



akıllı
belediyecilik
zirvesi

19-20 Aralık 2018
MARMARA
BELEDİYELER BİRLİĞİ

E-Devlet Açısından KVK Uygulamaları, Mustafa AFYONLUOĞLU
19.12.2018

**E-DEVLET AÇISINDAN
KVK UYGULAMALARI**

Kişisel Verilerin Yönetiminde Sorumluluklar ve Riskler

MUSTAFA AFYONLUOĞLU
Siber Güvenlik, E-Yönetişim ve E-Devlet Kıdemli Uzmanı

Hazırlayan : Mustafa AFYONLUOĞLU

Tarih : 19.12.2018

Etkinlik : Akıllı Belediyecilik Zirvesi 2018 (Marmara Belediyeler Birliği – Point Hotel Barbaros İstanbul) <http://www.abz.com.tr/>

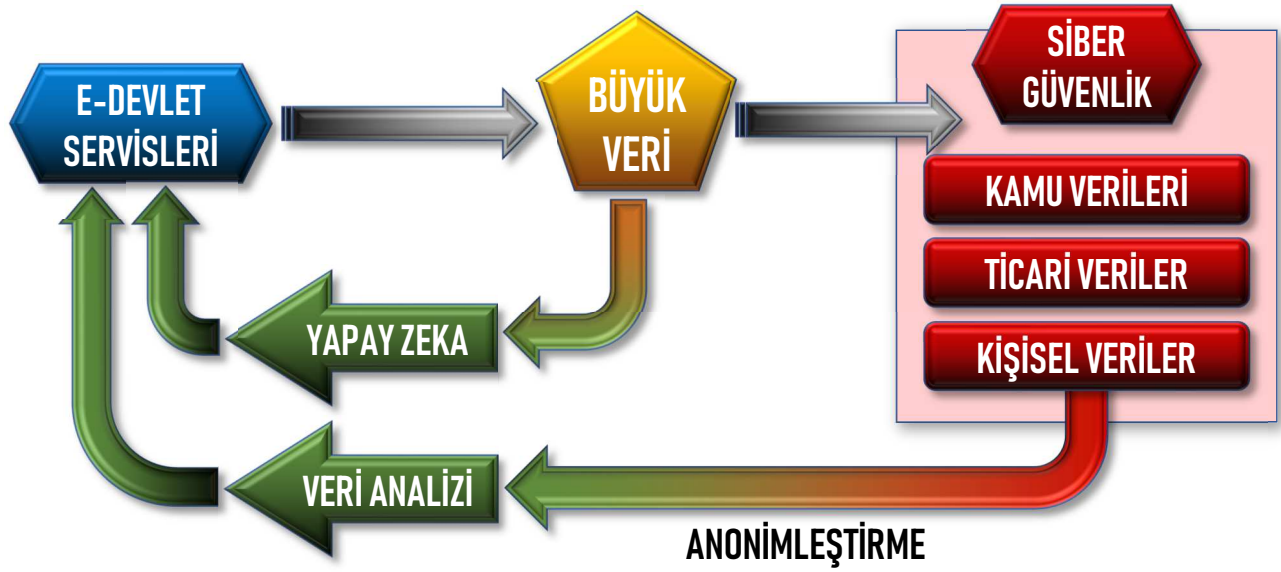
Erişim : <http://afyonluoglu.org> → KAYNAKLAR → SUNUMLAR

Telif Hakkı: Aralık 2018, Mustafa Afyonluoğlu

Yayım / Alıntı Şartı: Sunumdan alıntı yapılması için açık referans (Eser Sahibinin Adı Soyadı, Yayınlandığı Web Sayfası Adresi) gösterilmesi zorunludur.

NOT: Bu sunumda herhangi bir kurum temsil edilmemektedir. Tüm görüş ve değerlendirmeler sunumu yapan kişinin uzmanlık değerlendirmeleridir.

E-DEVLET'İN HAYATIMIZDAKİ YERİ



Kamu kurumları tarafından vatandaşa (G2B), iş dünyasına (G2B) ya da diğer kamu kurumlarına (G2G) verilen elektronik hizmetler kapsamında gerek hizmeti sağlayabilmek için toplanan veriler, gerekse hizmet sonucu oluşan yeni veriler, ciddi bir «**büyük veri**» oluşturmaktadır. Yeni alanlarda ekonomik katma değer sağlamak (**Açık Veri**), istatistiki çalışma yapmak veya hizmet kalitesini iyileştirmek için, oluşan bu veriden istifade etmek oldukça önemli hal almıştır. Özellikle bilgi işleme ve analiz kapasitelerinin gelişmesi ve yapay zeka gibi araçlara ait algoritmaların daha olgunlaşması, bu cazibeyi daha da arttırmıştır.

Oluşan bu büyük verinin yapay zeka algoritmasının olgunlaşması ve gelişmesinde girdi olarak kullanılması ve bunun sonucunda daha nitelikli hizmetlerin ortaya çıkmasında veri gizliliği bakımından bir sakınca oluşmamaktadır. Çünkü mevcut veriler ifşa edilmemekte, paylaşılmamakta, sadece derin öğrenme sürecinde yapay zekanın olgunlaşması için gerekli olan sayısal değerlerin çözümlülüğünün artmasında kullanılmaktadır.

Bununla birlikte, **ticari veriler**, **kamu verileri** ve **kişisel verilerden** oluşan bu büyük veri havuzu ile birlikte **verinin siber güvenliğinin** sağlanması gündeme gelmektedir. Bir alt küme olan kişisel verilerin korunması bakımından bu havuzdaki verilerin korunması da hem hassasiyet gerektirmekte, hem de bu alandaki mevzuata uyum açısından (ticari verilerde ve kamu verilerinde olduğu gibi) bir takım yükümlülükler ve buna bağlı olarak cezai müeyyideler getirmektedir.

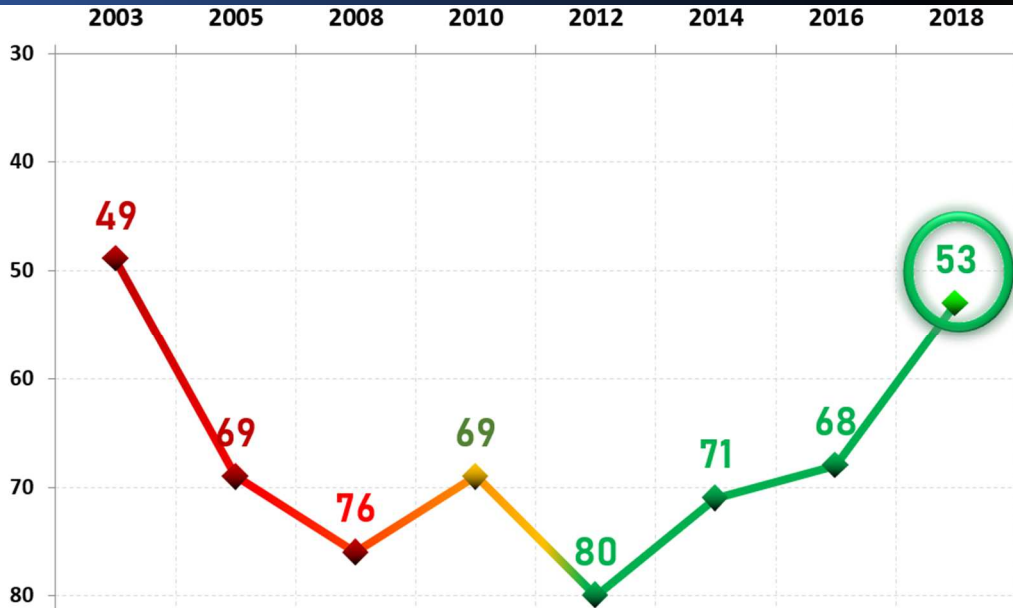
Bu havuzdaki verilerin **anonimleştirilmesi** sayesinde oluşan **açık veri**, **yeni ekonomik faydalar** sağlamak, **istatistiki sonuçlar** yayımlamak ve **araştırma-geliştirme çalışmalarına** altlık sağlamak bakımından oldukça önemli bir konuma sahiptir. Bu kapsamda faydayı üretebilmek için anonimleştirme işleminin yapılması giderek daha büyük bir ihtiyaç olarak karşımıza çıkacak, üstelik bu işlemin hatasız yapılması (yani ifşaya mahal vermemesi) ve hatta mümkün olduğunca **veri fayda kaybının en az olmasına** yönelik baskılar artacaktır. (Veri fayda kaybının minimum olması, hedeflenen anonimleştirme seviyesini elde ederken anonimleştirmeden kaynaklı kaybın en az hale getirilmesidir)

