ACCERT
ACCREDITATION – CERTIFICATION

Sektör İncelemeleri - 2

Kişisel Verilerin Korunması

Sağlık

Prof. Dr. Turhan MENTEŞ
Prof. Dr. Mustafa ALKAN
Mehmet Ali İNCEEFE

www.accert.com.tr

Bu Sektör İnceleme Raporu ACCERT A.Ş. Tarafından Hazırlanmıştır.

Ankara Mayıs.2020

ISBN-978-605-06236-0-4

İçindekiler

Önsöz

ACCERT Sektörel İnceleme Raporlarını hazırlayıp yayınlamayı planladığımızda hedefimiz, çeşitli sektörlerin kendisine has yasal ve pratik durumunu kişisel veriler ve mahremiyetin korunması açılarından ele alıp ilgili sektöre bir rehberlik sunabilmekti. Bu kapsamdaki kişisel verilerin işlenmesi ve korunmasına yönelik çok yönlü bir inceleme niteliğindeki ilk raporumuz Denizcilik sektörüne yönelikti.

Bugün, dünya derin ve gerçek anlamda küresel bir salgınla (*pandeminin*) mücadele içerisindedir.

Kişisel veriler ve mahremiyet, bir salgın sırasında hala önemlidir, ancak ortamın hayati koşulları ve ölçeği göz önüne alındığında elbette toplumsal öncelikler değişebilmektedir.

Korona virüsünün yayılmasını kesin verilerle –kişisel sağlık verileri de dâhil- takip etmek, salgının yayılmasını yavaşlatmak için gerekli olduğu kadar da hayati öneme sahiptir. Sağlık uzmanları vakaların ne zaman, nerede ve nasıl yayıldığını veya daraldığını tam olarak bilemedikçe salgını yavaşlatmak veya önüne geçmek neredeyse olanaksızdır.

KVKK'da olmasa da Avrupa'nın Genel Veri Koruma Tüzüğü'ndeki (*GDPR*) açıklamalarında salgınlardan bahsedilmektedir.

Korona virüsü salgını, mahremiyetin korunma şeklini değiştirmeye başlamıştır. Çeşitli veri koruma otoriteleri, kişisel verilerin bu salgın sırasında daha etkin kullanımına ilişkin kurallarını mahremiyetin korunmasından da taviz verilmeden kullanılması için daha fazla görüş ve değerlendirmeler üretmeye başlamışlardır.

Elbette asıl olan hayattır, insan hayatı...

Kişisel verilerin koruması ile salgınla mücadelede kişisel verilerin (*özellikle sağlık verilerinin*) kullanımını bir çatışmaya dönüştürmeye veya kişisel veri korumadan feragat edilmesini gerektiren bir ortam yaratılmasına gerek yoktur.

Teknoloji politikaları ve gizlilik haklarıyla ilgili olan her şey şu anda daha düşük önceliğe sahiptir, ancak kişisel verileri ve mahremiyeti etkileyen koruma ve düzenlemelerin nasıl değiştirildiği konusu yeterince dikkat ve özenle ele alınmazsa, bu durum kurumlara duyulan inanç ve güveni ciddi bir biçimde aşındıracaktır.

Konum takibi, temas izleme gibi insanların uzun süredir endişe duydukları gözetim türleri, bir salgında hastalığın yayılmasını izleme ve önlemede kesinlikle fayda sağlayabilir. Bu tür uygulamaların genişletilmesi, normal şartlar altında kabul edilecek ve desteklenecek bir durum olmamakla birlikte, bir salgında daha az sayıda insanın enfekte olmasını ve salgının yayılmasını azaltmak için bu tür kişisel verilerin kullanılması birçok hayatı kurtaracaktır.

Finlandiya'da, telekomünikasyon işletmecisi Telia, hükümetin virüsle savaşması için gerçek zamanlı, ancak anonimleştirilmiş kullanıcı hareketi verilerini sağlamaktadır.[1]

Bu noktadaki kritik konu, salgın gibi istisnai durumdaki haklar ve imtiyazlar kriz ortadan kalktığında neredeyse eski haline hiç döndürülemediğidir. Özellikle kişisel veriler ve mahremiyet açılarından bu durum, yeni sıkıntıların kaynağı olma olasılığı taşımaktadır.

İşte böyle bir ortamda, sağlık sektöründeki kişisel verilerin, özellikle de kişisel sağlık verilerinin ve mahremiyetin korunmasına yönelik Sektör İnceleme Raporlarımızın 2.sini yayınlamanın, zamanlama açısından çok doğru olduğu düşüncesindeyiz.

Bütün dünyayı istediği gibi yöneteceğini, her istediğini yapabileceğini ve her şeyi düzenleyip, denetleyip, kontrol altına alacağını sanan insanoğlu, aslında bu kadar güçlü olmadığını, aksine evrenin kanunları karşısında ne kadar çaresiz ve zayıf olduğunu da çok acı bir deneyimle görmeye başlamıştır.

Ancak insanlık tarihinin çok önemli olaylarından birisi olan bu "Korona Salgını" bir gerçeği daha net bir şekilde ortaya koydu. Bu gerçek, yakın gelecekte yani korona sonrası dünyada, insanoğlunun hayatının hemen hemen her şeyiyle sayısallaştığı, bir siber hayat ve siber dünya olacağı gerçeğidir.

Yarının "Siber Dünyasında" veri ve bilgi kavramları bugünden daha fazla anlam ve kıymet ifade edecek, bilginin ve verinin korunması ise daha önemli bir hale gelecektir. Kişisel verilerin korunması ve kişisel mahremiyet özelinde ise konu her zamankinden daha başka bir anlam kazanacaktır. Çünkü yeryüzünde yaşayan insanoğlunun tüm kişisel bilgileri, siber dünya içinde dolaşmaya başlayacak ve yeni bir e-insan tipi ortaya çıkacaktır.

[1] https://www.teliacompany.com/en/about-the-company/updates/

Korona sonrası kimler hayatta kalır bilinmez ama bütün insanlığın en az kayıp ve zararla bu süreci atlatacağı umudu ve dileğiyle bu çalışmanın bundan sonraki süreçte insan için önemli bir kaynak olacağı inancını taşıyoruz.

İnsanoğlunun varlığını sürdürmesinde, sağlıklı yaşamasında, mutlu olmasında en büyük paya sahip, başta Türk Hekimleri, sağlık kurumları ve çalışanları olmak üzere, tüm dünya sağlık insanlarına bu vesileyle bir kez daha şükranlarımızı sunuyoruz. Bu raporun sağlık sektörü ve sağlık çalışanları için küçük de olsa bir katkısı olursa kendimizi mutlu hissedeceğiz.

Bundan sonraki süreçte farklı sektörler için hazırlamayı planladığımız Kişisel Verilerin Korunması kapsamındaki sektör inceleme raporlarını da kamuoyuyla paylaşıyor olacağız.

Raporun hazırlanması sürecinde bizlere destek olan ve bu çalışmaya katkı veren tüm kişi ve kuruluşlarımıza teşekkür ediyoruz.

Prof. Dr. Mustafa Alkan / Prof. Dr. Turhan Menteş / Mehmet Ali İnceefe
Mayıs.2020 Ankara

Tanım ve Kısaltmalar

AB	Avrupa Birliği
A.B.D.	Amerika Birleşik Devletleri
Alt Veri İşleyen	Veri işleyen tarafından kendisine verilen yetkiye dayanarak ve yine Veri İşleyen'in talimatları doğrultusunda veri işleme faaliyetleri gerçekleştiren
AT	Avrupa Topluluğu
BT	Bilişim Teknolojileri
CYSH	Cepten yapılan sağlık harcamaları
CCTV	Kapalı Devre Kamera Sistemi (*Closed Circuit Camera System*)
Çalışan	Kurum bünyesinde istihdam edilen gerçek kişi
Direktif	Veri Koruma Direktifi (*95/46/EC Data Protection Directive*)
DTÖ	Dünya Sağlık Örgütü (World Health Organization)
e-Devlet	e-Devlet, vatandaşlara devlet tarafından verilen hizmetlerin elektronik ortamda sunulması
e-Nabız	Kişisel sağlık bilgilerinin yönetebileceği, T.C. Sağlık Bakanlığı kişisel sağlık kaydı sistemidir.
GDPR	Avrupa Genel Veri Koruma Tüzüğü (*General Data Protection Regulation)*
GP	Pratisyen Hekim
GPS	Küresel Konum Sistemi (*Global Positioning System*)
GSYİH	Gayrisafi Yurt İçi Hâsıla
HHS	A.B.D. Sağlık ve İnsan Hizmetleri Bakanlığı (*Department of Health and Human Services*)
HIPAA	Sağlık Sigortası Taşınabilirliği ve Hesap Verebilirlik Yasası (*Health Insurance Portability and Accountability Act*)
ICO	İngiltere Bilgi Komiseri Ofisi (*Information Commissioner's Office*)
İK	4857 Sayılı iş Kanunu
İlgili Kişi	Kişisel verisi işlenen gerçek kişi
JCI	Uluslararası Ortak Komisyon (*Joint Commission International*)
KVKK	6698 sayılı Kişisel Verilerin Korunması Kanunu
KVK Kurumu	Kişisel Verileri Koruma Kurumu
MEDULA	e-Nabız Sistemi
NHS	İngiliz Sağlık Bakanlığı (*National Health Service*)
OCR	Sivil Haklar Ofisi (*Office for Civil Rights*)
OECD	Ekonomik işbirliği ve Kalkınma Teşkilatı (*Organization for Economic Cooperation and Development)*
OHSAD	Özel Hastaneler ve Sağlık Kuruluşları Derneği
PPP	Kamu özel iştirakler
SATURK	Sağlık Turizmi Koordinasyon Kurulu
Sağlık Hizmeti Sunucusu	Sağlık hizmetini sunan veya üreten gerçek kişiler ile kamu hukuku ve özel hukuk tüzel kişilerini
Sağlık.NET	T. C. Sağlık Bakanlığı tarafından "Ulusal Sağlık Bilgi Sistemi" kapsamında yürürlüğe konan internet hizmetleri ağı
SGK	Sosyal Güvenlik Kurumu
SUT	Sağlık Uygulama Tebliği
TBK	6098 sayılı Türk Borçlar Kanunu
TCK	5237 sayılı Türk Ceza Kanunu
TCSB	T.C. Sağlık Bakanlığı
TKHK	Türkiye Kamu Hastaneleri Kurumu
TMK	4721 sayılı Türk Medeni Kanunu
TOBB	Türkiye Odalar ve Borsalar Birliği
TÜİK	Türkiye İstatistik Kurumu
VERBİS	Veri Sorumluları Sicil Bilgi Sistemi
Veri İşleyen	Veri sorumlusunun verdiği yetkiye dayanarak onun adına kişisel verileri işleyen, veri sorumlusunun organizasyonu dışındaki gerçek veya tüzel kişiler

