:

a) Ulusal güvenlik;
b) Savunma;
c) Kamu güvenliği;
d) Suçların ya da düzenlenmiş etik kuralların ihlalinin önlenmesi, araştırılması, soruşturulması ve kovuşturulması,
e) Para, bütçe ve vergiyle ilgili konular dahil olmak üzere, Avrupa Birliğinin veya Üye Devletin önemli bir ekonomik veya mali çıkarı,
f) Yukarıda (c), (d) ve (e)'de belirtilen resmi yetkinin kullanılmasıyla bağlantılı olarak izleme, soruşturma veya düzenleme,
g) İlgili kişinin veya diğerlerinin hak ve özgürlüklerinin korunması.

Görüldüğü gibi kamu çıkarının ağır bastığı bazı durumlarda kişisel verilerin korunmasına yönelmiş ilkelere istisna getirilmesi olanaklıdır.

3. VERİLERİN KORUMASININ DENETİMİ İLE İLGİLİ AB KAPSAMINDA YAPILAN DÜZENLEMELERDE YER ALAN MEKANİZMALAR

Verilerin korumasının denetimi ile ilgili AB kapsamında yapılan düzenlemelerde iki çeşit mekanizmanın bulunduğu görülmektedir. Bunlardan ilki Avrupa Veri Koruma Denetçisi; ikincisi ise 29 uncu madde Veri Koruma Grubu'dur. Konuya ilişkin açıklamalara aşağıda yer verilmiştir.

3.1. Avrupa Veri Koruma Denetçisi

Avrupa Veri Koruma Denetçisi (European Data Protection Supervisor-EDPS), AB kurum ve organları tarafından kişisel verilerin işlenmesini denetlemek ile sorumludur. Ancak kurumun etkisi bu temel görevi ile sınırlı değildir. Bu bağımsız organ, AB düzeyinde kişisel verilerin korunması konusunda politikaların geliştirilmesinde oldukça etkilidir. Ayrıca, özellikle ticaret ile ilgili kişisel verilerin korunması sorunlarında görüş bildirdiği görülmektedir. Bunun yanında Avrupa Veri Koruma Denetçisi, AAD önünde veri korumasına ilişkin davalara müdahil olabilmektedir.

3.2. 29 uncu Madde Veri Koruma Grubu

AB bünyesinde verilerin korunmasına ilişkin bir diğer önemli organ, 29.Madde Veri Koruma Grubu'dur. 95/46/AT sayılı Veri Koruma Yönergesi'nin 29 uncu maddesi uyarınca kurulan bu Grup, bağımsız bir danışma organı olarak görev yapmaktadır. Kişisel verilerin korunmasına ilişkin çeşitli konularda görüşlerini belirten ve yorum geliştiren Veri Koruma Grubu, uygulamada oldukça önemli bir görev üstlenmiş bulunmaktadır. Kişisel verilerin korunmasına ilişkin çok çeşitli konularda hazırladığı rapor, görüş ve öneriler hem teoriye, hem uygulamaya ışık tutacak niteliktedir.

AB Temel Haklar Şartı'nın "Kişisel verilerin korunması" kenar başlıklı 8 inci maddesi şöyledir:

"(1) Herkes, kendisini ilgilendiren kişisel verilerin korunması hakkına sahiptir.

(2) Bu veriler, dürüst bir şekilde (fairly), belirli amaçlar için ve ilgili kişinin rızasına veya yasa ile öngörülmüş diğer meşru bir temele dayanılarak işlenir. Herkes kendisi hakkında toplanmış verilere erişme ve bunları düzelttirme hakkına sahiptir.

(3) Bu kurallara uyulması bağımsız bir makam tarafından denetlenir"

4. VERİLERİN KORUNMASI, SAKLANMASI VE PAYLAŞIMI HAKKINDA SUÇ GELİRLERİNİN AKLANMASI VE TERÖRÜN FİNANSMANININ ÖNLENMESİ İLE BAĞLANTILI ULUSLARARASI DÜZENLEMELERDE YER ALAN HUSUSLAR

4.1. Mali Eylem Görev Gücü (FATF) Tavsiyelerinde Yer Alan Hususlar

Verilerin korunmasına, saklanmasına, ulusal ve uluslararası düzeyde paylaşımı hususlarına çeşitli FATF düzenlemelerinde yer verilmiştir.

FATF'ın 11 inci tavsiyesinde belirtildiği üzere finansal kuruluşların,

- Ulusal veya uluslararası işlemlere ilişkin bütün işlemlere dair belgeleri en az 5 yıl süre ile saklamalarının;
- Müşterini Tanı tedbirleri çerçevesinde elde edilen tüm kayıtları; hesap dosyalarını ve iş yazışmalarını, yürütülen herhangi bir analizin sonuçlarını da kapsayacak şekilde iş ilişkisinin sona erdirilmesinden veya arızi işlem tarihinden sonra en az beş yıl süre ile saklamalarının zorunlu tutulması gerektiği.

ifade edilmektedir.

FATF'ın uluslararası işbirliğinde kullanılmasını önerdiği enstrümanlara Tavsiyelerin 36 ncı maddesinde yer verilmiştir. Buna göre ülkeler,

- 1988 tarihli Viyana Konvansiyonuna,
- 2000 tarihli Palermo Konvansiyonuna,
- 2003 tarihli Yolsuzluğa Karşı Birleşmiş Milletler Konvansiyonuna,
- 1999 tarihli Terörün Finansmanı Konvansiyonuna,

taraf olmaya ve tam olarak uygulamak için acil tedbirler almaya çağrılmaktadır.

Mali istihbarat birimlerinin elindeki veriler Mutabakat muhtıraları veya paylaşım esasları önceden belirlenmek kaydıyla güvenli ağ üzerinden paylaşılabilmektedir. Bu bilgiler, kimi zaman da adli istinabeye konu olabilmektedir. Bu bakımdan uluslararası anlaşmalarda yer alan adli istinabeye ilişkin yer alan hükümler mali istihbarat birimleri açısından da önem taşımaktadır.

Uyuşturucu ve Psikotrop Maddelerin Kaçakçılığına Karşı Birleşmiş Milletler Sözleşmesi (Viyana Konvansiyonu)'nin 7 nci maddesinde adli yardımlaşmanın, Sözleşmenin 3 üncü maddesinin birinci fıkrasında belirtilen soruşturulmasında, cezai takibatında ve yargılanmasında karşılıklı olarak adli yardımda bulunacakları

belirtilmektedir. Bahsi geçen adli yardımlaşma talebinin diğer bazı amaçların yanı sıra,

- Bilgi ve kanıt sağlamak;
- Banka kayıtlar, muhasebe belgeleri, şirket dosyaları ve ticari belgeler de dahil olmak üzere ilgili belge ve kayıtların asıllarını veya tasdikli suretlerinin sağlanması,

amaçları ile gerçekleştirilebileceği ifade edilmiştir.

Bilgi talep edilen tarafın ön muvafakate olmadan, talep eden taraf, anılan tarafın verdiği bilgi ve delilleri talepte yer alan soruşturma takibat veya muhakeme amaçları dışında kullanılamayacağı ve başkalarına verilemeyeceği belirtilmiştir.