Tüm bu anlatılan süreçlerdeki hedeflenen faydaya ulaşabilmek için 2 önemli hususta

olgunlaşma ihtiyacı bulunmaktadır:

1. E-Devlet Alanında yeterli olgunluęa ulaşmak ve bu vesileyle kaliteli (temiz, hatasız ve güvenilir) büyük veri oluşturmaya başlamak
2. Bu verilerden istifade ederken özellikle kişisel veriler bakımından sağlıklı anonimleştirme süreçlerini sağlayabilmek

Türkiye BM e-Devlet Puanlaması



Kaynak: BM e-Devlet Kalkınma Endeksi, <http://goo.gl/n2Pt7i>

<http://unpan3.un.org/egovkb/en-us/Data/Country-Information/id/176-Turkey/dataYear/2014>



E-DEVLET AÇISINDAN KVK UYGULAMALARI

E-Devlet açısında ülkemize baktığımızda, özellikle Başbakanlık tarafından e-Devletin en üst seviyeden koordinasyonunu ele aldığı ve uluslararası ölçümlerle kuruluşları ile birebir çalışmaların ve yakın temasların başladığı yıllardan itibaren, kamu kurumlarının da sağladığı elektronik hizmetlerin çeşitlenmeye ve olgunlaşmaya başlaması ile birlikte Türkiye'nin e-Devlet sıralamasında hızla yukarıya doğru tırmandığı görülmektedir.

2003 yılında bu yana yaklaşık 16 farklı uluslararası e-devlet ölçümlerine çalışması yapılmakla beraber(*1) bu çalışmalar arasında en geniş kesimi kapsayan (193 ülke), en uzun süredir düzenli ve tutarlı olarak devam eden (2003'den bu yana her 2 yılda bir, toplam 8 kez) ve şeffaf yöntemlerle ölçümlemeyi yapan en çok dikkate alınan çalışma Birleşmiş Milletler E-Devlet Olgunluk Ölçümlemesidir (*2). (UN e-Government Survey). Grafikte, bu ölçümlerlerdeki Türkiye'nin yıllar içerisindeki ilerlemesi görülmektedir.

(*): E-Devlet Uluslararası Ölçümler çalışmaları ile ilgili geniş bir araştırma makalesi şu adresten ulaşabilirsiniz:

Sayfa : <http://afyonluoglu.org/kaynaklar/makale-ve-yazilar/>

Makale: <http://afyonluoglu.org/PublicWebFiles/Papers/ECDG2017-Mustafa%20Afyonluoglu%20Ali%20Ziya%20Alkar.pdf>

(*2) Birleşmiş Milletler E-Devlet Olgunluk Ölçümler Raporlarının tamamına şu adresten ulaşabilirsiniz:

http://afyonluoglu.org/e-devlet/egovbench/bench_un/

BM Yerel E-Devlet Endeksi (LOSI)

- 4 Ana Başlıkta 60 Gösterge
 - Teknoloji : 12 Gösterge
 - İçerik Sunumu : 26 Gösterge
 - Hizmet Sunumu : 13 Gösterge
 - Katılımcılık : 9 Gösterge
- Dünya üzerinde bölgeleri temsilen seçili 40 Pilot Şehir
 - Avrupa : 12 Şehir
 - Amerika : 6 Şehir
 - **Asya : 13 Şehir**
 - Afrika : 7 Şehir
 - Okyanusya : 2 Şehir

Çin- Şangay	: 14.35 Milyon
Türkiye – İstanbul	: 14.10 Milyon
Hindistan – Mumbai	: 11.98 Milyon
G.Kore – Seul	: 9.86 Milyon
Endonezya -Jakarta	: 9.61 Milyon
Pakistan – Karaçi	: 9.34 Milyon
Japonya – Tokyo	: 9.27 Milyon
Tayland – Bangkok	: 6.46 Milyon
BAE – Dubai	: 2.98 Milyon
Kazakistan – Almatya	: 1.51 Milyon
Malezya – Kuala Lumpur	: 1.59 Milyon
S.Arabistan – Riyad	: 5.19 Milyon
Sri Lanka – Kolombo	: 0.65 Milyon

Bununla birlikte, e-Devlet Ölçümlenmesi denilince büyük bir kesim tarafından çok bilinmeyen kıymetli bir diğer ölçümlenme, BM LOSI (Birleşmiş Milletler E-Devlet Yerel Yönetimler Çevrimiçi Hizmet Endeksi) ölçümlenmesidir (*1). İlk kez 2018 yılında başlatılan bu çalışma ile, tüm dünyadan, geneli temsil edecek 40 ülke ve her ülkeden bir şehir seçilmiş ve ölçümlenmede 60 kriter esas alınmıştır. Bu kriterlerin 12 tanesi teknoloji bakımından, 26 tanesi içerik sunumundaki kalite ve yeterlilik bakımından, 13 tanesi hizmetin sunulmasındaki yöntemler bakımından ve 9 tanesi de yerel yönetimin elektronik katılımcılıkta ortaya koyduğu imkanlar bakımından ele alınmıştır.

Türkiye, bu çalışmada **Asya** grubundaki 13 ülkeden birisi olarak seçilmiş ve Türkiye'den **de İstanbul Belediyesi** ele alınmıştır. İstanbul, 14.1 milyon nüfusu ile, Asya bölgesinden seçilen diğer pilot şehirler arasında, **nüfusu en büyük 2. şehirdir**.

(*1): Bu çalışma ilk kez 2018 yılında başlatılmış olup, bu konudaki tüm detaylar ve sonuçlar **E-Devlet Olgunluk Ölçümlenme 2018 Raporu'nun 7. bölümünde** yer almaktadır.

LOSI: Local Online Service Index

LOSI Kriterlerine Örnekler

- **Teknoloji:** Tarayıcı uyumluluğu, mobil cihazlardan erişilebilirlik, portalde kolay arama ve bilgiye erişim, yabancı dil desteği ...
- **İçerik Sunumu:** Belediye hakkında bilgiler, bütçesel bilgiler, ihale duyuruları, iletişim bilgileri, sağlanan servislerle ilgili bilgiler, açık veri sunumu, çevrimiçi destek, ilgili diğer kamu kurumlarına bağlantılar...
- **Hizmet Sunumu:** Kişisel verilere erişim, kimlik doğrulama imkanı, e-postalara cevap gecikme süresi, adres değişiklik bildirimleri, e-ödeme, çevrimiçi yapı izni, ...
- **Katılımcılık:** Gerçek zamanlı iletişim, taleplere geri dönüş, sosyal ağ özellikleri, halka açık alanlardaki etkinlik bildirimleri, katılımcı bütçe, katılımcı ortak alan planlama, yaklaşan e-katılım etkinliklerinin duyurulması, ...