Veri Sorumlusu	Kişisel verilerin işleme amaçlarını ve vasıtalarını belirleyen, veri kayıt sisteminin kurulmasından ve yönetilmesinden sorumlu olan gerçek veya tüzel kişiyi
WHO	Dünya Sağlık Örgütü (*World Health Organization*)
Yönetmelik	T.C. Sağlık Bakanlığı Kişisel Sağlık Verileri Hakkında Yönetmelik

1. Sağlık Sektörü ve Kişisel (Sağlık) Verileri

Günümüzde kişisel verilerin en yoğun kullanıldığı sektörlerin başında sağlık sektörü gelmektedir. Sağlık sektöründe kullanılan verilerin önemli bir bölümünün özel nitelikli kişisel veriler (*kişisel sağlık verileri*) olduğu göz önünde bulundurulduğunda konu daha önemli ve kritik bir hale gelmektedir. Bunun sonucu olarak sağlık kurum ve kuruluşlarının mevcut düzenlemelere uyumluluğu konusu da diğer alanlara göre daha fazla önemli bir duruma gelmektedir. Çünkü bu alanda yaşanacak kişisel veri ihlalleri hem ilgili kişiler için büyük mağduriyetler yaratacak hem de ihlale neden olan kurum ve kuruluşlar için de daha ciddi yasal ve idari sorumluluklar doğuracaktır.

Hem ulusal hem de uluslararası düzenlemelere bakıldığında bu alana yönelik önemli tanımlamalar ve düzenlemeler olduğu görülmektedir. Ülkemizde 7.Nisan.2016 tarihinde yürürlüğe giren 6698 sayılı KVK Kanunun 6. Maddesinde "**özel nitelikli kişisel veriler**"; "*kişilerin ırkı, etnik kökeni, siyasi düşüncesi, felsefi inancı, dini, mezhebi veya diğer inançları, kılık ve kıyafeti, dernek, vakıf ya da sendika üyeliği, sağlığı, cinsel hayatı, ceza mahkûmiyeti ve güvenlik tedbirleriyle ilgili verileri ile biyometrik ve genetik verileri*" olarak tanımlanmıştır.

Uluslararası düzenlemeler arasında en önemlisi olan ve ülke olarak bizim de sorumluluk kapsamına girdiğimiz Avrupa Genel Veri Koruma Tüzüğü'nde ise (*GDPR*) özellikle sağlık sektörü ile ilgili olan üç tür kişisel veri tanımlanmıştır; **sağlıkla ilgili veriler**, **genetik veriler** ve **biyometrik veriler**.

T.C. Sağlık Bakanlığı tarafından 21.Haziran.2019 tarihinde yayınlanan Kişisel Sağlık Verileri Hakkındaki Yönetmelikte de kişisel sağlık verileri; "*Kimliği belirli ya da belirlenebilir gerçek kişinin fiziksel ve ruhsal sağlığına ilişkin her türlü bilgi ile kişiye sunulan sağlık hizmetiyle ilgili bilgiler*" olarak açıklanmıştır.[2]

KVKK/GDPR kapsamında tanımlanmış olan kişisel veriler, çok çeşitli kişi, kurum ve kuruluş tarafından toplanmakta, işlenmekte ve paylaşılmaktadır. Bu denli geniş bir kapsamda ve büyük miktarda toplanıp işlenen ve paylaşılan kişisel verilerin yönetilmesi de oldukça zordur. Bunun tabii sonucu olarak, veri ihlalleri ve saçılma riskleri de artacaktır.

Aşağıda kişisel sağlık verisi toplayan ve işleyen tarafların başlıcaları yer almaktadır:

1) T.C. Sağlık Bakanlığı
2) Hastaneler
3) Eczaneler
4) Doktorlar / Diş Doktorları
5) SGK
6) Sigorta Şirketleri
7) Sağlık Turizmi Yetkili Aracı Kurumlar
8) Şirketler/Kurumlar/Kuruluşlar

T.C. Sağlık Bakanlığı'nın bu alanda yapmış olduğu düzenleme ve çalışmalar incelendiğinde, kişisel sağlık verilerinin merkezi olarak toplanmasının ve yönetilmesinin hedeflendiği görülmektedir. Bu konuya yönelik 3359 sayılı Sağlık Hizmetleri Temel Kanunu;

> *Herkesin sağlık durumunun takip edilebilmesi ve sağlık hizmetlerinin daha etkin ve hızlı şekilde yürütülmesi maksadıyla, Sağlık Bakanlığı ve bağlı kuruluşlarınca gerekli kayıt ve bildirim sistemi kurulur. Bu sistem, e-Devlet uygulamalarına uygun olarak elektronik ortamda da oluşturulabilir. Bu amaçla, Sağlık Bakanlığınca, bağlı kuruluşları da kapsayacak şekilde ülke çapında bilişim sistemi kurulabilir.*

Denilmektedir. Ayrıca, Kişisel Sağlık Verileri Hakkında Yönetmelik'te de Bakanlıkça "*kişisel sağlık verilerinin toplandığı*" bir "*Merkezi sağlık veri sistemi*" kurulması öngörülmüştür. Bu amaçla, tüm sağlık hizmeti sunucularındaki hastane bilgi yönetim sistemleri aracılığıyla bireylere ait tetkik, tanı, teşhis, rapor, reçete

[2] 21 Haziran 2019 tarihli T.C. Sağlık Bakanlığı, Kişisel Sağlık Verileri Hakkında Yönetmelik

gibi her türlü kişisel sağlık verileri merkezi olarak toplanmakta, işlenmekte ve paylaşılmaktadır. Bununla ilgili olarak ta Bakanlık tarafından başta e-Nabız olmak üzere birçok uygulama hayata geçirilmiştir.

Sağlık sektörünün kendi doğası ve ulusal sağlık mevzuatının karmaşık yapısı ulusal ve uluslararası alanda, özellikle de sağlık turizmi kapsamında işlenen ve aktarılan yüksek düzeyde kişisel sağlık verileri açısından da daha kırılgan hale getirmektedir. Özellikle 2016 yılında hem ülkemizde yürürlüğe giren KVKK, hem de AB'de yürürlüğe giren GDPR düzenlemeleri, bu kişisel verilerin toplanması, işlenmesi, paylaşılması ve silinip yok edilmesi konusunda daha katı kurallar, daha ağır yaptırımları ve cezaları gündeme getirmiştir.

GDPR düzenlemeleri, verilerin nerede tutulduğuna bakılmaksızın, Avrupa Birliği'nde yerleşik bir tüzel kişiliği bulunan bir işletme tarafından tutulan AB yerleşik bireylere ait kişisel verilerin, özellikle de kişisel sağlık verilerinin işlenmesi durumunda AB dışındaki kurum ve kuruluşları da kapsamaktadır. **AB'de yerleşik veri sahiplerine mal ve hizmet sağlayan ya da davranışlarını izleyen** AB üyesi olmayan veri sorumlusu ve/veya veri işleyenleri, dolayısıyla **ülkemizdeki sağlık turizmi hizmeti verenler başta olmak üzere tüm sağlık hizmeti sunucularını** da kapsamaktadır.

Sağlık sektörü bu düzenlemelerden etkilenecek olup yeni düzenlemelere en etkili ve verimli biçimde uyumluluk sağlaması gerekmektedir.

Sağlık sektöründe sunulan hizmetlerde, hasta ve yakın bilgileri, bağışçı bilgileri, doktor, hemşire ve çalışan bilgileri, tedarikçi listeleri ve iş bağlantılarının ayrıntıları dâhil olmak üzere çok sayıda kişisel veri toplamaktadır.