Talep eden taraf, talep edilen taraftan, talebin ve muhtevasının uygulanması için gerekli olabilecek ölçülerin ötesinde talebin gizli tutulmasını isteyebilir. Talep edilen taraf bu isteği yerine getiremeyecek ise talep eden tarafa durumu hemen bildirecektir.

Sözleşmenin 9 uncu maddesinde, tarafların adli yardımlaşma dışında ikili veya çok taraflı anlaşma ve düzenlemeleri çerçevesinde işbirliği gerçekleştirebileceklerine vurgu yapılmıştır. Bu bağlamda güvenli ve ivedi bilgi değişimi sağlamak amacıyla yetkili kurum ve servisleri arasında iletişim kanalları kurulabileceği belirtilmektedir.

Sınır Aşan Örgütlü Suçlara Karşı Birleşmiş Milletler Sözleşmesinin 18 inci maddesinde belirtildiğine göre, Sözleşmeye taraf devletler, diğer bazı amaçların yanı sıra resmi daire, banka, şirket veya ticaret kayıtlan ve mali kayıtlar dahil, ilgili belge ve kayıtların asıllarını veya onaylı kopyalarını temin etmek amaçlarıyla da adli yardım talebinde bulunabileceklerdir. Bilgiyi alan yetkili makamlar anılan bilginin gizli kalması talebine veya kullanımındaki sınırlamalara geçici bir süre dahi olsa uyacaklardır.

Talepte bulunan taraf devlet, talebe konu soruşturma, kovuşturma veya yargısal işlemler için talepte bulunulan taraf devlet tarafından verilen bilgiyi veya delili, talepte bulunulan taraf devletin önceden rızası olmaksızın, talepte belirtilen amaçlar dışında aktarmayacak veya kullanmayacaktır.

Talepte bulunan taraf devlet, talepte bulunulan taraf devletten, talebin yerine getirilmesi bakımından zorunlu olmadığı ölçüde, yapılan talebin ve içeriğinin gizli tutulmasını isteyebilir. Eğer talepte bulunulan taraf devlet gizlilik gerekliliğine uyamaz ise, talepte bulunan taraf devleti derhal bilgilendirecektir.

Talepte bulunan taraf devlete kendi iç hukukuna göre kamuya açık olan kendi elindeki resmi kayıt, belge veya bilgilerin örneklerini verecektir; kendi takdiriyle,

tamamen, kısmen veya uygun gördüğü koşullara tabi olarak kendi iç hukukuna göre kamuya açık olmayan resmi kayıt, belge veya bilgilerin örneklerini talepte bulunan taraf devlete verebilir.

Birleşmiş Milletler Yolsuzlukla Mücadele Sözleşmesi'nin 14 üncü maddesinde, Sözleşmenin 46 ncı maddesindeki hükümler saklı kalmak kaydıyla, (iç hukukunca uygun olan hallerde, adlî makamlar da dâhil karapara aklamayla mücadeleye hasredilmiş idarî makamlar, düzenleyici makamlar, kolluk makamları ve diğer makamların, iç hukukunda öngörülen koşullar dâhilinde, ulusal ve uluslararası düzeyde işbirliği yapma ve bilgi değişiminde bulunma olanağına sahip olmalarını sağlayacak ve bu amaçla, muhtemel karapara aklamaya ilişkin bilginin toplanması, analizi ve dağıtılması için ulusal bir merkez olarak hizmet verecek bir malî istihbarat biriminin kurulmasını değerlendirecektir.

Sözleşme'nin 37 nci maddesinde, Sözleşme ile ihdas edilmiş olan bir suçun işlenmesine iştirak eden veya etmiş olan kişilerin, yetkili makamlara, soruşturmaya ve delil elde etmeye yönelik faydalı bilgi sunmasını ve suçluları suç gelirlerinden mahrum kılmaya ve bu gelirlerin geri alınmasına katkı sağlayacak somut yardımlarda bulunmasını teşvik etmek üzere uygun önlemleri alacaktır.

Sözleşmesi'nin 38 inci maddesinde, Sözleşmeye taraf devletlerin diğer hususların yanı sıra, talep olduğu takdirde, bu makamlara gerekli bütün bilgileri sağlamaları konusunda da gerekli tedbirleri almaları gerektiği ifade edilmiştir.

Sözleşmesi'nin 46 ncı maddesinde, Sözleşmeye taraf devletlerin adli yardım kapsamında Resmî daire, banka, şirket veya ticaret kayıtları ve malî kayıtlar dâhil, ilgili belge ve kayıtların asıllarını veya onaylı suretlerini temin etmeleri gerektiği. Bilgiyi alan yetkili makamlar anılan bilginin gizli kalması talebine veya kullanımındaki sınırlamalara, geçici bir süre dahi olsa uyacaklardır. Talepte bulunan taraf devlet, talebe konu soruşturma, kovuşturma veya yargılamalar için talepte bulunulan taraf devlet tarafından sağlanan bilgiyi veya delili, talepte bulunulan taraf devletin önceden rızası olmaksızın, talepte belirtilen amaçlar dışında iletmeyecek veya kullanmayacaktır.

Talepte bulunan taraf devlet, talepte bulunulan taraf devletten, talebin yerine getirilmesi bakımından zorunlu olmadığı ölçüde, yapılan talebin ve içeriğinin gizli tutulmasını isteyebilir. Eğer talepte bulunulan taraf devlet gizlilik zorunluluğuna uyamaz ise, talepte bulunan taraf devleti derhal bilgilendirecektir.

Talepte bulunulan taraf devlet;

a) Talepte bulunan taraf devlete, iç hukukuna göre kamuya açık olan elindeki resmî kayıtların, belgelerin veya bilginin örneklerini verecektir.

b) Kendi takdiriyle, tamamen, kısmen veya uygun gördüğü koşullara tâbi olarak, iç hukukuna göre kamuya açık olmayan resmî kayıt, belge ve bilgilerin örneklerini talepte bulunan taraf devlete verebilir.

Terörizmin Finansmanının Önlenmesine Dair Uluslar arası Sözleşmenin 12 nci maddesine göre taraf devletler, ellerinde bulunan ve yargılama amacıyla gerekli kanıt unsurlarının temini için yardım da dahil olmak üzere, 2 nci maddede belirtilen suçlarla ilgili cezai soruşturmalarda ya da ceza davalarında veya iade işlemlerinde, mümkün olan en geniş şekilde adli yardımlaşmada bulunurlar.

Talep eden taraf, talep edilen devlet tarafından sağlanan bilgi ve verileri, onun ön onayı olmaksızın, talebe konu olanlar haricindeki soruşturma, kovuşturma ya da davalarda kullanamaz.

Taraf devletler, kendilerine 1 ve 2 nci paragraflar çerçevesinde düşen yükümlülükleri, aralarında mevcut bulunan adli yardımlaşma ve bilgi teatisi anlaşmaları ve düzenlemeleri çerçevesinde yerine getirirler. Bu tür anlaşmalar veya düzenlemelerin yokluğunda, taraf devletler, söz konusu adli yardımlaşmayı ulusal mevzuatlarına uygun olarak gerçekleştirirler.