BM Yerel E-Devlet Endeksi (LOSI)

Çin- Şangay	: 14.35 Milyon
Türkiye – İstanbul	: 14.10 Milyon
Hindistan – Mumbai	: 11.98 Milyon
G.Kore – Seul	: 9.86 Milyon
Endonezya -Jakarta	: 9.61 Milyon
Pakistan – Karaçi	: 9.34 Milyon
Japonya – Tokyo	: 9.27 Milyon
Tayland – Bangkok	: 6.46 Milyon
BAE – Dubai	: 2.98 Milyon
Kazakistan – Almatya	: 1.51 Milyon
Malezya – Kuala Lumpur	: 1.59 Milyon
S.Arabistan – Riyad	: 5.19 Milyon
Sri Lanka – Kolombo	: 0.65 Milyon

Sıra	Şehir	Karşılanan Kriter
1	Moskova	55
2	Cape Town	53
2	Tallinn	53
4	Londra	51
4	Paris	51
6	Sidney	50
7	Amsterdam	49
7	Seul	49
9	Roma	48
9	Varşova	48
11	Helsinki	47
11	İstanbul	47
11	Şangay	47
14	Madrid	46
14	NYC	46

Değerlendirme sonucunda, Asya grubundan 3 ülkenin ilk 15'e girdiği görülmektedir. İstanbul bu listede 11. sırada yer almaktadır.

BM Yerel E-Devlet Endeksi (LOSI)

Sıra	Şehir	Karşılanan Kriter
1	Moskova	55
2	Cape Town	53
2	Tallinn	53
4	Londra	51
4	Paris	51
6	Sidney	50
7	Amsterdam	49
7	Seul	49
9	Roma	48
9	Varşova	48
11	Helsinki	47
11	İstanbul	47
11	Şangay	47
14	Madrid	46
14	NYC	46

Sıra	Şehir	Karşılanan Kriter
1	Moskova	55
2	Cape Town & Tallinn	53
3	Londra & Paris	51
4	Sidney	50
5	Amsterdam & Seul	49
6	Roma & Varşova	48
7	Varşova	48
8	Helsinki & İstanbul & Madrid	47
9	NYC	46

Aynı puanı alan ülkeler de olduğu dikkate alındığında, aslında **İstanbul'un 8. sırada olduğu** görülmektedir. Bu nüfusta bir şehir için çok ciddi bir başarı olan bu değer, **yerel yönetimlerdeki olgunluğumuzda da diğer belediyelerimize örnek teşkil edecek bir başarıdır.**

Belediyeler, vatandaşa en çok temas eden ve en yoğun hizmeti sağlayan birimler olarak bu anlamda en önemli yönetim birimleridir. Bu birimlerdeki **elektronik hizmet sunumunun olgunluğu**, en başta söylediğimiz hedeflere ulaşmak bakımında çok önemli avantajlar sağlamaktadır.

Belediyeler ve Kişisel Veriler

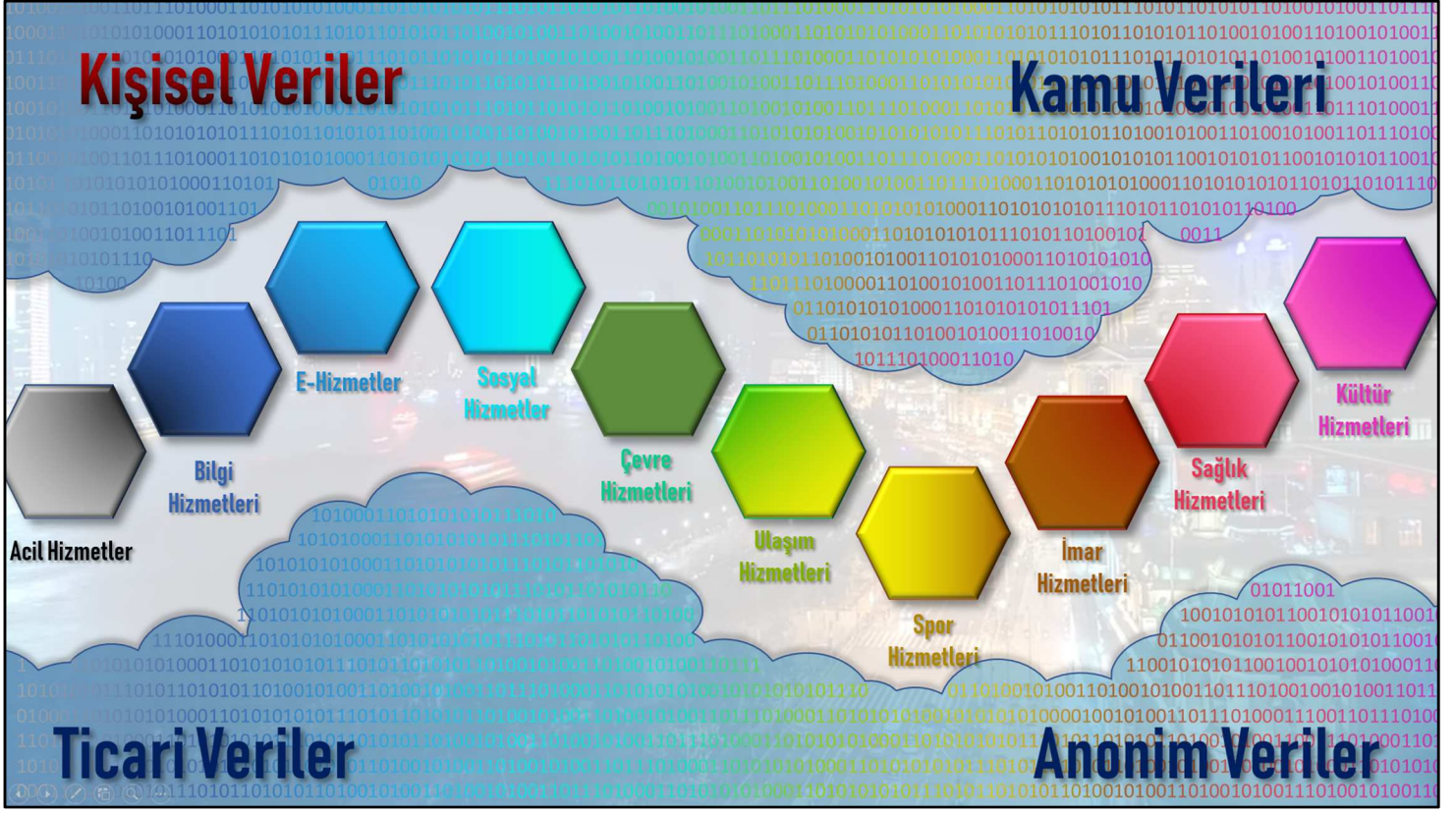
- Belediyeler **vatandaşa** en çok **erişen** ve en çok **hizmet sağlayan** konumuyla ülkedeki en kritik yönetim birimleridir
- Belediye e-hizmetleri akıllandıkça **veri** artıyor.
- **Kişisel Veriler** belediyelerin 2 kritik veri deposudan birisidir.
 - **YBS Verileri** : Ruhsat , ...
 - **CBS Verileri** : İmar planları, kadastral altlıklar, haritalar, ...
 - **Abonelik Sözleşmeleri** (iltihaki Sözleşmeleri) : Su, elektrik, doğalgaz, sosyal tesis, pazaryeri, ulaşım vd. (Özel Hukuk)
 - **İmtiyaz Sözleşmeleri** : içme, kullanma, endüstri suyu, kaynak suyu, atık su, toplu taşıma hizmetleri, katı atıkların toplanması.. 5393 Bld Kn / Md 15
 - **Personel Bilgileri** : İş başvuruları, ...
 - **Sosyal Hizmetlerden Kaynaklı Veriler** : Yaşlı hizmetleri, sosyal yardımlar, ...
 - **Genel Hizmetlerden Kaynaklı Veriler** : Veteriner, pazaryeri, engelli, kurslar, bilgi edinme hakkı, Sosyal tesisler, ...
 - **E-Devlet Hizmetlerinden Kaynaklı Veriler**: Nikah, cenaze, vergiler (emlak, çevre temizlik, reklam ...), kira sözleşme, ruhsat, ...
 - **E-Devlet Entegrasyonları Kaynaklı Veriler**
 -

Bu açıdan belediyelerdeki veri çeşitliliğine baktığımızda, aslında sadece hizmet sunduğu vatandaşların yanısıra, personeli ile ilgili veriler, imtiyaz sözleşmeleri kapsamında özel sektör ile oluşturduğu iş ilişkileri de **kişisel veriler** içermektedir.