Günlük çalışma süreçlerine etkili veri koruma denetimleri uygulamak bazı sıkıntı ve zorluklar getirmektedir, ancak KVKK/GDPR düzenlemeleri yürürlüğe girdiğinden bu yana, kişisel verilerin toplanması, işlenmesi ve paylaşılması, bu düzenlemeler açısından bazı uyumsuzluklara yol açabileceğinden ülkemizde sağlık hizmeti veren kurum ve kuruluşları büyük para cezaları ve itibar kaybı gibi ciddi riskler beklemektedir.

Etkili bir uyumluluk sürecinde ticari faydalar da vardır: hastaların, çalışanlarının ve iş ortaklarının mahremiyetini koruyan ve uygun şekilde hedeflenmiş çalışmalar yürüten sağlık hizmeti sunucularının, iş, personel ve hastalar için daha güvenli ve tercih edilir olmalarını sağlayacaktır.

Düzenlemelere göre sağlık hizmeti sunucuları çoğu durumlarda doğrudan **veri sorumlusu**, bazı durumlarda da **veri işleyen** niteliğini haiz olmaktadır. Bu sağlık hizmeti sunucuları için, gerek doğrudan **veri sorumlusu**, gerekse de **veri işleyen** niteliği ile hem kendisinin eylemlerinden **doğrudan** hem de kişisel verileri paylaştıkları 3. tarafların işleyeceği eylemlerden dolayı **müştereken sorumluluklar** doğmaktadır.

Bu kapsamda, sağlık turizmi de dâhil sağlık hizmeti sunucuları tarafından;

- ✔ Bazı verileri **kanunun açık hükümleri** uyarınca işlemekte,
- ✔ Bazı işlemler için **ilgili kişinin aydınlatılması**,
- ✔ Bazı işlemler için ise **açık rıza alınması,**
- ✔ Ayrıca, bu verilerin yurtdışına aktarılması durumunda bazı **özel işlem** ve **izinlerin alınması** gerekmektedir.

Bu durum, KVKK uyarınca bu sağlık hizmeti sunucuları tarafından, yapılan işlemler ile ilgili çok kapsamlı ve detaylı bir "**envanter**" çıkarılmasını ve "**risk/etki analizlerinin**" yapılmasını gerektirmektedir.

Zira bazı sorumlulukların yerine getirilememesi veya yükümlülüklerin ihlal edilmesi **TCK 135-140** ile düzenlenmiş suçlar bakımından **hapis cezası gerektirmektedir**. Benzer biçimde KVKK 18. maddesindeki kabahatleri işleyen şirketlere **idari para cezaları** uygulanması riski de bulunmaktadır.

Yurtdışına aktarılacak kişisel sağlık verileri ise, KVKK düzenlemelerindeki koşullara ve yerine göre KVK Kurulu'nun iznine tabiidir. Bu nedenle yurtdışına veri aktarımı gerektiren tüm işlem süreçleri de KVKK düzenlemelerine uyum bakımından gözden geçirilmelidir.

Bu örneklerden görüleceği üzere, KVKK uyumluluğu sağlık sektöründe faaliyet gösterenler için hayati önemi haizdir. Aksi takdirde, telafisi mümkün olmayan maddi ve manevi sonuçlar doğuracaktır. Bu sonuçlar, idari para cezaları ve hapis cezaları başta olmak üzere güven ve itibar kayıplarına sebep olacaktır.

Diğer taraftan KVKK sorumluluk ve yükümlülüklerinin yanı sıra, yaptığı iş ve işlemler ile aktardığı veya aktarılan bir takım kişisel verilerden dolayı sağlık hizmeti sunucularının Avrupa Veri Koruma Tüzüğü (GDPR) kapsamına girmeleri de söz konusudur. Bu nedenle GDPR düzenlemeleri gereğince ek bazı teknik, idari ve cezai sorumluluk ve yükümlülükleri de bulunabileceği, GDPR yaptırımlarının sonuçlarının ise daha ağır olduğu göz önünde bulundurulmalıdır.

2. Kişisel Verileri Koruma Kanunu (KVKK)

6698 sayılı Kişisel Verileri Koruma Kanunu 07.Nisan.2016 tarihinde yürürlüğe girmiş ve 07.Nisan.2018 tarihinde 2 yıllık geçiş sürecini de tamamlamıştır. Kanunun **amacı**;

> *"kişisel verilerin işlenmesinde başta özel hayatın gizliliği olmak üzere kişilerin temel hak ve özgürlüklerini korumak ve kişisel verileri işleyen gerçek ve tüzel kişilerin yükümlülükleri ile uyacakları usul ve esasları düzenlemek"*

olarak tanımlanmaktadır. Kanunda "***verilerin işlenmesi***" ise şöyle tanımlanmıştır:

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

Verilerin işlenmesi ile ilgili olarak KVKK ve diğer düzenlemeler kapsamında bir dizi kurumsal ve kişisel sorumluluklar ve yeni ünvanlar getirilmiş ve yükümlülükler de ayrıntılı olarak tanımlamıştır.

Veri Sorumlusu

KVKK'da Veri Sorumlusu; *"Kişisel verilerin işleme amaçlarını ve vasıtalarını belirleyen, veri kayıt sisteminin kurulmasından ve yönetilmesinden sorumlu olan gerçek veya tüzel kişi"* olarak tanımlanmış, ***herhangi bir kişi ya da kurum bu yükümlülükten muaf tutulmamıştır***.

Veri İşleyen

Diğer yandan KVKK, Veri İşleyeni de; *"Veri sorumlusunun verdiği yetkiye dayanarak onun adına kişisel verileri işleyen gerçek veya tüzel kişi"* olarak tanımlamaktadır.

KVKK'nın ilgili tanımlarına göre sağlık sektöründe faaliyet yürüten kurum ve kuruluşları bazı durumlarda doğrudan **veri sorumlusu**, bazı durumlarda da **veri işleyen** niteliğini haiz olmaktadır.

2.1. Yükümlülükler

KVKK'nın 10. ve 12. maddeleri **Veri Sorumlu** ile ilgili yükümlülükleri sıralamıştır:

> ***MADDE 10-****1) Kişisel verilerin elde edilmesi sırasında veri sorumlusu veya yetkilendirdiği kişi, ilgili kişilere;*
>
> *a) Veri sorumlusunun ve varsa temsilcisinin kimliği,*
> *b) Kişisel verilerin hangi amaçla işleneceği,*
> *c) İşlenen kişisel verilerin kimlere ve hangi amaçla aktarılabileceği,*
> *ç) Kişisel veri toplamanın yöntemi ve hukuki sebebi,*
> *d) 11 inci maddede sayılan diğer hakları*
>
> *Konusunda bilgi vermekle yükümlüdür.*

Kişisel verilerin güvenliğine yönelik yükümlülükler:

> ***MADDE 12-*** *1) Veri sorumlusu;*
>
> *a) Kişisel verilerin hukuka aykırı olarak işlenmesini önlemek,*
> *b) Kişisel verilere hukuka aykırı olarak erişilmesini önlemek,*
> *c) Kişisel verilerin muhafazasını sağlamak,*
>
> *Amacıyla uygun güvenlik düzeyini temin etmeye yönelik gerekli* ***her türlü teknik ve idari tedbirleri almak zorundadır****.*

Diğer taraftan denetime yönelik sorumluluklar da *"Veri sorumlusu, kendi kurum veya kuruluşunda, bu* ***Kanun hükümlerinin uygulanmasını sağlamak amacıyla gerekli denetimleri yapmak veya yaptırmak zorundadır****."* olarak açıklanmıştır.

2.2. Yaptırımlar

6698 sayılı kanun, ilgili hükümleri ihlal edilmesi durumunda, ihlalleri niteliğine göre "***suçlar***" ve "***kabahatler***" olarak ayırmış olup, kabahatler için sorumlu kişi veya kurumlara KVKK idari para cezası uygulamayı, söz konusu ihlalin bir kamu kurumu tarafından yapılması durumunda disiplin cezası uygulanması için ilgili kurumun bilgilendirilmesini öngörmektedir.

Kişisel veriler ile ilgili ihlallerin suç niteliğini haiz olması durumunda ise TCK'nın 135-140. maddeleri gereği işlem yapılmasını öngörmektedir.

İdari Para ve Disiplin Cezaları

6698 sayılı kanun kişisel verilere yönelik yükümlülüklerin yerine getirilmemesi durumunda Veri Sorumlusuna **5.000 TL**'ndan **1.000.000 TL**'na kadar **idari para cezası** verilir ve/veya **diğer idari işlemler** uygulanır.

Hapis Cezaları

6698 sayılı kanunun 17. maddesinde kişisel verilere yönelik yükümlülüklerin ihlal edilmesinden kaynaklanacak suçlar için uygulanacak ceza işlemleri aşağıdaki gibi tanımlanmaktadır;

Kişisel verilere ilişkin suçlar bakımından 26/9/2004 tarihli ve 5237 sayılı Türk Ceza Kanununun 135 ila 140. madde hükümleri uygulanır.