Terörizmin Finansmanının Önlenmesine Dair Uluslararası Sözleşmenin 18 inci maddesinde taraf devletler,

Taraf Devletler, topraklarının dahilinde veya haricinde işlenecek suçların kendi topraklarında gerçekleştirilen hazırlıklarının önlenmesi amacıyla gerektiğinde iç hukuklarında lazım gelen düzenlemeleri yapmak da dahil olmak üzere 2 nci maddede belirtilen suçların önlenmesi amacıyla mümkün olan her türlü tedbiri almak suretiyle işbirliği yaparlar. Bu meyanda, diğer tedbirlerin yanı sıra, finansal kurumlar ve finans işleri yapan diğer kuruluşları, devamlı veya arızi müşterilerinin veya lehlerine hesap açılan kişilerin teşhisi için mevcut en etkili yöntemleri kullanmaya, olağandışı veya şüpheli işlemlere özel bir dikkat göstermeye ve suç teşkil eden bir eylemden kaynaklandığından şüphelenilen işlemleri haber vermeye mecbur eden önlemler. Bu amaçla taraf devletler, aşağıdaki tedbirleri öngörmelidirler.

- Malî kurumların ulusal veya uluslararası işlemlere ilişkin tüm gerekli belgeleri asgari beş yıl saklamalarını talep etmek,
- 2 nci maddede belirtilen suçlara ilişkin olarak, aşağıda belirtilen hususlarda soruşturma yapılmasında birbirleriyle işbirliğinde bulunmak,

- Bu tür suçlara katıldığına dair haklarında makul şüpheler bulunan kişilerin kimliği, yeri ve faaliyetleri,

Sözleşmenin 27 nci maddesinde belirtildiği üzere, Sözleşmeye taraf devletlerin yetkili makamları, kurumları ve kuruluşları arasında Sözleşmede belirtilen suçların bütün yönlerine ilişkin güvenli ve hızlı bilgi alışverişini kolaylaştırmaya yönelik uygun görülebilecek iletişim kanalları kurmak ve bunları geliştirmek için gerekli tedbirleri alacaklardır.

37 nci FATF tavsiyesinde belirtildiği üzere ülkeler, karapara aklama, buna bağlı öncül suçlar ve terörün finansmanıyla ilgili soruşturma, kovuşturma ve ilgili yargı süreçlerinde karşılıklı adli yardımlaşmada bulunmalıdırlar. Ülkeler, kendilerine gelen adli yardımlaşma taleplerinin ve bunların içerdiği bilgilerin gizliliğini sağlamalıdır. Talep edilen ülke gizlilik yükümlülüğünü karşılayamıyorsa bunu talep eden ülkeye derhal bildirmelidir.

Başvurulabilecek diğer işbirliği şekillerine 40 ıncı FATF Tavsiyesinde yer verilmiştir. Buna göre ülkelerin yetkili makamlarının ihtiyaç duyması halinde, ikili yada çok taraflı anlaşma ya da bir mutabakat muhtırası düzenlemek sureti ile; bu düzenlemelerin hükümleri çerçevesinde işbirliği yapmalıdırlar. Yetkili makamlar, en azından, değişime konu bilgileri yurtiçi kaynaklardan alınan benzer bilgilerle aynı şekilde korumalıdır. Talebi yapan yetkili makamın bilgiyi etkin bir şekilde koruyamaması halinde, yetkili makamlar bilgi vermeyi reddedebilmelidir.

Mali istihbarat birimleri yabancı muadillerine, talep üzerine ve mümkün olduğu zaman, verilen bilginin kullanımı ve verilen bilgiler temelinde yapılan analiz sonuçları hakkında geribildirim yapmalıdır.

Mali istihbarat birimleri aşağıda belirtilen bilgilerin değişimi için yetki sahibi olmalıdır:

- Bilhassa 29. Tavsiye uyarınca mali istihbarat birimi tarafından doğrudan veya dolaylı olarak erişilebilir ya da elde edilebilir olması gereken bütün bilgiler,
- Karşılıklılık ilkesine tabi olarak, mali istihbarat birimlerinin yurt içinde doğrudan veya dolaylı olarak elde etme ve erişme yetkisine sahip oldukları diğer her türlü bilgi.

Değişime konu bilgi yalnızca isteme veya verilme amacına uygun olarak kullanılmalıdır. Bilginin diğer yetkililere veya üçüncü kişilere verilmesi veya başlangıçta kabul edildiğinin haricinde herhangi bir idari amaçla, soruşturma,

kovuşturma amacıyla veya adli amaçla kullanılması, talep edilen ülkenin yetkili makamının önceden vereceği izne tabidir.

Yetkili makamlar yapılan soruşturma veya araştırmanın bütünlüğünü her iki tarafın gizlilik ve veri koruma ile ilgili yükümlülüklerine uygun olarak korumak amacıyla her türlü işbirliği ve bilgi değişimi talebinin gizliliğini muhafaza etmelidir. Yetkili makamlar, en azından, değişime konu bilgileri yurtiçi kaynaklardan alınan benzer bilgilerle aynı şekilde muhafaza etmelidir. Ülkeler yetkili makamların değişime konu bilgileri yalnızca yetki verildiği şekilde kullanmasını temin etmek üzere kontrol mekanizmaları ve koruma önlemleri tesis etmelidir. Bilgi değişimi güvenli bir şekilde ve güvenilir kanallar veya mekanizmalar vasıtasıyla yerine getirilmelidir. Talep edilen ülkenin yetkili makamları uygun görürlerse, talebi yapan yetkili makamın bilgiyi etkin bir şekilde koruyamaması halinde, bilgi vermeyi reddedebilir.

Mali istihbarat birimleri bir işbirliği talebi yaparken, analiz edilen olayın açıklanması ve talep edilen ülke ile olan muhtemel bağlantı da dahil olmak üzere, bütün gerçek ve ilgili olabilecek bilgileri vermek için azami ölçüde çaba göstermelidir. Mali istihbarat birimleri yabancı emsallerine, talep üzerine ve mümkün olduğu zaman, verilen bilginin kullanımı ve ayrıca verilen bilgiler temelinde yapılan analiz sonuçları hakkında da geribildirim yapmalıdır.

Mali istihbarat birimleri aşağıda belirtilen bilgilerin değişimi için yetki sahibi olmalıdır:

- FATF Tavsiyeleri, bilhassa 29 uncu Tavsiye hükmünde belirtilen mali istihbarat birimi tarafından doğrudan veya dolaylı olarak erişilmesi ya da elde edilmesi talep edilen bütün bilgiler,
- Karşılıklılık ilkesine tabi ve mali istihbarat birimlerinin yurtiçinde doğrudan veya dolaylı olarak elde etme ve erişme yetkisinin olduğu diğer bütün bilgiler.

Ülkeler kendi yetkili makamlarının yukarıdaki ilgili esasları uygulayarak emsalleri olmayan yetkili makamlarla dolaylı olarak bilgi değişimi yapmalarına izin vermelidir. Dolaylı bilgi değişimi, talep edilen bilginin talebi yapan yetkili makam tarafından alınmadan önce bir veya daha çok yerli ya da yabancı yetkili makam vasıtasıyla talep edilen yetkili makam tarafından gönderilmesini ifade etmektedir. Bu tür bir bilgi değişimi ve bunun kullanımı talep edilen ülkenin bir ya da daha çok yetkili makamının iznine tabi olabilecektir. Talebi yapan yetkili makam daima talebin hangi amaçla ve kimin adına yapıldığını açıklamalıdır.

Ülkeler, emsal olmayan yetkili makamlar ile doğrudan acil ve yapıcı bilgi değişimine izin vermelidir.