Ek Bilgi:

Yargıtay 13. Hukuk Dairesinin E: 1996/1734, K:1996/2495 sayılı ve 18.03.1996 tarihli kararında; “Belediyelerin EGO İşletmeleri ile tüketiciler arasında düzenlenen “Doğalgaz Abonman Sözleşmeleri”, özel hukuk kurallarına tabi, iltihaki sözleşmelerdir (*1). Hukukumuzda sözleşme özgürlüğü varsa da, tekel durumundaki idareler, sözleşmelere, kamu yararına, kamu düzenine aykırı hükümler koyamazlar. ...” denilmiştir.

(*1) **İltihaki sözleşmeler**, bir kamu hizmeti ifa edip, hukuken veya eylemli olarak tekel durumu arz eden ve tüketicinin bağlanması gereken(elektrik, havagazı, doğalgaz, PTT sözleşmeleri) standart hükümler içeren ve tüketicinin olduğu gibi bağlanmak zorunluluğunda kaldığı sözleşmelerdir. Bu sözleşmelerde taraflardan biri olan idare, önceden sözleşme koşullarını hazırlayarak bir icap şeklinde, umuma arz eder ve hizmetten yararlanma ihtiyacı içinde olan yurttaş bunları zımnen kabul etmek suretiyle bağlanır. Genel koşulları önceden tespit eden taraf, bunlarda değişiklik yapma olanağına sahiptir. Ekonomik olarak güçlü olduğu için karşı tarafın ileri sürebileceği değişiklikleri kabule yanaşmaz. Bu durumda taraflardan birinin kendi şartlarını diğerine dikte etmesine yol açan bir sözleşme özgürlüğü; özgürlük olmaktan çıkıp bir ayrıcalık halini kazanır. (**Kaynak:** Şafak Başa, Mülkiye Başmüfettişi, «Belediyelerin Özel Hukuk Sözleşmeleri ve Bu Sözleşmelerden Doğan Alacaklarının Takibi, Sayfa: 30-31 >)



Belediyelerin verdiği hizmetler ele alındığında bunların 10 temel grupta toplandığı görülmektedir. Bu hizmetler vesilesiyle ortaya çıkan veriler:

- Kişisel veriler
- Ticari veriler ve
- Kamu verileri

olarak öbeklenmekte, ayrıca bu verilerin anonimleştirilmesinden oluşan bir veri grubu da doğmaktadır.

Kişisel Veriler
Ticari Veriler
Kamu Verileri
Anonim Veriler

E-DEVLET

MERNİS e-nabız KAYSİS AKBİS
esbis MERSİS ekap TÜİK Resmi İstatistik

Sağlık Hizmetleri İmar Hizmetleri Ulaşım Hizmetleri

Bunula birlikte verilerde en büyük hacmi ve en geniş çeşitliliği oluşturan başlık **elektronik devlet hizmetleridir**. Dolayısıyla verimliliği yüksek tutmak için ilk aşamada e-devlet kapsamında elde edilen ve üretilen verilere odaklanmak en pratik yaklaşım olacaktır.

Kişisel Verilerin Korunması Neden Önemli?



MEVZUAT CEZAI HÜKÜMLER

Veri Sorumlusu için:

6698 Sayılı Kişisel Verilerin Korunması Kanunu

Madde 18-1-ç:

1.000.000 TL + Disiplin Soruşturması
(Aydınlatma Yükümlülüğü, Veri Güvenliği, Kurul Kararları ,
VERBİS Kayıt ve Bildirim)

GDPR – Avrupa Veri Koruma Tüzüğü

Madde 83-4: 20 Milyon Euro ya da yıllık dünya cirosunun %4'ü



ETİK ve GÜVEN

Gartner 2019 Teknoloji Trendleri - 15.11.2018

«Etik ve Güven»

- Kişisel Verilerin Korunması → Farkındalık oluştu.
- Devletler hızla uyum yasalarını ve yaptırımları hayata geçiriyor.
- «Uyumlu muyuz?» çekincesi yerine «Doğru şeyi yapıyor muyuz?»
(Bu veriyi almak gerçekten şart mı?)

Kişisel verilerin kurumların gündeminde önem kazanmasındaki temel motivasyon, ilk aşamada, ortaya koyulan yasal yükümlülükler ve bu yükümlülüklerin yerine getirilmemesi durumunda oluşacak **cezai müeyyideler** olmuştur. Nitekim ülkemizde bir milyon liraya kadar uygulanabilen cezai müeyyide, GDPR kapsamında Avrupa Birliği'nde 20 milyon Euro (veya küresel cironun %4'ü) gibi oldukça büyük rakamları karşımıza çıkarmaktadır.

Ancak Gartner'ın Kasım 2019'daki bir raporunda bu alanda önemli bir tespit dikkati çekmektedir. Artık **kurumlar ve sektörün motivasyonu**, mevzuata uyumdaki eksiklik ya da hatalardan kaynaklı cezai müeyyideler yerine, verilmesi hedeflenen hizmet için «**bu veriyi almanın gerçekten şart olup olmadığına**» doğru kaymıştır. Çünkü bu alanda yapılan hatalar, yasayla verilen maddi cezalardan daha da önemli olarak kurum ya da şirketin itibarını zedelemektedir. Dolayısıyla **etik ilkeler ve kurumsal güvenin korunmasına** yönelik hassasiyet daha çok öne çıkmaya başlamıştır.

E-DEVLET HİZMETLERİNDE VERİLER



Hizmet için Şart olan Veriler

Gücünü mevzuattan alır
Hizmeti sağlayabilmek için elzemdir.



Yardımcı Veriler

Mevzuatta öngörülmez
Pratik hayatı kolaylaştırır

Taksi: Kaza anında kolay kan bulmak için Kan GRUBU bilgisi

Belediye: Vergi ödemelerini hatırlatabilmek için cep telefonu bilgisi

UYGULAMADAKİ HATA: Hizmeti vermek için bu verinin verilmesini ŞART KOŞMAK
(Battaniye Rıza)

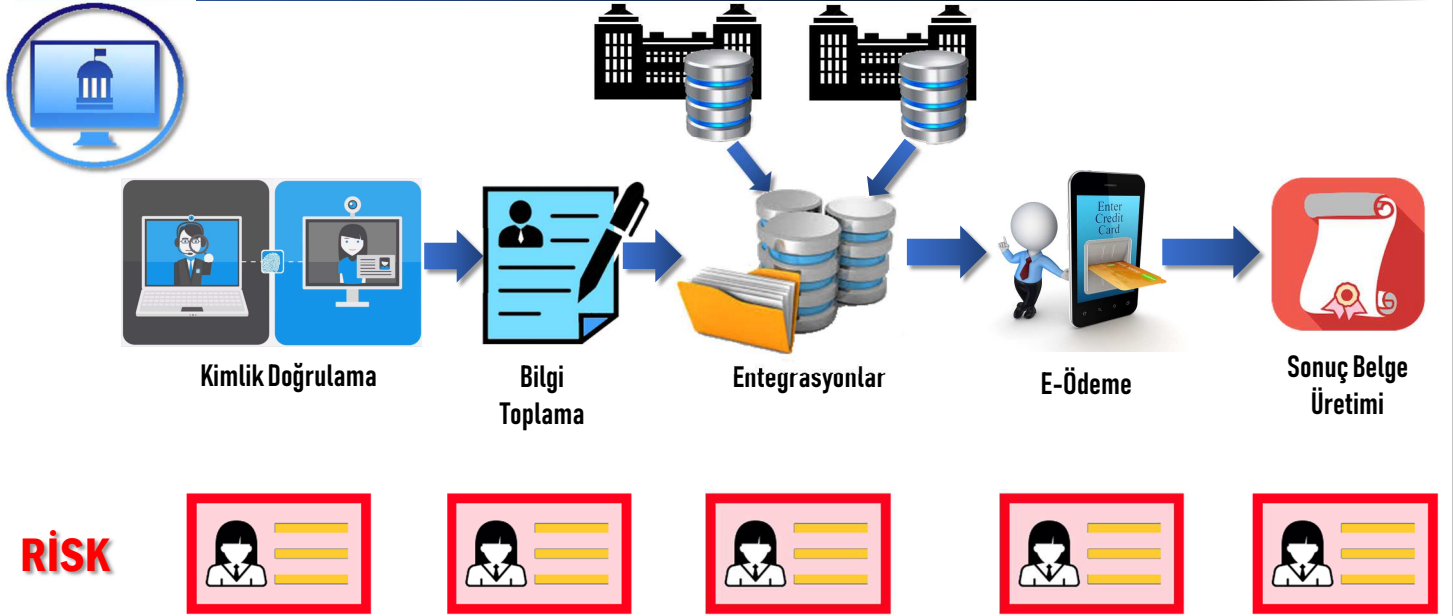
ÇÖZÜM: Açık Rıza Şartlarına Uygun Yaklaşım
(6698 Madde 5: Kişisel Verilerin İşlenme Şartları)