- ✓ *Hukuka aykırı olarak kişisel verileri kaydeden kimseye bir yıldan üç yıla kadar hapis cezası,*
- ✓ *Kişisel verileri, hukuka aykırı olarak bir başkasına veren, yayan veya ele geçiren kişi, iki yıldan dört yıla kadar hapis cezası uygulanır.*

Tazminat Hakkı

İdari para ve disiplin cezaları ile hapis cezalarının yanı sıra 6698 sayılı kanunun 14. maddesinin (3). fıkrasına göre "*Kişilik hakları ihlal edilenlerin, genel hükümlere göre **tazminat hakkı** saklıdır.*"

2.3. KVKK Uygulama Örnekleri

6698 sayılı KVKK ile kurulan Kişisel Verileri Koruma Kurumu ve Kurulu bugüne kadar bir dizi ikincil mevzuatı düzenleyip uygulamaya koymuştur. Bu düzenlemeler gereğince bir dizi inceleme ve yaptırımları da uygulamaya başlamıştır.

KVK Kurumu, kuruluşundan bugüne kadar çeşitli uygulamaları ve yaptırımları hayata geçirmiştir. Başlıca ceza gerekçeleri;

- ✓ *Veri Güvenliğine Yönelik Gerekli Teknik ve İdari Tedbirlerin Alınmaması*
- ✓ *Kanuna Aykırı Şekilde Kişisel Verilerin Paylaşılması*
- ✓ *Kişisel Veri Güvenliğinin Sağlanması Amacıyla Uygun Güvenlik*
- ✓ *İlgili Kişinin Verilerinin Silinmesi Talebinin Yerine Getirilmemesi*
- ✓ *Açık Rızanın Hizmet Şartına Bağlanması*
- ✓ *Özel Nitelikli Kişisel Verilerin Kanuna Aykırı Şekilde İnternet ve Sosyal Medya Mecralarında Paylaşılmasıdır.*

Tarih	Veri Sorumlusu / İşleyen	Ceza [TL]	İlgili Maddeler	Açıklamalar
18.09.2019	Facebook	**1.150.000**	m. 12/1 a	Veri Güvenliği için Gerekli İdari ve Teknik Tedbirlerin Alınmaması
16.05.2019	Marriott International In.	**1.000.000**	m. 12/1 a	Veri Güvenliği için Gerekli İdari ve Teknik Tedbirlerin Alınmaması
11.04.2019	Facebook	**1.000.000**	m. 12/1 a	Veri Güvenliği için Gerekli İdari ve Teknik Tedbirlerin Alınmaması
17.08.2019	Dubsmash Inc	**680.000**	m. 12/1 a	Veri Güvenliği için Gerekli İdari ve Teknik Tedbirlerin Alınmaması
11.04.2019	Facebook	**550.000**	m. 12/5	En Kısa Zamanda Bildirimde Bulunmamak
18.09.2019	Facebook	**450.000**	m. 12/5	En Kısa Zamanda Bildirimde Bulunmamak
16.05.2019	Cathay Pacific Havayolu	**450.000**	m. 12/1 a	Veri Güvenliği için Gerekli İdari ve Teknik Tedbirlerin Alınmaması
16.05.2019	Click Bus	**450.000**	m. 12/1 a	Veri Güvenliği için Gerekli İdari ve Teknik Tedbirlerin Alınmaması
27.08.2019	Turizm Şirketi	**400.000**	m. 12/1 a-b-c	Veri Güvenliği için Gerekli İdari ve Teknik Tedbirlerin Alınmaması
16.05.2019	Marriott International In.	**350.000**	m. 12/5	En Kısa Zamanda Bildirimde Bulunmamak
6.02.2020	Banka	**210.000**	m. 12/1 a	Veri Güvenliği için Gerekli İdari ve Teknik Tedbirlerin Alınmaması
27.08.2019	S Şans Oyunları	**150.000**	m. 12/1 a	Veri Güvenliği için Gerekli İdari ve Teknik Tedbirlerin Alınmaması
14.02.2019	Teknik Servis	**150.000**	m. 12/1 a	Veri Güvenliği için Gerekli İdari ve Teknik Tedbirlerin Alınmaması
9.12.2019	Gazete	**125.000**	m. 12/1 a	Veri Güvenliği için Gerekli İdari ve Teknik Tedbirlerin Alınmaması
1.10.2019	Havayolu Taşımacılığı	**100.000**	m. 12/1 a	Veri Güvenliği için Gerekli İdari ve Teknik Tedbirlerin Alınmaması
10.09.2019	Banka	**100.000**	m. 12/1 a	Veri Güvenliği için Gerekli İdari ve Teknik Tedbirlerin Alınmaması
27.08.2019	Turizm Şirketi	**100.000**	m. 12/5	En Kısa Zamanda Bildirimde Bulunmamak
16.05.2019	Cathay Pacific Havayolu	**100.000**	m. 12/5	En Kısa Zamanda Bildirimde Bulunmamak
16.05.2019	Click Bus	**100.000**	m. 12/5	En Kısa Zamanda Bildirimde Bulunmamak
8.07.2019	Yatırım Şirket	**75.000**	m. 12/1 a	Veri Güvenliği için Gerekli İdari ve Teknik Tedbirlerin Alınmaması
26.11.2019	Banka	**70.000**	m. 12/1 a	Veri Güvenliği için Gerekli İdari ve Teknik Tedbirlerin Alınmaması
7.11.2019	Doktor	**50.000**	m. 12/1 a	Veri Güvenliği için Gerekli İdari ve Teknik Tedbirlerin Alınmaması
18.09.2019	Sevinç Eğitim Kurumları	**50.000**	m. 12/1 a	Veri Güvenliği için Gerekli İdari ve Teknik Tedbirlerin Alınmaması
17.08.2019	Dubsmash Inc	**50.000**	m. 12/5	En Kısa Zamanda Bildirimde Bulunmamak
31.05.2019	Avukat	**50.000**	m. 12/1 a	Veri Güvenliği için Gerekli İdari ve Teknik Tedbirlerin Alınmaması
31.05.2019	Şirket	**50.000**	m. 12/1 a	Veri Güvenliği için Gerekli İdari ve Teknik Tedbirlerin Alınmaması
5.03.2019	Teknik Servis	**50.000**	m. 12/1 a	Veri Güvenliği için Gerekli İdari ve Teknik Tedbirlerin Alınmaması
26.11.2019	Banka	**30.000**	m. 12/5	En Kısa Zamanda Bildirimde Bulunmamak
27.08.2019	S Şans Oyunları	**30.000**	m. 12/5	En Kısa Zamanda Bildirimde Bulunmamak
31.05.2019	Varlık Şirketi	**20.000**	m. 12/1 a	Genel Veri İşleme İlkelerine Uyumsuzluk
1.10.2019	Operatör Şirket	Talimat		
1.07.2019	M.S.G.S.Üniversitesi	Disiplin		
25.03.2019	Spor Salonu	İdari Para Cezası		
14.02.2019	Teknik Servis	Linkleri Durdurma		
2.05.2019	Ziraat Bankası	Talimat		

Tablo.1. KVKK tarafından kesilen başlıca idari para cezaları ve gerekçeleri.

3. Avrupa Veri Koruma Tüzüğü (GDPR)

Sağlık sektöründe faaliyet yürüten kurum ve kuruluşların KVKK sorumluluk ve yükümlülüklerinin yanı sıra Avrupa Veri Koruma Tüzüğü (GDPR) gereğince ek bazı teknik, idari ve cezai sorumluluk ve yükümlülükleri de bulunmaktadır.

3.1. Kapsam

AB, GDPR düzenlemelerinin kapsamını AB ülkeleri ile sınırlı bırakmayıp, Avrupa vatandaşları ile ilgili kişisel verilerin işlendiği **Avrupa dışında yerleşik tüm kurum ve kuruluşları** da kapsayacak biçimde genişletmiştir.

3.2. Cezalar

AB, Avrupa Veri Koruma Tüzüğü (GDPR) kapsamında öngörülen idari para cezaları da oldukça ciddi miktarlara ulaşmaktadır;

Bir takım idari yükümlülüklerin yerine getirilmemesi durumunda;

- ***10.000.000 Euro****'ya kadar* ***veya*** *bir teşebbüs olması halinde, bir önceki mali yılın yıllık* ***dünya çapındaki cirosunun %2'sine kadar*** *idari para cezalarına (hangi meblağ yüksek ise, o geçerlidir)*

Bir veri saçılması durumunda ise;

- ***20.000.000 Euro'ya kadar veya bir teşebbüs olması halinde, bir önceki mali yılın yıllık dünya çapındaki cirosunun %4'üne kadar idari para cezalarına*** *(hangi meblağ yüksek ise, o geçerlidir)*