4.2. Avrupa Parlamentosu ve Konseyinin 2005/60/EC Sayılı Direktifi (Üçüncü Direktif)

AB Üçüncü Direktifi'nin 33 ncü paragrafında belirtildiğine göre, Direktifin açıklamaya ilişkin yasakları içeren 2 nci Bölümünde yer alan 28'inci maddesinde belirtilen hususların 95/46/EC sayılı Avrupa Parlamentosu Direktifine ve Konseyin 24 Ekim 1995 tarihli Verilerin Serbest Dolaşımına İlişkin Yönergesi'nde belirtilen kişisel verilerin üçüncü ülkelere transferine ilişkin hükümlere uygun olması gerektiği belirtilmiştir.

3 üncü Direktifin 28 inci maddesinin ikinci paragrafında ise, birinci paragrafta belirtilen bildirim yasaklamalarının maddede belirtilen diğer bazı durumların yanı sıra 37 nci maddede belirtilen muadil kurumlara yapılan bildirimleri, öz düzenleyici kurumları, hukuk uygulama amaçlı bildirimleri kapsamadığı ifade edilmektedir.

Üçüncü Direktifin 30 uncu maddesinde, anılan maddede belirtilen kişi ve kuruluşların Müşterinin Tanınması İlkesinin uygulanması kapsamında almış oldukları bilgilere ilişkin belgelerin bir kopyasını, iş ilişkisinin sona ermesinden sonra en az 5 yıl boyunca saklamalarını öngörmektedir. Ayrıca iş ilişkisi ve işlemlerine ilişkin destekleyici kanıt ve kayıtların da işlemin gerçekleştirilmesinden veya iş ilişkisinin sonlandırılmasından itibaren en az 5 yıl boyunca saklanması gerektiği belirtilmektedir.

Üçüncü Direktifin giriş kısmında yer alan 40 ıncı paragrafta Mali İstihbarat Birimleri (FIU)'lar arasında 17 Ekim 2000 tarihli 2000/642/JHA sayılı Konsey Kararında belirtilen işbirliği kanallarından FIU-net'in işlerliğe kavuşturulmasının faydalı olacağı belirtilmektedir.

4.3. Basel Komitesinin Konuya İlişkin Uygulamaları

Basel Komitesi, Eylül 2012 tarihinde Etkin Bankacılık Denetimi Temel Prensipleri konulu belge yayımlamıştır. Bu belgede yer alan 3 numaralı Prensipte, yurtiçi otoritelerle ve yabancı denetçilerle işbirliği ve ortak çalışma alanını sağlayacak hukuki düzenlemelerin yapılmış olması gerektiğinden ve bu düzenlemelerin gizli bilgilerin güvenliğini sağlayıcı nitelikte olması gerektiğinden bahsedilmiştir. Bu hususta sağlanan bilgilerin yalnızca bankacılığa özel ve sistem çapında kullanılması

gerektiği; bilginin edinildiği kaynağın izni olmaksızın üçüncü taraflarla paylaşılmaması (mahkeme kararı ve yasa yapıcı yapıların emir vermesi hariç) gerektiği; denetçinin edindiği bilgiyi açıklamasının yasal olarak emredildiği durumda bilgiyi edindiği kaynağı bu durumdan haberdar etmesi gerektiği; bilginin açıklanması hususunda kaynak denetçi ile fikir birliğinin sağlanamaması halinde, bilgiyi açıklayacak olan denetçinin söz konusu bilgiyi açıklamamak için elinden gelen çabayı göstermesi gerektiği belirtilmektedir.

Konuya ilişkin olarak belirlenmiş 29 uncu Prensipte, bankaların mali istihbarat birimine, diğer belirlenmiş otoritelere ve banka denetçilerine yaptıkları bildirimlerin güvenliğini sağlamış olmaları gerektiği; Müşterini Tanı Prensibi gereğince alınan belgelere; bireysel işlemlere ilişkin bilgi ve belgelerin en az 5 yıl süre ile muhafaza edilmesinin sağlanmış olması gerekmektedir. Bankaların, muhabir bankacılık uygulamaları bağlamında, müşteri temelli olarak işin niteliği hakkında bilgi temin edecek politika ve prosedürlere sahip olup olmadığının tespitinin gerektiği belirtilmektedir.

4.4. Uluslararası Sigorta Denetçileri Birliğinin Konuya İlişkin Uygulamaları

Uluslararası Sigorta Denetçileri Birliğinin kayıt tutma, veri güvenliği ve bilgi paylaşımı hakkında belirlediği esaslara Sigorta Temel Prensipleri, Standartlar, Rehber ve Değerlendirme Metodolojisinde yer verilmiştir.

Sigorta Temel Prensipleri, Standartlar, Rehber ve Değerlendirme Metodolojisi'nde yer alan 2 nci Sigorta Temel Prensibi başlığı altında yapılış açıklamada diğer denetçilerden alınan bilgileri de içerecek şekilde denetçilerin, çalışanların ve adına hareket edenlerin geçmişte ve halihazırda edinmiş oldukları bilgilerin gizliliğini sağlamalarının hukuki alt yapısının oluşturulması gerektiği belirtilmiştir.

3 üncü Sigorta Temel Prensibi başlığı altında yapılış açıklamada ise sigorta denetçisinin gizliliği olan bilgiyi diğer denetçilerle; gizlilik, amaç ve kullanım gereklerini karşılayabilen otoritelerle değişime tabi tutabileceği belirtilmektedir. Bilgi değişimi maksadı ile denetçiler arasında anlaşmalar veya mutabakat muhtıraları imzalanabileceği belirtilmiştir. Diğer denetçilerle bilgi değişimi yapılmak istenmesi durumunda yasal çıkarın ve geçerli amacın bulunması gerektiği belirtilmiştir. Her bir bilgi talebinin ayrı ayrı değerlendirilmesi gerektiği; taleplerin yazılı olarak yapılması

esas olmakla birlikte, olağanüstü durumlarda talebin mutlaka yazılı olarak yapılması gerektiğine dair bir ısrarda da bulunulmaması gerektiği ifade edilmiştir. Acil durumlarda ve kriz anlarında ilgi talebinin karşılanması için katı bir karşılıklılık uygulamasına gidilmemesi gerektiği; gizli bilginin sadece talep edilme amaçları doğrultusunda kullanılması gerektiği; edinilen bilginin başka amaçlar için kullanılmasından önce kaynak denetçinin izninin alınması gerektiği; edinilen bilginin açıklanması zorunluluğunun doğması halinde kaynak denetçinin durumdan haberdar edilmesi,

22 nci Sigorta Temel Prensibi başlığı altında yapılış açıklamada ise denetçinin diğer yetkili otoritelerle işbirliğini, koordinasyonu ve bilgi değişimini yapabilmek için mümkün olan her tedbiri almaları gerektiği vurgulanmaktadır. Gerçekleştirilecek olan bilgi değişiminin 3 üncü Temel Prensipte belirtilen usullere uygun olması gerektiği vurgulanmaktadır.