Bu açıdan bakıldığında, e-devlet hizmetleri sağlarken toplanabilecek verileri 2 kategoriye ayırmak mümkündür:

- Hizmetin verilmesi için şart olan, bu veri olmadan hizmeti sağlamanın mümkün olmadığı veriler:** Kurum veya şirketler, bu verinin talebine yönelik gücü mevzuattan alırlar. Aynı şekilde ilgili mevzuatta bu verinin alınış ve kullanım şekilleri ile saklama yükümlülükleri de tanımlanmış olabilir.
- Mevzuatta herhangi bir talep ve tanım bulunmamakla birlikte, pratik yaşamı kolaylaştırmak için alınan yardımcı veriler:** Örneğin bir kaza anında daha hızlı sağlık müdahalesi için taksicilerden kan grubu bilgisinin alınması veya belediyelerin, vergilerin unutulmuş geç yatırılması durumunda vatandaşlarının mağdur olmaması için onlara daha önceden SMS ile haber verebilmek amacıyla cep telefonu numaralarını alması

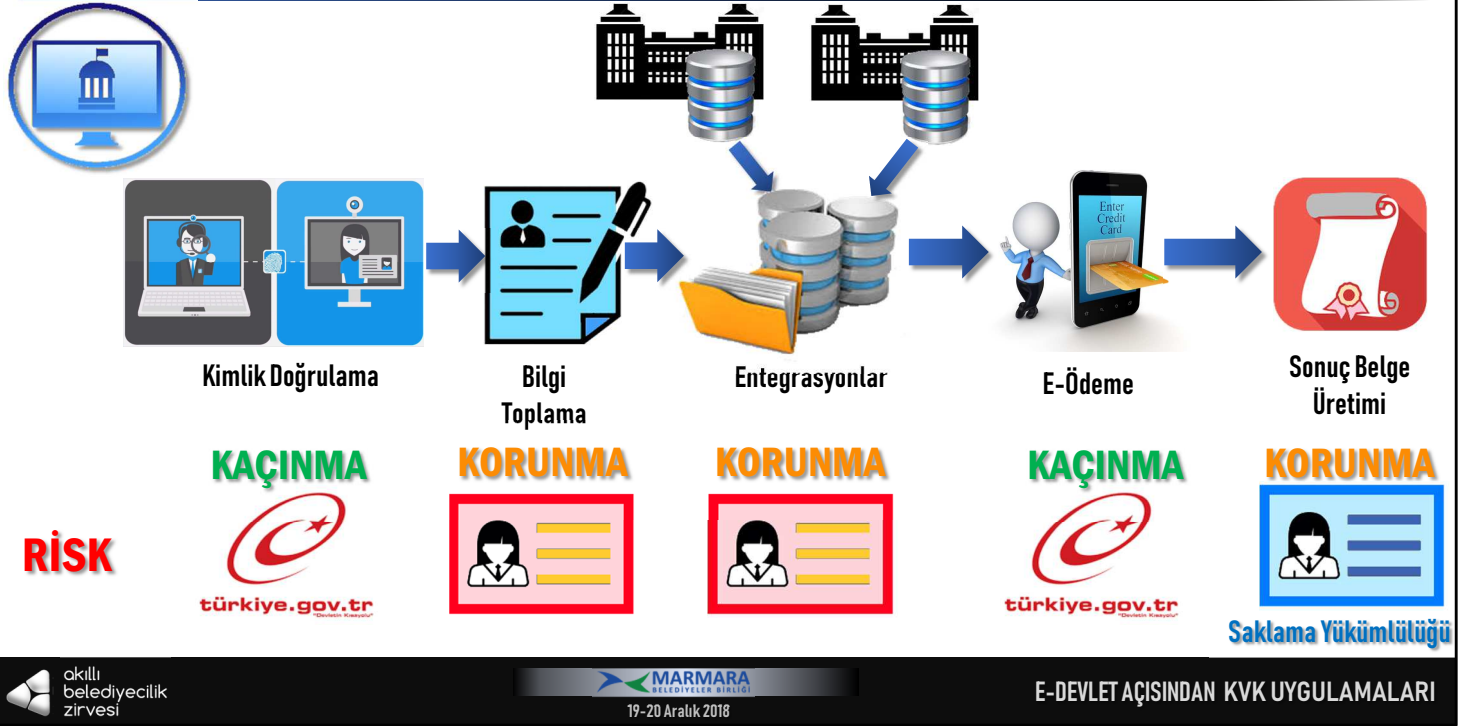
Uygulamada genel olarak en yaygın hata, ikinci gruptaki ekstra bilgileri vatandaştan isterken, asıl hizmetin yapılmasına ilişkin şarta bu verinin teminini bağlamalarıdır. **Battaniye Rıza** olarak da bilinen bu yaklaşım ile, vatandaş hizmeti alabilmesi için **bu veriyi vermek zorunda bırakılmakta**, aslen kanunda belirlenen açık rıza prensipleri işletilmemiş olmaktadır. Çözüm olarak 6698 sayılı kanunun 5. maddesinde belirtilen çerçevede açık rıza alınmalı ve **hizmet şartına bağlanmamalıdır**.

Bir e-Devlet Hizmet Örneği: Emlak Vergisi (Beyan ve Tahsilat)



Belediyelerdeki yaygın bir elektronik hizmet örneğine bakıldığında, önce kimlik doğrulama, ardından alınacak hizmete ilişkin vatandaşın alınması gereken bilgileri sağlama, akabinde bu hizmet için diğer kurumlarda var olan bilgileri entegrasyonlarla alma, sonrasında bu hizmete ilişkin bir hizmet bedeli var ise elektronik ödeme işlemini gerçekleştirme ve son aşamada da hizmetin sonuç çıktısını (makbuz, ruhsat, izin yazısı vb.) oluşturma olarak basitçe bir süreç ele alınabilir. İçerikleri incelendiğinde **bu aşamaların hepsinde kişisel verilerin olduğu** görülmektedir. Dolayısıyla bu süreçte **riskleri minimuma indirmek için**, (bilgi güvenliği süreçlerinde olduğu gibi) her adımın **risk değerlendirmesini** yapmak en sağlıklı yöntemdir.