Ülke	Tarih	Ceza [€]	Veri Sorumlusu / İşleyen	İlgili Maddeler (GDPR)	Açıklamalar
İNGİLTERE	8.07.2019	204.600.000	British Airways	m.32	Veri Güvenliği için Gerekli İdari ve Teknik Tedbirlerin Alınmaması
İNGİLTERE	9.07.2019	110.390.200	Marriott International, Inc	m.32	Veri Güvenliği için Gerekli İdari ve Teknik Tedbirlerin Alınmaması
FRANSA	21.01.2019	50.000.000	Google Inc.	m.13, m.14, m.6, m.5	Veri İşleme için Yetersiz Yasal Dayanak
İTALYA	15.01.2020	27.800.000	TIM	m.5, m.6, m.17, m.21, m.32	Veri İşleme için Yetersiz Yasal Dayanak
AVUSTURYA	23.10.2019	18.000.000	Austrian Post	m.5(1) a, m.6	Veri İşleme için Yetersiz Yasal Dayanak
ALMANYA	30.10.2019	14.500.000	Deutsche Wohnen SE	m.5, m.25	Genel Veri İşleme İlkelerine Uyumsuzluk
ALMANYA	9.12.2019	9.550.000	1&1 Telecom GmbH	m.32	Veri Güvenliği için Gerekli İdari ve Teknik Tedbirlerin Alınmaması
İSVEÇ	11.03.2020	7.000.000	Google LLC	m.5, m.6, m.17	Veri Sahibi Hakları Sağlanama Yükümlüğünün Tam Sağlanamaması
BULGARİSTAN	28.08.2019	2.600.000	Ulusal Gelir İdaresi	m.32	Veri Güvenliği için Gerekli İdari ve Teknik Tedbirlerin Alınmaması
HOLLANDA	31.10.2019	900.000	UWV (Çalışan Sigorta Hizmetleri)	m.32	Veri Güvenliği için Gerekli İdari ve Teknik Tedbirlerin Alınmaması
POLONYA	10.09.2019	644.780	Morele.net	m.32	Veri Güvenliği için Gerekli İdari ve Teknik Tedbirlerin Alınmaması
HOLLANDA	3.03.2020	525.000	Royal Dutch Tennis Association ("KNLTB")	m.5, m.6	Veri İşleme için Yetersiz Yasal Dayanak
BULGARİSTAN	28.08.2019	511.000	DSK Bank	m.32	Veri Güvenliği için Gerekli İdari ve Teknik Tedbirlerin Alınmaması
FRANSA	21.11.2019	500.000	Futura Internationale	m.5, m.6, m.13, m.14, m.21	Veri Sahibi Hakları Sağlanama Yükümlüğünün Tam Sağlanamaması
HOLLANDA	18.06.2019	460.000	Haga Hastanesi	m.32	Veri Güvenliği için Gerekli İdari ve Teknik Tedbirlerin Alınmaması
PORTEKİZ	17.07.2018	400.000	Kamu Hastanesi	m.5(1) f, m.32	Veri Güvenliği için Gerekli İdari ve Teknik Tedbirlerin Alınmaması
FRANSA	28.05.2019	400.000	SERGIC (Emlak)	m.32	Veri Güvenliği için Gerekli İdari ve Teknik Tedbirlerin Alınmaması
İNGİLTERE	20.12.2019	320.000	Doorstep Dispensaree Ltd. (Pharmacy)	m.32	Veri Güvenliği için Gerekli İdari ve Teknik Tedbirlerin Alınmaması
İSPANYA	11.06.2019	250.000	Profesyonel Futbol Ligi (LaLiga)	m.5(1) a, m.7(3)	Veri Sahibi Hakları Sağlanama Yükümlüğünün Tam Sağlanamaması
POLONYA	26.03.2019	219.538	Özel Veri Şirketi	m.14	Veri Sahibi Hakları Sağlanama Yükümlüğünün Tam Sağlanamaması
NORVEÇ	29.04.2019	203.000	Oslo Belediyesi Eğitim Birimi	m.32	Veri Güvenliği için Gerekli İdari ve Teknik Tedbirlerin Alınmaması
DANİMARKA	3.06.2019	200.850	IDdesign A / S	m.5(1) e, m.5(2)	Genel Veri İşleme İlkelerine Uyumsuzluk
YUNANİSTAN	7.10.2019	200.000	Telekom Hizmet Sağlayıcısı	m.5(1) c, m.25	Genel Veri İşleme İlkelerine Uyumsuzluk
YUNANİSTAN	7.10.2019	200.000	Telekom Hizmet Sağlayıcısı	m.21(3), m.25	Genel Veri İşleme İlkelerine Uyumsuzluk
ALMANYA	19.09.2019	195.407	Delivery Hero	m.15, m.17, m.21	Veri Sahibi Hakları Sağlanama Yükümlüğünün Tam Sağlanamaması
FRANSA	25.07.2019	180.000	ACTIVE ASSURANCES (Otomobil Sigorta)	m.32	Veri Güvenliği için Gerekli İdari ve Teknik Tedbirlerin Alınmaması
NORVEÇ	2019-03	170.000	Bergen Belediyesi	m.5(1) f, m.32	Veri Güvenliği için Gerekli İdari ve Teknik Tedbirlerin Alınmaması
DANİMARKA	11.07.1905	160.000	Taxa 4x35	m.5(1) e	Genel Veri İşleme İlkelerine Uyumsuzluk
ROMANYA	9.10.2019	150.000	Raiffeisen Bank SA	m.32	Veri Güvenliği için Gerekli İdari ve Teknik Tedbirlerin Alınmaması
LATVIA	2019-11	150.000	Bilinmiyor	m.6	Veri İşleme için Yetersiz Yasal Dayanak
YUNANİSTAN	19.12.2019	150.000	Aegean Marine Petroleum Network Inc.	m.5, m.6, m.32	Veri Güvenliği için Gerekli İdari ve Teknik Tedbirlerin Alınmaması
YUNANİSTAN	30.07.2019	150.000	PWC Business Solutions	m.5(1),5(2), m.6(1), m.13(1)c, m.14(1)c	Veri İşleme için Yetersiz Yasal Dayanak
ROMANYA	27.06.2019	130.000	UNICREDIT BANK SA	m.25(1), m.5(1)c	Veri Güvenliği için Gerekli İdari ve Teknik Tedbirlerin Alınmaması
İSPANYA	27.02.2020	120.000	Vodafone España, S.A.U.	m.5, m.6	Veri İşleme için Yetersiz Yasal Dayanak
ALMANYA	3.12.2019	105.000	Hastane	m.5	Genel Veri İşleme İlkelerine Uyumsuzluk
MACARİSTAN	23.05.2019	92.146	SZIGET ve VOLT festivalleri Organizatörü	m.6, m.5(1)b, m.13	Veri İşleme için Yetersiz Yasal Dayanak
İSPANYA	14.02.2020	80.000	Iberdrola Clientes	m.6	Veri İşleme için Yetersiz Yasal Dayanak
ALMANYA	11.07.1905	80.000	Bilinmiyor	m.32	Yetersiz İdari ve Teknik Veri Güvenliği Tedbirleri
ALMANYA	11.07.1905	80.000	Bilinmiyor	m.32	Yetersiz İdari ve Teknik Veri Güvenliği Tedbirleri
İSPANYA	3.02.2020	75.000	Vodafone España, S.A.U.	m.5, m.6	Veri İşleme için Yetersiz Yasal Dayanak
İSPANYA	3.02.2020	75.000	Vodafone España, S.A.U.	m.5, m.6	Veri İşleme için Yetersiz Yasal Dayanak
İSPANYA	7.01.2020	75.000	EDP España S.A.U.	m.6	Veri İşleme için Yetersiz Yasal Dayanak
İSPANYA	7.01.2020	75.000	EDP Comercializadora, S.A.U.	m.6	Veri İşleme için Yetersiz Yasal Dayanak
LİTVANYA	16.05.2019	61.500	Payment service provider UAB MisterTango	m.5, m.32, m.33	Veri İhlali Bildirim Yükümlülüğünün Tam Olarak Yerine Getirilmemesi
İSPANYA	4.03.2020	60.000	Vodafone España, S.A.U.	m.5, m.6	Veri İşleme için Yetersiz Yasal Dayanak
İSPANYA	3.02.2020	60.000	Xfera Moviles S.A.	m.5, m.6	Veri İşleme için Yetersiz Yasal Dayanak
İSPANYA	3.02.2020	60.000	Vodafone España, S.A.U.	m.5, m.6	Veri İşleme için Yetersiz Yasal Dayanak
İSPANYA	21.11.2019	60.000	Viaqua Xestión Integral Augas de Galicia	m.6	Veri İşleme için Yetersiz Yasal Dayanak
İSPANYA	19.11.2019	60.000	Corporación radiotelevisión espanola	m.32	Veri Güvenliği için Gerekli İdari ve Teknik Tedbirlerin Alınmaması
İSPANYA	19.11.2019	60.000	Xfera Moviles S.A.	m.32	Veri Güvenliği için Gerekli İdari ve Teknik Tedbirlerin Alınmaması
İSPANYA	16.10.2019	60.000	Xfera Moviles S.A.	m.5, m.6	Veri İşleme için Yetersiz Yasal Dayanak
İSPANYA	16.08.2019	60.000	AVON COSMETICS	m.6	Veri İşleme için Yetersiz Yasal Dayanak
İSPANYA	-	60.000	Debt collecting agancy (GESTIÓN DE COBROS, YO COBRO	m.5(1) f	Veri İşleme için Yetersiz Yasal Dayanak
İSPANYA	11.07.1905	60.000	ENDESA (Enerji Dağıtımı)	m.5(1) f	Veri İşleme için Yetersiz Yasal Dayanak
İSPANYA	3.02.2020	50.000	Vodafone España, S.A.U.	m.5	Genel Veri İşleme İlkelerine Uyumsuzluk
SLOVAKYA	-	50.000	Sosyal Güvenlik Kurumu	m.32	Veri Güvenliği için Gerekli İdari ve Teknik Tedbirlerin Alınmaması
İTALYA	17.04.2019	50.000	Italian political party Movimento 5 Stelle	m.32	Veri Güvenliği için Gerekli İdari ve Teknik Tedbirlerin Alınmaması
ALMANYA	03.2019	50.000	N26	m.6	Veri İşleme için Yetersiz Yasal Dayanak
AVUSTURYA	03.2020	50.000	Sağlık Sektöründe Bir Şirket	m.13, m.37	Aydınlatma Yükümlülüğünün Tam Olarak Yerine Getirilmemesi
İSPANYA	28.02.2020	48.000	Vodafone ONO, S.A.U.	m.32	Veri Güvenliği için Gerekli İdari ve Teknik Tedbirlerin Alınmaması
İSPANYA	25.02.2020	48.000	HM Hastaneleri	m.5, m.6	Veri İşleme için Yetersiz Yasal Dayanak
POLONYA	16.10.2019	47.000	ClickQuickNow	m.5	Genel Veri İşleme İlkelerine Uyumsuzluk
İSPANYA	7.01.2020	44.000	Vodafone España, S.A.U.	m.5(1) f	Genel Veri İşleme İlkelerine Uyumsuzluk
İSPANYA	3.03.2020	42.000	Vodafone España, S.A.U.	m.5(1) f, m.32	Veri Güvenliği için Gerekli İdari ve Teknik Tedbirlerin Alınmaması
İSPANYA	14.02.2020	42.000	Vodafone España, S.A.U.	m.5(1) f, m.32	Veri Güvenliği için Gerekli İdari ve Teknik Tedbirlerin Alınmaması
İSPANYA	3.03.2020	40.000	Vodafone España, S.A.U.	m.5, m.6	Veri İşleme için Yetersiz Yasal Dayanak
SLOVAKYA	-	40.000	Slovak Telekom	m.32	Veri Güvenliği için Gerekli İdari ve Teknik Tedbirlerin Alınmaması
İSPANYA	25.10.2019	36.000	Vodafone España, S.A.U.	m.5, m.6	Veri İşleme için Yetersiz Yasal Dayanak
İSVEÇ	16.12.2019	35.000	Nusvar AB	m.6	Veri İşleme için Yetersiz Yasal Dayanak
MACARİSTAN	5.04.2019	34.375	Hugarian political party	m.33(1), m.33(5), m.34(1)	Veri İhlali Bildirim Yükümlülüğünün Tam Olarak Yerine Getirilmemesi
İSPANYA	14.02.2020	30.000	Xfera Moviles S.A.	m.5(1) f, m.32	Veri Güvenliği için Gerekli İdari ve Teknik Tedbirlerin Alınmaması
İSPANYA	14.11.2019	30.000	Telefónica SA	m.5	Genel Veri İşleme İlkelerine Uyumsuzluk
İSPANYA	1.10.2019	30.000	Vueling Airlines	m.5, m.6	Veri İşleme için Yetersiz Yasal Dayanak
İTALYA	23.01.2020	30.000	Azienda Ospedaliero Universitaria Integrata di Verona	m.5(1) f, m.32	Veri Güvenliği için Gerekli İdari ve Teknik Tedbirlerin Alınmaması
İTALYA	23.01.2020	30.000	Sapienza Università di Roma	m.5(1) f, m.32	Veri Güvenliği için Gerekli İdari ve Teknik Tedbirlerin Alınmaması
BULGARİSTAN	26.02.2019	27.100	Telekom Hizmet Sağlayıcısı	m.6, m.5(1) a	Veri İşleme için Yetersiz Yasal Dayanak
İSPANYA	-	27.000	Vodafone España, S.A.U.	m.5(1) d	Veri Sahibi Hakları Sağlanama Yükümlüğünün Tam Sağlanamaması
İSPANYA	3.03.2020	24.000	Vodafone España, S.A.U.	m.5, m.6	Veri İşleme için Yetersiz Yasal Dayanak
İZLANDA	10.03.2020	20.600	National Center of Addiction Medicine ('SAA')	m.5(1) f, m.32	Veri Güvenliği için Gerekli İdari ve Teknik Tedbirlerin Alınmaması
İSPANYA	3.02.2020	20.000	Iberia Lineas Aereas de Espana, S.A. Operadora	m.5, m.6, m.21	Veri İşleme için Yetersiz Yasal Dayanak