Uluslararası Sigorta Denetçileri Birliğinin Ekim 2013'te yayımladığı Karapara Aklanması ve Terörün Finansmanı ile Mücadele Uygulama Rehberi'nde sigortacı ve aracıların FATF Tavsiyelerine göre Müşterini Tanı İlkesi kapsamında edindikleri bilgi ve belgeleri iş ilişkisinin sonlandırılma tarihinden veya itibaren en az 5 yıl süre (veya uygun yetkiye dayalı olarak belli bir olay ile ilgili olarak yetkili merci tarafından daha uzun süre) ile saklamaları gerektiği; bu bilgilerin,

- Her bir müşterinin risk profiline veya gerçek faydalanıcıya ilişkin bilgileri,
- Müşterini Tanı İlkesinin uygulanması kapsamında elde edilmiş bilgileri (müşterinin/ gerçek faydalanıcının adı, adresi veya aracı tarafından kaydedilmiş diğer tanımlayıcı bilgiler gibi),
- İşlemin doğasına ve gerçekleştirilme zamanına dair bilgileri,
- İşlemde kullanılan para biriminin/birimlerinin tipini ve miktarını
- İşlem ile ilgili hesaplara ilişkin hesap numarasını ve hesabın tipini
- Resmi kimlik belgelerini,

  İçerebileceğinin belirtildiği; sigortacılar için poliçenin sona ermesini takip eden zaman diliminde en az 5 yıl bilgi ve belgelerin saklanmasının uygun olacağının belirtildiği ifade edilmiştir.

Ayrıca, sigortacıların ve aracıların yurt içi ve yurtdışı işlemlerle ilgili edindikleri bilgi ve belgeleri ilgili işlemin gerçekleştirilmesinden sonra en az 5 yıl süre (veya uygun yetkiye dayalı olarak belli bir olay ile ilgili olarak yetkili merci tarafından daha

uzun süre) muhafaza edilmesinin FATF tarafından istendiği belirtilmiştir. Bu uygulamanın iş ilişkisinin sona erip ermediğine bakılmaksızın gerçekleştirilmesi gerektiği ifade edilmektedir. İşleme ilişkin kayıtların, bireysel olarak işlemin yeniden tesisine yetecek; ceza kovuşturmasına kanıt teşkil edecek düzeyde olması gerektiği belirtilmiştir.

Bu bağlamda sigortacıların ve aracıların,

- Sigortacılar tarafından yapılacak teyidi desteklemek amacıyla, müşterinin finansal değerlendirmesine, müşteri ihtiyaçları analizine, düzenleyici belgelerin kopyalarına, ödeme metotlarının detaylarına, menfaatlerin açıklamalarına, belgelerin kopyalarına,
- Bütün satış sonrası kayıtlara ulaşılabilmesi,
- Kontratın sonlandırılma sürecine ve sonlandırılmış kontratlara ilişkin detaylara ulaşılabilmesi için yeterli prosedüre sahip olmalıdır

4.5. Sermaye Piyasası Kurulları Uluslararası Organizasyonu (OICU-IOSCO)

IOSCO, Metodoloji belgesini 2011 Eylül ayında yayınlayıp 2013 Ağustos ayında revize etmiştir. Söz konusu Metodoloji belgesinde yer alan 5 numaralı prensipte, düzenleyici otoritenin çalışanlarının kişisel verilerin korunmasına, mahremiyet hükümlerine ve gizliliğe riayet etmelerinin gerekliliğine vurgu yapılmaktadır.

Metodolojide yer alan 13 numaralı prensipte, düzenleyicilerin kamuya açık olan ve olmayan bilgileri paylaşabilme kapasitelerinin olup olmadığı sorgulanmaktadır. Gizlilik içeren bilgilerin korunmasına yönelik tedbirlerin alınması gerektiği vurgulanmaktadır.

Uluslararası seviyede bilgi değişimi yapıldığında IOSCO tarafından tasarlanmış MoU çerçevesinde davranılması gerektiği; bu MoU'da yer almayan hususlarda ise bilgi talebinde bulunulan taraf ile uzlaşının aranması gerektiği ifade edilmiştir. Banka sırrı, gizlilik ve yasal engellemelerin olması durumunda, düzenleyicinin bilgi paylaşımını sağlayacak istisnai durumların yaratılıp yaratılamayacağının araştırılması gerektiği belirtilmektedir.

Metodolojide yer alan 14 numaralı prensipte, düzenleyicilerin bilgi paylaşımına yönelik mekanizmalar kurmalarının gerektiği belirtilmektedir. Bu mekanizmaların,

- Hangi otorite ve düzenleyicinin paylaşılan bilgiye ulaşabileceğini,

- Erişimin mevcut hukuk düzenlemelerinde ne şekilde gerçekleştirilebileceğini,
- Uygulanan yasalar çerçevesinde gizliliğin ne şekilde sağlanacağını;
- Uygulanan yasalar çerçevesinde paylaşımın ne şekilde sağlanacağını,
- Yardımın veya bilgi değişiminin şeklini ve zamanını,
- Araştırma ve mali bilgilerin paylaşımı için MoU ve diğer düzenlemelerin otoriteler arasında yapılabilirliği,
- Düzenleyicinin fonksiyonlarını yerine getirmesi esnasında elde ettiği gizli bilgiyi diğer bir otorite ile paylaşması durumunda, bilginin kullanımı, gizliliğinin sağlanması ve açıklanma şartları hakkında uzlaşılmış olması,

Hisse senetlerine ve future'a ilişkin kanunların uygulanmasına hakkında Kayıt Tutma, Bilgi Toplama, Uygulama Yetkileri, Karşılıklı İşbirliği ile ilgili olarak IOSCO Başkanlar Komitesinin Kasım 1997 tarihinde almış olduğu kararda, konuya ilişkin işlemler ile ilgili olarak tutulan kayıtların işlemin yeniden tesisine yetecek düzeyde olması gerektiği; yetkili otoritelerin konuya ilişkin edinecekleri bilgileri zamanında edinebilmeleri için yetkilendirilmiş olmaları gerektiği; diğer IOSCO üyeleri ile gerekli olduğunda bilgi değişimi gerçekleştirebilmek için engellerin kaldırılması konusunda yurtiçi otoritelerle ortak çalışma yapmaları gerektiği belirtilmiştir.

5. VERİLERİN KORUNMASI, SİLİNMESİ VE PAYLAŞIMINA İLİŞKİN TASLAK ÇALIŞMALARI

5.1.Avrupa Parlamentosu ve Konseyinin Mali Sistemin Suç Gelirlerinin Aklanması ve Terörün Finansmanında Kullanılmasının Önlenmesine Dair Direktif Taslağı (Dördüncü Direktif)

Dördüncü AB Direktifi'nin 2015 yılı içerisinde yasalaşması beklenmektedir.

Direktifte belirtildiğine göre, Direktifin 39 uncu maddesi kapsamında Müşterini Tanı İlkesi kapsamında temin edilen verilerin kopyası veya kanıt niteliğindeki referansların iş ilişkisinin sona ermesinin ardından 5 yıl süre ile saklanması gerekmektedir. Yine aynı Direktif maddesine göre söz konusu verinin tutulmasını gerektirecek kanuni dayanağın bulunmadığı durumda bu sürenin sonlanmasının ardından söz konusu verinin silinmesi gerekmektedir. Diğer taraftan, kayıtların maksimum muhafaza süresinin 10 yılı aşmaması gerekmektedir.