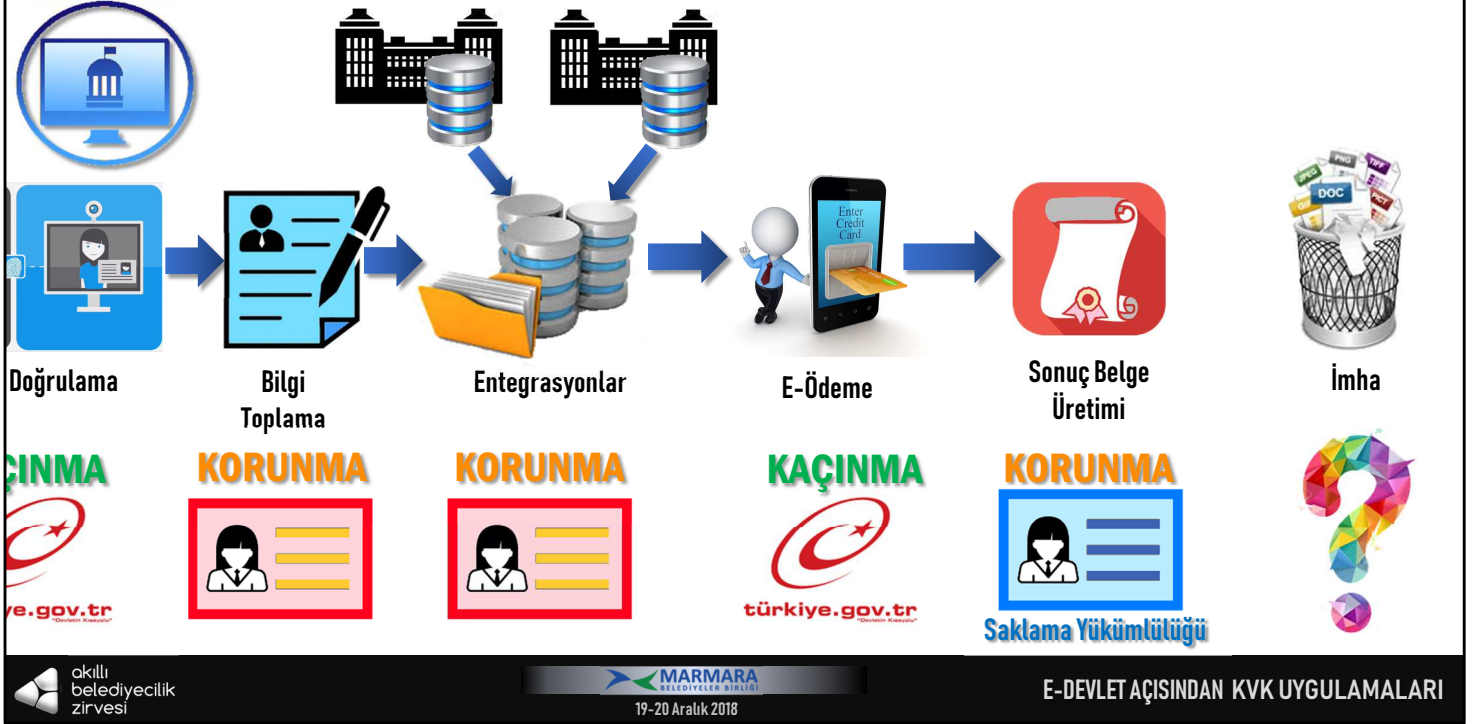
Bir e-Devlet Hizmet Örneği: Emlak Vergisi (Beyan ve Tahsilat)



Risk değerlendirmesinde en çok tercih edilen yöntem, **riskten kaçınma** yollarından birisi olarak, çözüm var ise bu **riski başka bir aktöre devretmektir**. Nitekim verdiğimiz örnek için, kimlik doğrulama ve elektronik ödeme hizmetlerinde e-devlet kapısı (zaten ana hizmet amacı, elektronik hizmetlerde kimlik doğrulama olduğundan) bu hizmetleri sağlayabilir. Dolayısıyla bu iki aşamadaki kişisel veri alma , saklama ve imha yükümlülükleri kendiliğinden ortadan kalkacaktır.

Son aşamada ise, resmi bir belge üretildiğinden, buna ilişkin **saklama yükümlülükleri** dikkate alınarak veri koruma modeli geliştirilmelidir. Bu hususa ilerleyen sayfalarda ayrıca değerlendirilecektir. Geriye kalan 2 aşama için (bilgi toplama ve entegrasyonlar) neler yapılabileceğine öncelikle bakalım:

Bir e-Devlet Hizmet Örneği: Emlak Vergisi (Beyan ve Tahsilat)



Gözden kaçırılmaması gereken daha da önemli bir husus, **saklama yükümlülüğünün** sona ermesine müteakip kurumun takdiri / kurumsal politikası veya ilgilinin **unutulma hakkı** kapsamında gündeme gelecek olan **kişisel verinin imhasıdır**. **Silme, yok etme** ya da **anonimleştirme** olarak gerçekleştirilecek olan bu süreçteki sorunlar ve çözüm önerileri, zaman kısıtı sebebiyle bu sunumda ele alınmamıştır. Konu hakkında detay bilgi alışverişine ihtiyaç duyan katılımcılar, bu alandaki doktora tezimde elde ettiğim sonuç ve değerlendirmelerimi de paylaşabileceğim <http://afyonluoglu.org> adresi üzerinden tarafımla irtibata geçebilir.

KVKK
KİŞİSEL VERİLERİ KORUMA KURUMU

GDPR

KİŞİSEL VERİLER

İLGİLİ KİŞİ (Veri Sahibi)
Kişisel verisi alınan gerçek kişi
Öğrenciler, akademik personel, sözleşmeli personel, ziyaretçiler, hastalar , WiFi Kullanıcıları

VERİ SORUMLUSU
Veri Sahibi'nden veriyi isteyen
İşleme amacı ve araçlarını belirler, veri kayıt sistemini kurar ve yönetir → NE, NEDEN, NASIL (İdari), PAYLAŞIM, SAKLAMA Şartları

VERİ İŞLEYEN
Veri Sorumlusunun verdiği yetki ile veriyi kullanan, üzerinde işlem yapan NASIL (Teknik)

akıllı belediyecilik zirvesi

MARMARA BELEDİYELER BİRLİĞİ
19-20 Aralık 2018

E-DEVLET AÇISINDAN KVK UYGULAMALARI

6698 sayılı kanunun çok yakın dönemde hayata geçmiş olması sebebiyle çoğu zaman **rol tanımlarında tereddütler** olduğu görülmektedir. Veri sorumlusu, veri işleyen ve ilgili kişiyi tayin etmek için en basit yöntem bu sayfada gösterilmiştir. Belirtilen sorular sorulduğunda cevabın karşılığı, bu sorunun olduğu bölümdeki tanımdır. **Örneğin**, işlenecek veride **teknik olarak nasıl yapılacağına** hangi teknik yöntemlerin kullanılacağına karar veren taraf, veri işleyen'dir.

VERİ SORUMLUSU

Tüzel kişiler, kişisel verileri işleme konusunda gerçekleştirdiği faaliyetler kapsamında **bizatihi kendileri** “veri sorumlusu” olup, ilgili düzenlemelerde belirtilen hukuki sorumluluk tüzel kişinin şahsında doğacaktır. Bu konuda **kamu hukuku tüzel kişileri ve özel hukuk tüzel kişileri bakımından bir farklılık gözetilmemiştir**. Veri sorumlusu ifadesiyle, bir şirket içerisinde veri işleme faaliyetlerinden sorumlu **bir kimse kastedilmemektedir**.

BİLGİ İŞLEM DAİRE BAŞKANI VERİ SORUMLUSU DEĞİLDİR

KVKK – Veri Sorumlusu ve Veri İşleyen Kılavuzu, Sayfa 2 «Tanımlar»



E-DEVLET AÇISINDAN KVK UYGULAMALARI

Bu kapsamda en çok yanlış değerlendirilen husus **veri sorumlusu** ile ilgilidir. Genelde bilgi sistemlerinden ve verilerin teknik muhafazasından sorumlu birim bilgi işlem birimleri olduğundan, kanunda bahsedilen **veri sorumlusu**’nun da **bilgi işlem yöneticisi** olduğu gibi **yanlış** bir algıya kapılanlar olabilir. Oysa KVK Kurumu’nun rehberlerinde de açıkça belirtildiği gibi, veri sorumlusu **tüzel kişiliğin bizatihi kendisidir**, burada veri sorumlusu olarak **bir şahıstan bahsedilmemektedir**.