Tablo.2. GDPR kapsamında Mayıs.2018 tarihinden itibaren kesilen başlıca idari para cezaları.

4. Sağlık Sektörü ve Kişisel (Sağlık) Verilerini Koruma

Sağlık sektörü, kişisel verilerin en fazla toplandığı, işlendiği ve paylaşıldığı sektörlerden birisidir. Bundan daha da önemlisi, siber saldırıların da en çok hedef aldığı sektörlerden başında gelmektedir. Yapılan araştırmalarda veri ihlalleri konusunda sağlık sektörünün genellikle ilk 3 içerisinde yer aldığı görülmektedir.

Bu durum, siber güvenlik ve kişisel verilerin korunması açılarından sağlık sektörünün en temel sorunlarından ve çözülmesi gereken öncelikli konularından birisi olarak değerlendirilmelidir.

Yapılan siber saldırılar ve veri ihlalleri incelendiğinde, ihlallerin büyük çoğunluğu kurum içi zafiyetlerden kaynaklamaktadır. Başta insan kaynaklı zafiyetler olmak üzere, kurumun bilişim altyapısındaki yetersizlikler, sistemlerdeki yapılandırma hataları, ardından da çalınan veya kaybedilen kayıt ortamları ile bilgisayarlar gelmektedir. Bir diğer önemli husus ise, sağlık kuruluşlarındaki kişisel verilerin maddi çıkar karşılığında ve reklam ve pazarlama amaçlı satışının yapılmasıdır.

Genel olarak bakıldığında, veri ihlalleri sonucunda saçılan verilerin büyük bölümünü *(%72)* **kişisel sağlık verileri** (*özel nitelikli kişisel veriler*) oluşturmaktadır.

Bütün bunlar göstermektedir ki, sağlık hizmet sunucularının KVKK/GDPR düzenlemelerinin gereklerini yerine getirerek, uyumluluk süreçlerini bir an önce tamamlamaları sadece KVKK/GDPR yükümlülükleri açısından değil aynı zamanda kurumsal itibar, hasta güvenliği ile sağlık kurumuna duyulan güven ve maddi kayıplar açısından büyük önem arz etmektedir.

4.1. Kişisel Sağlık Verileri

Kişisel sağlık verileri, hem KVKK hem de GDPR düzenlemelerinde üzerinde hassasiyetle durulan konulardan birisidir. Bu durum, kişisel sağlık verilerini kritik bir veri türü haline getirmektedir. Bu da, sağlık hizmet sunucularının düzenlemelere uyumluluğunu diğer sektörlere göre biraz daha fazla kritik bir noktaya taşımaktadır.

KVKK düzenlemelerinde "özel nitelikli kişisel veriler"; "*kişilerin ırkı, etnik kökeni, siyasi düşüncesi, felsefi inancı, dini, mezhebi veya diğer inançları, kılık ve kıyafeti, dernek, vakıf ya da sendika üyeliği, sağlığı, cinsel hayatı, ceza mahkûmiyeti ve güvenlik tedbirleriyle ilgili verileri ile biyometrik ve genetik verileri*" olarak tanımlanmıştır.

GDPR düzenlemelerinde de sağlık sektörü ile ilgili olan üç tür kişisel veri tanımlanmıştır:[3]

- ***Sağlıkla ilgili veriler:*** *Sağlık hizmetlerinin sağlanması da dâhil olmak üzere bir gerçek kişinin sağlık durumuyla ilgili bilgilerin açıklandığı, söz konusu gerçek kişinin fiziksel veya ruhsal sağlığına ilişkin kişisel verilerdir.*
- ***Genetik veriler:*** *Bir gerçek kişinin fizyoloji veya sağlığı ile ilgili eşsiz bilgiler sağlayan ve özellikle söz konusu gerçek kişiden alınan bir biyolojik numunenin analizinden kaynaklanan ve söz konusu kişinin kalıtım yoluyla alınan veya kazanılan özelliklerine ilişkin kişisel verilerdir.*
- ***Biyometrik veriler:*** *Yüz görüntüleri veya daktiloskopik veriler gibi bir gerçek kişinin özgün bir şekilde teşhis edilmesini sağlayan veya teyit eden fiziksel, fizyolojik veya davranışsal özelliklerine ilişkin olarak spesifik teknik işlemeden kaynaklanan kişisel verilerdir.*

T.C. Sağlık Bakanlığı tarafından 21.Haziran.2019 tarihinde yayınlanan Kişisel Sağlık Verileri Hakkındaki Yönetmelikte de kişisel sağlık verileri; "*Kimliği belirli ya da belirlenebilir gerçek kişinin fiziksel ve ruhsal sağlığına ilişkin her türlü bilgi ile kişiye sunulan sağlık hizmetiyle ilgili bilgiler*" olarak açıklanmıştır.[4]

Düzenlemelerde, hastalığın türü, hastanın ve hastalığın öyküsü, teşhis, tedavi, psikolojik belirtiler, uzuv eksiklikleri, muayene sonuçları, tıbbi tahlil sonuçları, görüntüleme filmleri, kişisel, ailevi, mesleki ve ekonomik duruma ilişkin bütün veriler kişisel sağlık verisi olarak değerlendirilmektedir.