Aynı Direktif maddesinin (b) fıkrasına göre, iş ilişkileri ve işlemler bazında, mahkemede kabul edilebilecek orijinal belge ve kopyalarından oluşan destekleyici kanıt ve kayıtların, işlemin gerçekleştirilmesini veya iş ilişkisinin sonlandırılmasını (hangisi daha kısa ise) müteakip 5 yıl saklanmasını şart koşmaktadır.

Veriyi saklayanın hangi şartlarda bu veriyi daha uzun süre tutabileceğine ya da tutması gerektiğine dair hukuki bir dayanak bulunmaması halinde ise kişisel verinin silinmesi gerekmektedir. AB Üyesi devletler, yalnızca karapara aklanmasının önlenmesi; soruşturulması ve incelenmesi maksadı ile verilerin elde tutulmasına olanak sağlamalıdırlar. Veriyi elde tutma süresi, işlemin gerçekleştirilmesinden veya iş ilişkisinin sonlandırılmasından hangisi daha erken bitiyorsa, bu süreden itibaren en fazla 10 yıl olmalıdır.

Direktifin "Ulusal İşbirliği" başlıklı 46 ncı maddesinde belirtildiğine göre, politika yapıcılar, FIU, hukuk uygulama otoriteleri, denetleme mercileri ve diğer muadil otoriteler yurt içinde karapara aklanması ve terörün finansmanı ile mücadele alanlarında etkinliği sağlayacak işbirliği ve koordinasyon mekanizmaları kurmalıdırlar

Direktifin 49 uncu maddesinde FIU'ların, muadil FIU'ların yapılanma şekline bakılmaksızın yakın işbirliği yapması gerektiği ifade edilmektedir.

Direktifin 50 nci maddesinde FIU'ların kendiliğinden veya talebe bağlı bilgi değişimi yapabilecekleri belirtilmektedir. Bu hususta bilgi değişimi yapılması esnasında güvenli dijital araçların da kullanılabileceğinden bahsedilmektedir. Talebin

yapıldığı ülkede yürütülen soruşturmanın zarar görmesi ihtimali olması; bilginin açıklanmasının, gerçek veya tüzel kişilerin ya da üye devletin yasal çıkarlarına zarar vereceği; bilginin toplanma amacı ile uyumlu olmaması durumlarında FIU'nun bilginin açıklanması talebini reddedebileceği belirtilmektedir.

Direktifin 49 ve 50 nci maddeleri kapsamında edinilen bilgilerin FIU'ların bu Direktif kapsamında belirlenmiş görevleri yerine getirme maksatlı olarak kullanılması gerektiği; bilgiyi veren FIU'nun verdiği bilginin kullanımı hususunda kısıtlamalar getirebileceği[52]; bilgiyi veren FIU'nun ön izni alınmaksızın diğer kişi ve kurumlarla bu bilgilerin paylaşılmaması ve alınan bilgilerin güvenli bir şekilde muhafazası için gerekli önlemlerin alınması gerektiği[53] ifade edilmektedir.

Direktifte, üye devletlerin FIU'lar arası iletişimin güvenli iletişim kanallarının kullanılması ve merkezi network ağı özelliği olmayan fiu.net'in kullanılması konusunda teşvik etmeleri; FIU'larının diğer FIU'lar ile işbirliği yapmaları ve sofistike teknolojiler kullanmalarını sağlamaları gerektiği; kullanılan sofistike teknolojilerin bir FIU'nun elindeki bilgilerin, diğer FIU'nun elindeki tam koruma sağlanmış kişisel verileri anonimleştirilmiş şekilde karşılaştırabilecek nitelikte olması gerektiği[54]; Üye ülkelerin FIU'larının sınır aşan boyutu olan analizler konusunda Europol ile işbirliği yapmalarını sağlamaları gerektiği[55] belirtilmektedir.

5.2. Kişisel Verilerin İşlenmesi Ve Serbest Dolaşımı Karşısında Bireylerin Korunması Tüzüğü Taslağı (Genel Veri Koruma Tüzüğü Taslağı)

Tüzük taslağının 5 inci maddesine göre, işlenecek olan kişisel verilerin,

- Hukuka uygun, adil ve şeffaf bir şekilde verinin konusuna ile ilgili işlenmesi,
- Belli, açık ve yasal amaçlar için toplanması; amaç dışı bir şekilde işlenmemesi,
- İşlenme amaçları ile bağlantılı olarak minimum gerekler çerçevesinde yeterli, uygun ve sınırlı olması; kişisel veri ile ilintili olmayan bilginin işlenmesi sureti ile elde edilemeyecek amaçların varlığı halinde işlenmesi,

[52] Direktifin 51 inci maddesi.
[53] Direktifin 52 nci maddesi.
[54] Direktifin 53 üncü maddesi.
[55] Direktifin 54 üncü maddesi.

- Doğru ve güncel, işlenme amaçları ile uyumlu olup olmadığının dikkate alınarak yanlış olan verinin erteleme olmaksızın silinmesini sağlayacak makul adımların atılması,
- Kişisel verinin işlenmesindeki amacın ortadan kalkması halinde veri konusunun belirleyici niteliğinin ortadan kaldıracak formda tutulması gerekmektedir. Kişisel veri, 83 üncü maddede belirtilen şartların yerine getirilmesi kaydı ile yalnızca tarihi, istatistiki ve bilimsel amaçlar için işlenebilmesi maksadı ile daha uzun süre muhafaza edilebilir.
- Veri kontrolörlerinin sorumluluğunda bu tüzüğün maddeleri ile uyumlu bir şekilde veri işlemenin gerçekleştirilmesi,

  Gerekmektedir.

Tüzük taslağının 16 ncı maddesine göre işlenen verinin öznesi konumundaki kişinin eksik olan kişisel verileri tamamlanmasını veya yanlış olan bilgilerin düzeltilmesini isteme hakkı vardır.

Diğer taraftan Tüzük taslağının 17/2 nci maddesine göre, işlenen verinin öznesi konumundaki kişinin aşağıdaki şartların en az birinin varlığı durumunda, hakkındaki verinin silindiğine dair bilgiyi kontrolörden alma ve verinin daha fazla paylaşılmasının engellenmesini isteme hakkı bulunmaktadır.

- Verinin toplanma veya işlenme amacının ortadan kalkmış olması,
- Verinin işlenmesi konusundaki veri öznesinin rızasının geri çekilmiş olması; üzerinde uzlaşılan veri muhafaza zamanının dolması; verinin daha fazla işlenmesini gerektirecek yasal dayanağın olmaması,
- Veri öznesinin 19 uncu madde kapsamında itiraz etmiş olması,
- Verinin işlenmesinin diğer nedenlerle bu tüzük kuralları ile uyumsuz olması,

Tüzük taslağının 17/3 ncı maddesine göre kontrolör, silme işlemini aşağıdaki durumların bulunması dışındaki durumlarda gecikmeksizin yerine getirmek durumundadır.