Nereden Başlanmalı?

Veri Haritalama

27001 Bilgi
Güvenliği
Kategorileendirme



Bilgi Varlıklarının Gizlilik Derecelerinin Sınıflandırılması Kılavuzu <http://www.udhb.gov.tr/doc/siberg/siberbilgi.pdf>

Kişisel verilere ilişkin kurumda kolay bir geçiş başlatmak ve sonrasında sağlıklı bir işletme süreci yaşayabilmek için, öncelikle **veri haritalaması** yapılması gerekir. Bunu için gereken temel aşamalar şematikte gösterilmektedir. Bu süreçte yanlış bilinen bir husus, 27001 kapsamında yapılan **bilgi gizlilik kategorilelendirmesinin**, kişisel verilerde veri haritalaması sürecinde ihtiyaç duyulan **kişisel veri kategorileri** ile aynı olduğunun zannedilmesidir. Oysa 27001'de **BİLGİ** varlıkları ele alınırken, KVK'da **VERİ** 'ler kişisel veri perspektifinde (özellikle veri paylaşımı ve anonimleştirme süreçlerinde kullanılmak amacıyla) kategorilelendirilmektedir.

Nereden Başlanmalı?

Veri Haritalama

BİLGİ VARLIKLARI

GİZLİLİK KATEGORİLENDİRİLMESİ

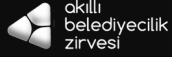


KİŞİSEL VERİLER

KATEGORİLENDİRİLMESİ

VERİ TİPLERİ	
	Bİ: Birincil İndex
	İİ: İkincil İndex
	K10: Açık Tanımlayıcılar Kimlik Tanımlayıcı Öznitelik (ID)
	K11: Tekil Açık Tanımlayıcılar Kimlik Tanımlayıcı Öznitelik (ID)
	K20: Özel Nitelikli Kişisel Veri Hassas Öznitelik (SA)
	K30: Hassas Kişisel Veri Hassas Öznitelik (SA)
	K40: Yarı Tanımlayıcı Birleşik Tanımlayıcı Öznitelik (QI)
	K99: Kişisel Veri Olmayan Alan Tanımlayıcı Olmayan Öznitelik (NSA)

Bilgi Varlıklarının Gizlilik Derecelerinin Sınıflandırılması Kılavuzu <http://www.udhb.gov.tr/doc/siberg/siberbilgi.pdf>



E-DEVLET AÇISINDAN KVK UYGULAMALARI

Örnek olarak Ulaştırma ve Altyapı Bakanlığı tarafından yayımlanan bilgi varlıkları gizlilik kategorileendirme seviyesi ile kişisel veri kategorileri tabloda gösterilmiştir.

Kaynaklar:

1. Bilgi Varlıklarının Gizlilik Derecelerinin Sınıflandırılması Kılavuzu, <http://www.udhb.gov.tr/doc/siberg/siberbilgi.pdf>
2. Kişisel Verilerde Anonimleştirme üzerine yapılan doktora çalışması, Mustafa Afyonluoğlu, 2018 Hacettepe Üniversitesi

Nereden Başlanmalı?

Veri Haritalama



Veri haritalama işlemi, kurumlarımız için genelde yeni bir husustur. Örnek olması bakımından, bir hastanedeki hasta, muayene ve tahlil tablolarına ilişkin bir veri haritasının neye benzediğini gösterir örnek görüntü bu sayfada yer almaktadır. Kurumun veri haritalaması yapacağı her bir tablo için, tablodaki her sütunun kategorilenmesi, diğer tablo alanları ile ilişkisi, hangi kurumlara ne kapsamda verildiği ya da hangi kurumlardan alındığı gibi, aslında **verinin takibini kolaylaştıracak bir zincir yönetim modelidir**. Haritalamadan sonra, mevcut yazılımların uyumlandırılması gerekecektir, çünkü mevzuattaki özellikle veri imhası ile ilgili süreçlerin çok pratik olarak yönetilebilmesi için, eğer imkan var ise (kaynak kodlar ya da dokümantasyondan veri yapısına hakimiyet var ise) veri tablolarına bazı güncellemeler yapma gibi imkanlar mevcuttur.

Nereden Başlanmalı?

Veri Haritalama

İletişim


Sosyal Medya


VERİ HARİTALAMA TABLOLARI

Tablo Kodu	Tablo Adı	Tablo Tipi	Kullanan Projeler	Açıklama
TAB-1	HastaKayıt	Kişisel Sağlık Verileri		
TAB-2	Muayene	Kişisel Sağlık Verileri		
TAB-3	Tahlil	Kişisel Sağlık Verileri		

Veri Tipi	Alan Kodu	Alan	İlişkili?	İlişkili Tablo Kodu	İlişkili Tablo	İlişkili Alan Kodu	İlişkili Alan	QI Tipi
BI	ALAN-1	ID						<Uygulanamaz>
K99	ALAN-2	KV_JMHA						<Uygulanamaz>
K11	ALAN-3	HASTASICILNO						<Uygulanamaz>
K11	ALAN-4	TCKN						<Uygulanamaz>
K10	ALAN-5	ADI						<Uygulanamaz>
K10	ALAN-6	SOYADI						<Uygulanamaz>
K40	ALAN-7	CINSIYET						Kategorik
K40	ALAN-8	DOGUMTARIHI						Kategorik
K40	ALAN-9	UYRUK						?

Kurum Kodu	Paylaş Kurum	Paylaş Tarihi	Paylaş Saati	Paylaşılan Alanlar	Protokol No	Protokol Tarihi	Paylaş Bitiş T	Paylaş Bitiş Saat	Açıklama
24316060	24322010	27.08.2018	21:36:28	TCKN,OGRENIMDURUMU,OGRENCISINIFI	2577	27.08.2018			
24304011	24322010	27.08.2018	21:36:55	TCKN,MESLEK,ISDURUMU,OZURLULUKDURUM	11375	27.08.2018			
24316011	24322010	27.08.2018	21:37:08	TCKN,GELIRDIRLUMU	46898	27.08.2018			
24322010	390779	Veriyi Gönderen: 24316011 - Hazine ve Maliye Bakanlığı		GUVENCEDURUM	24829	27.08.2018			
24322010	243010	Veriyi Alan: 24322010 - Sağlık Bakanlığı			29445	29.08.2018			
24306170	24325150	29.08.2018	14:45:34	CEPTEL,TCKN	12390	29.08.2018			





19-20 Aralık 2018

E-DEVLET AÇISINDAN KVK UYGULAMALARI

Veri haritalama işlemi, kurumlarımız için genelde yeni bir husustur. Örnek olması bakımından, bir hastanedeki hasta, muayene ve tahlil tablolarına ilişkin bir veri haritasının neye benzediğini gösterir örnek görüntü bu sayfada yer almaktadır. Kurumun veri haritalaması yapacağı her bir tablo için, tablodaki her sütunun kategorilenmesi, diğer tablo alanları ile ilişkisi, hangi kurumlara ne kapsamda verildiği ya da hangi kurumlardan alındığı gibi, aslında **verinin takibini kolaylaştıracak bir zincir yönetim modelidir**. Haritalamadan sonra, mevcut yazılımların uyumlandırılması gerekecektir, çünkü mevzuattaki özellikle veri imhası ile ilgili süreçlerin çok pratik olarak yönetilebilmesi için, eğer imkan var ise (kaynak kodlar ya da dokümantasyondan veri yapısına hakimiyet var ise) veri tablolarına bazı güncellemeler yapma gibi imkanlar mevcuttur.

Veri Haritalama Neden Gerekli ?

6698 Sayılı KVKK

Kişisel verilerin silinmesi, yok edilmesi veya anonim hâle getirilmesi

MADDE 7- (1) Bu Kanun ve ilgili diğer kanun hükümlerine uygun olarak işlenmiş olmasına rağmen, işlenmesini gerektiren sebeplerin ortadan kalkması hâlinde kişisel veriler resen veya **ilgili kişinin talebi üzerine** veri sorumlusu tarafından silinir, yok edilir veya anonim hâle getirilir.