[3] 2016/679 Sayılı Avrupa Genel Veri Tüzüğü (GDPR) m.4: Tanımlar
[4] 21 Haziran 2019 tarihli T.C. Sağlık Bakanlığı, Kişisel Sağlık Verileri Hakkında Yönetmelik

Ayrıca, tıbbi kayıt; hastanın hastalığının seyrini tarif eden periyodik gelişme notları da dâhil olmak üzere hastanın bakımı ile ilgili bütün sağlık disiplinleri tarafından gerçekleştirilen teşhis ve tedavi faaliyetlerinin organize edilmiş raporudur.[5]

4.2. Genel Sağlık Hizmetleri

Türkiye'de sağlık hizmetlerinin sunumunda kamu ağırlıklı olmak üzere, kamu-özel karışımı bir yapılanma söz konusudur. Çok sayıda aktör; koruyucu, tedavi edici, rehabilite edici ve geliştirici sağlık hizmetlerini sunabilmektedir. Ana hizmet sağlayıcıları arasında T.C. Sağlık Bakanlığı, üniversiteler ve özel sektör yer almaktadır. Bakanlık, birinci ve ikinci basamak sağlık hizmetlerinin ana hizmet sağlayıcısı ve aynı zamanda koruyucu sağlık hizmetlerinin de tek sağlayıcısı konumundadır. Bakanlık, hastaneler, klinikler, aile sağlık merkezleri, toplum sağlık merkezleri, dispanserler gibi kapsamlı sağlık hizmetleri tesislerini ve olanaklarını işletmektedir. Üniversite hastaneleri doğaları ve tanımları gereği teorik olarak üçüncü basamak sağlık hizmetleri sunmaları gerekirken, pratikte tüm basamak sağlık hizmetlerini sunabilmektedir. Özel sektör de; hastaneler, klinikler ve poliklinikler, muayenehaneler, eczaneler, laboratuvarlar, tıbbi cihazlar ve ilaç şirketleri aracılığıyla sağlık hizmetlerini üretmektedir. Ayrıca T.C. Milli Savunma Bakanlığı, azınlıklar ve vakıflar da sağlık hizmetlerini sunabilmektedirler.

Türkiye'de mevcut durumda hizmet basamakları arasında zorunlu sevk sistemi bulunmamaktadır. Hastalar istediği basamaktaki sağlık hizmet sunucusuna doğrudan başvurabilmektedir. Bu da beraberinde kaynak israfına yol açabilmekte ve sistemin sürdürülebilirliğini zorlamaktadır.

2003 yılından itibaren uygulanmaya başlanan Sağlıkta Dönüşüm Programı'nın temel bileşenlerinden birisi, birinci basamak sağlık hizmetinin çağdaş uygulama şekli olan aile hekimliğidir.

Genel olarak belirtmek gerekirse Türkiye'deki muayene sayılarının yaklaşık olarak **%40**'ı birinci basamak sağlık hizmetleri (*aile hekimliği*), **%40**'ı Bakanlık hastaneleri, **%15**'i özel sağlık kuruluşları ve **%5**'i de üniversite hastanelerinde olmaktadır.

Meslekler	2014	2015	2016	2017	2018
Uzman Hekim	75.251	77.622	78.620	80.951	82.894
Pratisyen Hekim	39.045	41.794	43.058	44.649	44.053
Asistan Hekim	21.320	21.843	23.149	24.397	26.181
Toplam Hekim	**135.616**	**141.259**	**144.827**	**149.997**	**153.128**
Toplam Diş Hekimi	22.996	24.834	26.674	27.889	30.615
Eczacı	27.199	27.530	27.864	28.512	32.032
Hemşire	142.432	152.803	152.952	166.142	190.499
Ebe	52.838	53.086	52.456	53.741	56.351
Diğer Sağlık Personeli	138.878	145.943	144.609	155.417	177.409
Diğer Personel ve Hizmet Alımı	303.110	311.337	321.952	339.241	376.367
Toplam Personel	823.069	856.792	871.334	920.939	1.016.401

Tablo.3. Yıllara Göre Sağlık Personeli Sayıları, Tüm Sektörler[6]

Bugün itibariyle **8.000** Aile Sağlığı Merkezinde yaklaşık **25.000** aile hekimi görev yapmaktadır. Türkiye'de toplam sağlık personeli sayısı **1.000.000**'u geçmiştir. Tüm bu sağlık profesyonelleri, aynı zamanda başta **kişisel sağlık verileri** olmak üzere birçok kişisel veri türünü işlemekte ve kullanmaktadır.

Sağlık personeli genellikle kişisel verileri kurumsal yapılar içinde işlemektedirler.

[5] TSE, Hastane Akreditasyon Tasarısı 1996
[6] T.C. Sağlık Bakanlığı Sağlık İstatistikleri Yıllığı 2018

Ancak hekime görünme sayılarında yıllar itibari ile artış görülmekte, bu ise 2018 rakamlarıyla neredeyse yıllık kişi başı 10 görünme seviyesine ulaşmıştır. Başka bir deyişle ortalama herkes yılda 10 kere hekime gitmektedir.

Kurumlar	2014	2015	2016	2017	2018
T.C. Sağlık Bakanlığı	3,8	3,9	4,3	4,4	4,6
Üniversite	0,4	0,4	0,5	0,5	0,5
Özel	0,9	1,0	0,9	0,9	0,9
Toplam	**1,9**	**5,1**	**5,3**	**5,6**	**5,8**

Tablo.4. Yıllara ve Sektörlere Göre Hastanelere Kişi Başı Müracaat Sayısı[7]

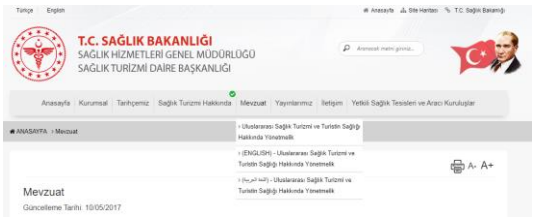
Kurumlar	2014	2015	2016	2017	2018
Aile Hekimliği	214.120.750	208.538.951	205.549.931	228.098.527	258.436.607
Verem Savaş Dispanseri	1.643.937	1.495.558	1.374.153	1.391.817	1.332.580
ÇEKÜS Birimi	660.056	548.433	525.011	646.856	366.095
TSM'ler Tarafından Yapılan Diğer Muayeneler	2.234.348	3.457.520	8.080.631	4.496.425	4.821.348
Özel Poliklinikler	546.514	523.694	461.013	501.993	539.593
Birinci Basamak Toplamı	219.205.605	214.564.156	215.990.739	235.135.618	265.496.223
Özel Tıp Merkezleri	28.208.781	26.953.360	22.069.610	18.912.829	19.055.722
Hastaneler	396.577.644	418.581.931	447.648.830	464.876.362	497.963.259
Sağlık Bakanlığı	292.100.331	306.825.524	340.080.539	353.703.814	380.623.055
Üniversite	32.143.930	34.539.363	36.420.413	38.963.933	42.665.139
Özel	72.333.383	77.217.044	71.147.878	72.208.615	74.675.065
2. ve 3. Basamak Toplamı	424.786.425	445.535.291	469.718.440	483.789.191	517.018.981
Genel Toplam	**643.992.030**	**660.099.447**	**685.709.179**	**718.924.809**	**782.515.204**

Tablo.5. Yıllara ve Kurum Türlerine Göre Toplam Hekime Müracaat Sayısı, Tüm Sektörler[8]

Kişisel verilerinin en çok işlendiği sektörlerden birisi sağlık sektörüdür. Veri türü çeşitliliğini de göz önüne alınırsa büyük veri olarak tanımlanabilecek bir yapı mevcuttur. Bu denli büyük veri toplama, işleme ve paylaşımının yapıldığı bir alanda, kişisel verilerin özellikle de kişisel sağlık verilerinin saçılma riski çok olup, bu verilerin güvenliğinin sağlanması ve korunması önemli bir çaba ve kaynak gerektirmektedir.

4.3. Sağlık Turizmi

Sağlık turizmi, 5510 Sayılı Sosyal Sigortalar ve Genel Sağlık Sigortası Kanunu ve milletlerarası ikili mütekabiliyet anlaşmaları kapsamına girmeyen, ancak; yurtdışından sağlık hizmeti almak amacıyla ülkemize gelenler ile turist olarak ülkemizde bulunduğu sırada sağlık hizmeti ihtiyacı ortaya çıkan kişilere kamu, üniversite ve özel sağlık kurum ve kuruluşları ile aracı kuruluşları aracılığıyla sunulacak sağlık hizmetidir.[9]



Avrupa Komisyonu'nun Türkiye ile "**hizmetlerin serbest dolaşımı müzakereleri**"ne ilişkin olarak hazırladığı bir taslak raporda hizmet sektörleri arasında sağlık hizmetleri öncelikli yer almıştır.[10]

Sağlık Turizmi, T.C. Sağlık Bakanlığı tarafından düzenlenmiş özel bir sağlık hizmetleri alanıdır. Sağlık turizmi;

- Yaşlı ve engelli turizmi[11] (*gezi turları, meşguliyet terapileri, rehabilitasyon ve özel bakım hizmetleri*)
- Termal Turizm ve SPA-Wellnes[12] (*Kaplıca tedavileri ve fizyoterapiler, Hidroterapi, Balneoterapi vb.)*
- Medikal Turizm (*Kardiyovasküler Cerrahi, Radyoterapi, Tüp bebek, Estetik Cerrahi, Göz-Diş tedavileri*)

hizmetlerini kapsamaktadır.