- 80 inci maddede belirtilen fikrini açıklama hürriyetinin uygulanabilmesi,
- 83 üncü maddede belirtildiği gibi tarihi, istatistiki ve bilimsel amaçların olması,

Birlik veya üye devletler, “kişisel verilerin işlenmesi prensipleri” başlıklı 5 inci maddenin (a) ila (e) bentlerine; “şeffaflık ve yönetim” kısım başlığı altındaki 11 ila 13 üncü maddelerine; “bilgi ve veriye ulaşım” kısım başlığı altındaki 14 ila 15 inci

maddelerine; “düzeltme ve silme” kısım başlığı altındaki 16 ila 18 inci maddelerine; “itiraz ve profil” kısım başlığı altındaki 19 ila 20 nci maddelerine,

- Kamu güvenliği,
- Mahkumiyet gerektiren fiillerin önlenmesi, kovuşturulması, araştırılması, incelenmesi,
- Piyasa istikrarının ve bütünlüğünün korunması; para, bütçe ve vergi konularını da içeren Üye Devletin veya Birliğin ekonomik ve finansal çıkarları dahilinde Üye Ülke ve Birliğin diğer kamu çıkarlarının gerektirmesi,
- Veri öznesinin veya diğer kişilerin özgürlük haklarının korunması.

Tüzük taslağının 30/1,2 nci maddelerine göre kontrolör ve veri işleyicisi,

- Uygulamalarının maliyetleri ve tekniğin son durumunu göz önünde bulundurmak; kişisel verinin doğasından ve işlemeden kaynaklanacak riskleri dikkate almak sureti ile makul derecede güvenlik tedbirlerini teknik ve organizasyonel yaptırımlar uygulamak sureti ile almak durumundadır.
- Risklerin gelişimini takip ederek kişisel veriler kazalara; hukuksuz yok etmelere; izinsiz açıklama, yayma, erişim ve değiştirme gibi yasadışı işlemelere korunması maksadı ile tedbir almalıdır.

Tüzük taslağının 40 ıncı maddesine göre, işlenen; üçüncü ülke veya uluslararası kuruluşa aktarıldıktan sonra işlenecek olan kişisel verilerin transferi ancak kontrolör ve işleyicinin bu Tüzüğün kurallarına uyması şartı ile mümkün olacaktır. Bu durum, üçüncü ülkelerden veya uluslararası organizasyonlardan diğer üçüncü ülkelere ve uluslararası organizasyonlara yapılacak veri transferlerinde de söz konusu olacaktır.

Yeterli derecede koruma olup olmadığı Komisyon tarafından karara bağlanacaktır. Bu yeterlilik,

- Kamu güvenliği, savunma, ulusal güvenlik, ceza hukuku, meslek kuralları alanlarında yürürlükteki hukuk kuralları; veri öznesinin haklarının korunması açısından etkin idari ve cezai tazminatın uygulanabilirliği,
- Üye Ülke ve Birlik ile işbirliği içerisinde veri öznesinin şikayetlerini değerlendirecek ve hakkını kullanmasında yol gösterici olacak denetim mekanizmasının varlığı,
- Talep üzerine uluslararası taahhüt verilmesi,

hallerinde söz konusu olacaktır.

Tüzük taslağının 41 inci maddesinde belirtildiğine göre Komisyon, yeterli güvenliğin sağlanamadığı yerlerde Tüzüğün 87/2 nci maddesindeki prosedürlerin yerine getirilmiş olması; kişisel verilerin korunması hakkı ile ilgili aşırı acil durumun ortaya çıkması durumunda 87/3 maddesindeki prosedürün yerine getirilmesi durumunda veri aktarımına izin verebilecektir.

Komisyonun 41 inci madde kapsamında karar almamış olması durumunda kontrolör veya işleyen, verinin aktarılacağı tarafta kişisel verilerin korunmasına ilişkin yasal bağlayıcılığın ortaya konulması durumunda aktarım yapabilecektir. Bunun gerçekleşmesi için,

- 43 üncü madde ile bağlantılı kurumsal kuralların var olması,
- Kontrolör, işleyici ve alıcı arasında 4 üncü paragraf ile uyumlu bir şekilde denetleyici otoritenin onayının olması,
- Onayın alınması,

Gerekecektir.

Veri öznesi diğer üye ülkedeyse veya verinin Birlik içerisinde hareketini ilgilendiriyor ise Denetleyici otorite 57 nci madde ile uyumu gözetmek durumundadır.

Kişisel verilerin korunması ile ilgili yasal bağlayıcılığı olan hükümlerle koruma sağlanmadığı durumlarda kontrolör veya işleyici, transfer için ön onay talep eder. Onay, transferlere temel oluşturmak üzere bu tür idari düzenlemelerin içine derç edilir. Bu hususstaki düzenlemelerin Tüzüğün 34/1 inci maddesi ile uyumlu olması gerekmektedir. Aktarımın Üye Devlet veya Devletlerde veri işlemesi ile ilgili olması; verinin Birlik içinde serbest dolaşımı ile ilgili olması durumunda denetleyicinin, 57 inci madde ile uyumu sağlaması gerekir.

Tüzük taslağının 42 nci maddesine göre 95/46/AT'nin 26 ncı maddesi ile uyumun denetletici otorite tarafından sağlanmış olması durumunda, denetleyici otoritenin bunu değiştirinceye, yürürlükten kaldırıncaya kadar geçerliliği devam eder.

Tüzük taslağının 43 üncü maddesinde belirtildiğine göre, denetleyici mekanizma, 58 inci maddede belirtilen hususları sağlaması şartı ile aşağıdaki şartların oluşması kaydı ile bağlayıcı kurumsal kuralları kabul edebilir:

- Yasal olarak bağlayıcı ve kontrolör veya işleyici grubunun her bir üyesi veya çalışanı tarafından uygulanması,
- Açık bir şekilde veri öznesinin haklarına uygulanabilirlik,

- Kişisel verilerin korunması ile ilgili olarak ikinci paragrafta belirtilen birtakım kurallar dahilinde gereklerin yerine getirilmesi.

Tüzük taslağının 44 üncü maddesinde belirtildiği üzere, 41 inci maddede belirtilen yeterlilik şartının kararının verilmesi için gerekli şartların sağlanmaması; 42 nci maddede belirtilen güvenliğin sağlanması için gerekli şartların yerine getirilmemesi halinde şu şartlarda üçüncü ülkelere veya uluslararası organizasyonlara veri aktarılabilir:

- Riskler hakkında veri öznesinin haberdar edilmesine rağmen rızasının olması,
- Anlaşma öncesi işlemlerin gerçekleştirilmesi ya da veri öznesi ile kontrolör arasındaki bir anlaşmanın uygulanması maksadıyla veri öznesinin talebinin olması,
- Kontrolör ile diğer gerçek ve tüzel kişiler arasında yapılan anlaşmanın veri öznesinin menfaatine sonuçlar doğuracak olması,
- Kamu yararı için gerekliliğin olması,
- Yasal bir hakkın oluşturulması uygulanması ve savunulması için gereklilik olması,
- Veri öznesinin fiziki veya yasal olarak onay vermesinin mümkün olmadığı durumlarda transferin, veri öznesinin veya üçüncü kişinin haklarının korunması için gerekmesi,
- Belli bir olay ile ilgili olarak danışmada bulunulması için üye ülke veya birlik hukukunda belirtilen durumlarda yasal çıkarlarını ispatlayabilen kişilerin veya genel kamu çıkarlarının gerektirmesi halinde kamuya açık sicilden veri aktarımı yapılması. Bu durum sicildeki tüm veriler için söz konusu değildir.