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

Madde 12 - (1) b) Kişisel verileri işleme şartlarının tamamı ortadan kalkmış ve talebe konu olan kişisel veriler **üçüncü kişilere aktarılmışsa** veri sorumlusu bu durumu üçüncü kişiye bildirir; **üçüncü kişi nezdinde bu Yönetmelik kapsamında gerekli işlemlerin yapılmasını temin eder.**

Veri haritalama, uygulama sürecinde hayatı çok kolaylaştıracağı için hem GDPR hem de 6698 tarafından öngörülmektedir. Örneğin gerek **saklama yükümlülüklerinin** sona ermesi gerekse ilgilinin **unutulma hakkını** kullanmak istemesi halinde, mevzuatta bu verilerin uygun imha yöntemlerinden birisi ile imha edilmesi gerektiği ve hatta yönetmelikte, bu verinin üçüncü kişilere aktarılması halinde buralar nezdinde de gerekli işlemlerin yapılması yükümlülüğü getirilmiştir. Yoğun veri ortamında **veri yerleşim ve paylaşım zincirini kolayca takip edebilmek için** veri haritalaması bu yükümlülüğün yerine getirilmesinde çok önemli bir araçtır.

Saklama ve İmha: İki Yönlü Yükümlülükler

Tablo Türü	Veri Türü	Mevzuat	Madde	Saklama Süresi	Açıklama
Mali Kayıt-Vergisel Yükümlülükler Bakımından	Defterler	213 sayılı Vergi Usul Kanunu (VUK)	253	5 Yıl	Buldukları yılı takip eden yılın başından itibaren süre başlar * tasfiye ve iflâs idaresi memurları ise görevleri süresince saklamak zorundadır.
Mali Kayıt-Ticari Yükümlülükler Bakımından	Ticari mektup (ticari işe ilişkin tüm yazışmalar), Bilanço, finansal tablo, yıllık faaliyet raporları, Defterlere yapılan kayıtların dayandığı belgeler,	6102 sayılı Türk Ticaret Kanunu (TTK)	82, 68	10 Yıl	
Sosyal Güvence ve Genel Sağlık Sigortası (GSS) bakımından		5510 sayılı SS-GSS	86	10 Yıl (Özel Sektör) /30 Yıl (Kamu Kurumları)	
İnsan Kaynakları ve Özlük bilgileri bakımından	Personel Kayıtları Ücret Kayıtları, Bordrolar Tazminatlara ilişkin tüm belgeler Yıllık izin ücretlerine ilişkin belgeler	4857 sayılı İş Kanunu		5 Yıl	
İş Sağlığı ve Güvenliği ile Borçlar Hukuku bakımından	İş kazası ve meslek hastalığının tespitine ilişkin belgeler	6331 sayılı İş Sağlığı ve Güvenliği Kanunu 6098 Sayılı Türk Borçlar Kanunu (TBK)	TBK: Md 146	10 Yıl	
Sağlık Verileri bakımından	Kişisel Sağlık Verileri	24.11.2017 tarihli Yönetmelik	10 Yıl: Md 9-3	Amaç tamamlanınca ya da ilgili talebi üzerine	Merkezi veri sistemine aktarıldıktan 10 yıl sonra "silinebilir".

Saklama yükümlülüğü ise, maalesef mevzuatımızda tek bir yede toplanmamıştır. Bu konuda bir derlemenin yapılması, kurumların bunları tek tek takibini yapmaması ve gözden kaçırmaları engellemek için önemli bir adımdır. Doktora çalışmamın konusu kişisel verilerin imhası ile ilgili olduğundan böyle bir envanter çalışması gerçekleştirdiğimde gerçekten dağınık bir yapı olduğunu görmüş olduk. KVK Kurumu'nun bu alanda inisiyatif alarak böyle bir çalışmayı (mevzuat derlemesi ve kategorilendirmesi) yaparak kamu ve özel sektöre sunması hem yeknesaklığı sağlayacak, hem de uygulama hatalarını minimuma indirecektir. Bu sayfada, yapılan çalışmadan örnek bir sayfa gösterilmektedir.

6698 ve e-Devlette Kişisel Verilerin Güvenliği

Veri güvenliğine ilişkin yükümlülükler

MADDE 12- (1) Veri sorumlusu;

- Kişisel verilerin hukuka aykırı olarak işlenmesini önlemek,
 - Kişisel verilere hukuka aykırı olarak erişilmesini önlemek,
 - Kişisel verilerin muhafazasını sağlamak,
- amacıyla uygun güvenlik düzeyini temin etmeye yönelik gerekli **her türlü teknik ve idari tedbirleri almak** zorundadır.

SORU: NE KADAR TEDBİR / HANGİ TEDBİRLER



Bazı Sektör temsilcileri tarafından, 5651 döneminde olduğu gibi sayısal bölünmeyi kullanarak bir fırsat dönemi olarak görülebilir



EU: «Birlikte Çalışabilirlik Çerçevesi, entegrasyon güvenliğinde kilit önemdedir»



2012 Mayıs - [Birlikte Çalışabilirlik Esasları Rehberi Sürüm 2.1](#)

Geçmişte Başbakanlık Genelgesine rağmen genellikle **tavsiye niteliğinde görüldü**

- Bu sayfa zaman kısıtı nedeniyle etkinlikte ele alınmamıştır-

Sonuç ve Öneriler



1

RİSK YÖNETİMİ:

- SADECE HİZMET İÇİN ŞART OLAN KİŞİSEL VERİLER'İ ALIN.
- KİMLİK DOĞRULAMA ve E-ÖDEME'DE ULUSAL ALTYAPILARI KULLANIN.

2

VERİ HARİTALAMA MEVZUATTAKİ BİR ÇOK YÜKÜMLÜLÜK İÇİN KİLİT BİR BAŞLANGIÇ AŞAMASIDIR.

3

BAŞARILI UYGULAMA İÇİN ÜST YÖNETİM SAHİPLİĞİ ŞARTTIR. NİTEKİM **VERİ SORUMLUSU** KİMLİĞİ İLE DOĞRUDAN İLİŞKİLİDİR.



akıllı
belediyecilik
zirvesi

Teşekkür Ederim

MUSTAFA AFYONLUOĞLU
Siber Güvenlik, E-Yönetişim ve E-Devlet Kıdemli Uzmanı
<http://afyonluoglu.org>

**E-DEVLET AÇISINDAN
KVK UYGULAMALARI**

19-20 Aralık 2018
MARMARA
BELEDİYELER BİRLİĞİ

Kişisel Verilerin Yönetiminde Sorumluluklar ve Riskler

Hazırlayan : Mustafa AFYONLUOĞLU

Tarih : 19.12.2018

Etkinlik : Akıllı Belediyecilik Zirvesi 2018 (Marmara Belediyeler Birliği – Point Hotel Barbaros İstanbul) <http://www.abz.com.tr/>

Erişim : <http://afyonluoglu.org> → KAYNAKLAR → SUNUMLAR

Telif Hakkı: Aralık 2018, Mustafa Afyonluoğlu

Yayım / Alıntı Şartı: Sunumdan alıntı yapılması için açık referans (Eser Sahibinin Adı Soyadı, Yayınlandığı Web Sayfası Adresi) gösterilmesi zorunludur.

NOT: Bu sunumda herhangi bir kurum temsil edilmemektedir. Tüm görüş ve değerlendirmeler sunumu yapan kişinin uzmanlık değerlendirmeleridir.



akıllı
belediyecilik
zirvesi

19-20 Aralık 2018
MARMARA
BELEDİYELER BİRLİĞİ

MUSTAFA AFYONLUOĞLU
Siber Güvenlik, E-Yönetişim ve E-Devlet Kıdemli Uzmanı

Kişisel Verilerin Yönetiminde Sorumluluklar ve Riskler

Point Hotel Barbaros- İstanbul

<Sosyal Medya – Etkinlik Tanıtım Kartı >