Tüzük taslağının 45 inci maddesinde belirtildiğine göre, Komisyon veya denetleyici otorite, üçüncü ülke veya uluslararası organizasyon ile ilgili olarak aşağıdaki adımları atacaktır:

- Kişisel verilerin korunmasına ilişkin kanunların uygulanmasını sağlamak için etkin uluslararası işbirliği mekanizmaları kurmak,
- Kişisel verilerin korunmasına ilişkin kanunların uygulanmasını sağlamak için uluslararası karşılıklı yardımlaşma sağlamak,
- Uluslararası işbirliğini arttırma maksadıyla paydaşlarla yakın ilişki kurmak,
- Kişisel verilerin korunması yaslarının ve uygulamalarının dokümantasyonu ve paylaşımı için destek olmak.

44 üncü maddenin birinci paragrafının (b), (c) ve (h) bentleri hükümleri, kamu otoritelerinin görevlerini ifaları esnasında gerçekleştirecekleri uygulamalar hakkında hüküm ifade etmez.

Kamu yararının ne olduğunun Birlik hukukunda veya kontrolörün tabi olduğu ulusal mevzuatta tanımlanmış olması gereklidir.

5.3. TBMM'de Bulunan Kişisel Verilerin Korunması Kanun Tasarısı

Kanun Tasarısının 3 üncü maddesinde belirtildiği üzere, kimliği belirli veya belirlenebilir gerçek kişiye ilişkin her türlü veri kişisel veri kapsamına girmektedir.

Tasarının 4 üncü maddesinde, kişisel verilerin işlendikleri amaç için gerekli olan süre kadar muhafaza edilmeleri esastır. Bu verilerin işlenmesi için gerekli sebebin ortadan kalkması durumunda yok edilmesi veya anonim hale getirilmesi gerekecektir.

Kanunun 7 nci maddesinde, verinin işlenmesini gerektiren sebeplerin ortadan kalkması halinde kişisel verilerin res'en veya ilgili kişinin talebi üzerine veri sorumlusu tarafından silineceği, yok edileceği veya anonim hale getirileceği[56] belirtilmektedir. Diğer taraftan Kanın Tasarısının aynı maddesinde, kişisel verilerin silinmesi, yok edilmesi veya anonim hale getirilmesine ilişkin diğer kanun hükümlerinin saklı olduğu belirtilmektedir.

Kanunun 5 inci maddesine göre kişisel veriler ilgili kişinin açık rızası olmaksızın işlenemez. Bu durumun çeşitli istisnaları bulunmaktadır. Bu istisnalardan en önemlileri ise,

- Kanunlarda açıkça öngörülmesi,
- Veri sorumlusunun hukuki yükümlülüğünü yerine getirebilmesi için zorunlu olması,

olarak sıralanabilir.

Kanun Tasarısının 7 nci maddesinde belirtildiği üzere kişisel veriler, ilgili kişinin açık rızası olmadan üçüncü kişilere veya yurtdışına çıkarılamaz. Kişisel veriler,

- Kanunun açıkça öngörmesi,

[56] kişisel verilerin, kimliği belirli veya belirlenebilir bir gerçek kişiyle ilişkilendirilemeyecek hale getirilmesini ifade etmektedir.

- Fiili imkansızlık nedeni ile rızasını açıklayamayacak durumda bulunan veya rızasında hukuki geçerlilik tanınmayan kişinin kendisinin veya bir başkasının hayatı veya beden bütünlüğünün korunması için zorunluluk olması,
- Bir sözleşmenin kurulması veya ifasıyla doğrudan doğruya ilgili olması kaydıyla, sözleşmenin taraflarına ait kişisel verilerin işlenmesinin gerekli olması,
- Veri sorumlusunun yükümlülüğünü yerine getirmesi için zorunlu olması,
- İlgili kişinin kendisi tarafından alenileştirilmiş olması,
- Bir hakkın tesisi, kullanılması veya korunması için veri işlemenin zorunlu olması,
- Kanunlarda açıkça öngörülmesi,
- Kamu sağlığının korunması, koruyucu hekimlik, tıbbi teşhis, tedavi ve bakım hizmetlerinin yürütülmesi ile sağlık hizmetlerinin yönetimi ve finansmanı amacıyla, sır saklama yükümlülüğü altında bulunan kişiler tarafından işlenmesi,

hallerden birinin bulunması durumunda, üçüncü kişilere; ilgili yabancı ülkede yeterli korumanın bulunması koşulu ile yurtdışına, ilgilinin açık rızası aranmaksızın aktarılabilir.

Kişisel verinin aktarılacağı yabancı ülkede yeterli koruma bulunmaması halinde kişisel veriler ancak;

- İlgili kişinin açık rızasının bulunması,
- Türkiye'deki ve kişisel verilerin aktarılacağı yabancı ülkedeki veri sorumlularının yeterli bir korumayı yazılı olarak taahhüt etmesi ve kurulun izninin bulunması,

hallerinde yurt dışına aktarılabilir.

Siyasi parti, vakıf, dernek veya sendika gibi kar amacı gütmeyen kuruluş ya da oluşumların, tabi oldukları mevzuata ve amaçlarına uygun olmak, faaliyet alanları ile sınırlı olmak ve üçüncü kişilere açıklanmamak kaydıyla kendi üyelerine ve yönelik verilerin,

- Kanunlarda açıkça öngörülmesi,
- İlgili kişinin açık rızası ile kurulun izninin birlikte bulunması,

Şartıyla üçüncü kişilere ve yeterli koruma bulunması koşuluyla yurtdışına aktarılabilir.

8 inci maddenin 5 inci fıkrasına göre, yabancı ülkelerde yeterli koruma bulunup bulunmadığı Kurulca belirlenerek ilan edilir. Veri paylaşımında bulunulacak ülkelerde yeterli koruma olup olmadığına,

- Taraf olduğumuz uluslararası sözleşme hükümleri,
- Kişisel veri talep eden ülke ile Türkiye arasında karşılıklılık durumunun olup olmadığı,
- Her somut kişisel veri aktarımına ilişkin olarak, kişisel verinin niteliği ile işleme amaç ve süresi,
- Kişisel verinin aktarılacağı ülkede geçerli olan mevzuat,
- Kişisel verinin aktarılacağı ülkedeki veri sorumlusu tarafından taahhüt edilen önlemler,

dikkate alınmak sureti ile karar verilir.

Kanun Tasarısının 11 inci maddesine göre veri sorumlusu,

- Kişisel verilerin hukuka aykırı işlenmesini önlemek,
- Kişisel verilere hukuka aykırı erişimini önlemek
- Kişisel verilerin muhafazasını sağlamak,

amacıyla uygun güvenlik düzeyini sağlamaya yönelik gerekli tedbirleri almak zorundadır.

Aynı Kanun Taslağı maddesine göre, veri sorumlusu, kişisel verilerin kendi adına başka bir gerçek ve tüzel kişi tarafından işlenmesi halinde, kişisel verilerin hukuka aykırı işlenmesinin önlenmesi; kişisel verilere hukuka aykırı erişimin önlenmesi; kişisel verilerin muhafazasının sağlanması hususlarında bu kişilerle müştereken sorumludur. Veri sorumluları ile veri işleyen kişiler, öğrendikleri kişisel verileri bu kanun hükümlerine aykırı olarak başkasına açıklayamaz ve kendi şahsi çıkarları için kullanamazlar. Bu yükümlülük görevlerinden ayrılmalarından sonra da devam eder.