[7] T.C. Sağlık Bakanlığı Sağlık İstatistikleri Yıllığı 2018
[8] T.C.Sağlık Bakanlığı Sağlık İstatistikleri Yıllığı 2018 s.119
[9] https://dosyamerkez.saglik.gov.tr/Eklenti/28811,saglik-turizmi-yonetmelikpdf.pdf?0
[10] Uluslararası Ticarette Hizmet Sektörü, https://dosyamerkez.saglik.gov.tr/Eklenti/10946,04pdf.pdf?0
[11] https://saglikturizmi.saglik.gov.tr/TR,183/ileri-yas-ve-engelli-turizmi.html
[12] https://saglikturizmi.saglik.gov.tr/TR,183/termal-saglik-turizmi-ve-spa-wellness.html

Sağlık turizmi kapsamında en çok turist Azerbaycan, Almanya, İngiltere, Gürcistan ve İran'dan gelmiş olup, bu ülkeleri İspanya, Hollanda, Bulgaristan, Fransa, Rusya, A.B.D., İtalya, Yunanistan ve İsveç takip etmiştir.

Bu amaçla Sağlık Turizmi Koordinasyon Kurulu (SATURK) kurulmuş, ayrıca SATURK aracılığıyla tek elden organize edilecek ülkemiz sağlık sistemine güveni tesis etmeye odaklanmış "*TURKEY Destination Health*" çalışmaları başlatılmıştır.

2018 yılında Türkiye'ye sağlık ve tedavi amacıyla gelen **551.748 ziyaretçi**, kişi başı ortalama **2.013 $** seviyesinde harcama gerçekleştirmiştir.[13]

20.03.2020 tarihi itibari ile uluslararası sağlık turizmi yetki belgesi almaya hak kazanmış olan sağlık tesisleri ve aracı kuruluşları sayıları aşağıdaki gibidir;[14]

Kamu Sağlık Tesisleri 127
Kamu Üniversite Hastaneleri 24
Vakıf Üniversite Hastaneleri 24
Özel Sağlık Tesisleri 679
Aracı Kuruluş 105
Toplam 959

Bakanlık, "*sağlık hizmeti almak amacıyla Türkiye'ye gelen yabancıların aldıkları sağlık hizmetinin sonucunda veya seyahat sürecinin her hangi bir basamağından kaynaklanan taraf olduğu hukuki olay veya işlemler neticesinde değişik boyutları olan hukuki problemlerin çıkması kaçınılmaz olduğunu*" düşünmektedir.[15]

Ayrıca sağlık turizmi ticari bir sektör olarak uluslararası ticaretin parçasıdır ve özellikle sigorta geri ödeme sistemleri ile yapılacak anlaşmalar nedeniyle uluslararası ticari hukukun da ilgi alanına girmektedir. [16]

Bu durum, hızla gelişen bir sektör olarak sağlık turizmini, özellikle AB ile KVKK/GDPR düzenlemeleri kapsamında da gündeme getirmektedir.

GDPR bölgesel kapsamı açısından, hizmetlerin AB yerleşik veri sahiplerini **hedefleme kriterlerinin** varlığı en kritik uygulama esaslarından birisidir. Hedefleme kriterinin uygulanması, kişisel verileri işlenen veri sahibinin vatandaşlığı, ikametgâhı veya diğer yasal statüsü ile sınırlı değildir.[17] GDPR tarafından sağlanan korumanın, "*kişisel verilerinin işlenmesi ile ilgili olarak milliyetleri veya ikamet yerleri ne olursa olsun gerçek kişiler için geçerli olması gerektiğini*" belirtir.[18]

Diğer taraftan hizmet teklifi ve işlem faaliyetleriyle ilgili olarak; hizmetin, AB'deki kişileri yanlışlıkla veya tesadüfen değil, özellikle hedeflemesi, söz konusu hizmetleri ve hizmet sağlayanları doğrudan GDPR yükümlüsü hâline getirmektedir.[19]

Nitekim Yönetmelik, sağlık turizmi hizmetlerinin sunulabilmesi için koyduğu yeterlilik kriterleri içerisinde, "*İngilizceden veya hizmet sunulacak uluslararası* ***sağlık turistinin dilinden Avrupa Dil Portfolyosunda*** *yer alan B2 dil düzeyini gösterir belgeye sahip olmayı*" şart koşmaktadır.[20]

Ayrıca, sağlık turizmi hizmeti sunacakların "*tanıtımları, tanıtım yapılacak ülkelerin dilleri ve/veya İngilizce dilinde yapılabilme*" koşulu da sağlık turizmi hizmeti sunacakların GDPR kapsamında "*AB'de bir temsilci tayin etmesi*" de dâhil tüm yükümlülükleri yerine getirmeleri gerekmektedir.

[13] https://www.medimagazin.com.tr/guncel/genel/tr-saglik-turizmi-icin-gelen-normal-turistten-3-kat-daha-fazla-harciyor-11-681-82626.html
[14] https://saglikturizmi.saglik.gov.tr/
[15] Sağlık Turizmi Hukuku, https://dosyamerkez.saglik.gov.tr/Eklenti/10954,12pdf.pdf?0
[16] Sağlık Turizmi Hukuku, https://dosyamerkez.saglik.gov.tr/Eklenti/10954,12pdf.pdf?0
[17] Guidelines 3/2018 on the territorial scope of the GDPR (Article 3) Version 2.1 12 November 2019
[18] Avrupa Veri Koruma Tüzüğü GDPR Açıklama.14
[19] Guidelines 3/2018 on the territorial scope of the GDPR (Article 3) Version 2.1 12 November 2019
[20] https://dosyamerkez.saglik.gov.tr/Eklenti/28811,saglik-turizmi-yonetmelikpdf.pdf?0

4.4. KVKK/GDPR ve Sağlık Sektöründeki Yükümlülükler

KVKK düzenlemelerine göre, sağlık hizmetleri ile ilgili işlemlerde işlenen kişisel veriler bakımından **sağlık hizmetleri sunucuları** veri sorumlusudur.

Sağlık hizmetleri sunucuları genel olarak işlediği kişisel veriler (*örneğin, personel kayıtları ve hasta kayıtları*) ile ilgili olarak **veri sorumlusu** iken, 3. taraflardan alarak kendi bilişim sisteminde kaydedip saklamakta olduğu kişisel veriler için de bir **veri işleyen** konumundadır.

Veri sorumlusu sıfatıyla sağlık hizmet sunucuları Kişisel Verilerin Korunması Kanunu'nda sayılan "*ilkeler*"e ve "*veri işleme şartları*"na eksiksiz uymakla yükümlüdürler. Örneğin, kanunlarda "*açıkça*" öngörülen hallerde kişisel verilerin ilişkili olduğu kişinin *(ilgili kişi*) "açık rızası"nı almadan veri işleyebilecektir. Bunun gibi Kanun'da sayılan istisnai işleme şartlarından herhangi birinin bulunmaması halinde ise veriyi işleyebilmek için ilgili kişinin açık rızasının alınması bir zorunluluktur.

Kişisel sağlık verileri öncelikle ilgili sağlık hizmeti sunucuları tarafından toplanıp işlenmekte ve bu veriler T.C. Sağlık Bakanlığı ve Sosyal Güvenlik Kurumu (SGK) ile paylaşılmaktadır.

3359 Sayılı Sağlık Hizmetleri Temel Kanunu; "*herkesin sağlık durumunun takip edilebilmesi ve sağlık hizmetlerinin daha etkin ve hızlı şekilde yürütülmesi maksadıyla, T.C. Sağlık Bakanlığı ve bağlı kuruluşlarınca gerekli kayıt ve bildirim sistemi kurulmasını*" hükmetmektedir.

Bu sistemin, "*e-Devlet uygulamalarına uygun olarak elektronik ortamda da oluşturulması*" ve buna yönelik olarak T.C. Sağlık Bakanlığı, bağlı kuruluşlarını da kapsayacak şekilde ülke çapında bilişim sistemi kurmuştur.

Diğer taraftan, 663 sayılı KHK'nın 47. maddesine göre "*Bakanlık ve bağlı kuruluşları, mevzuatla kendilerine verilen görevleri, e-devlet uygulamalarına uygun olarak daha etkin ve hızlı biçimde yerine getirebilmek için, bütün kamu ve özel sağlık kurum ve kuruluşlarından; sağlık hizmeti alanların, aldıkları sağlık hizmetinin gereği olarak ilgili sağlık kurum ve kuruluşuna vermek zorunda oldukları **kişisel bilgileri** ve bu kimselere verilen hizmete ilişkin bilgileri her türlü vasıtayla **toplamaya, işlemeye** ve **paylaşmaya***" yetkilendirilmiştir.

Herkesin sağlık durumunun takip edilebilmesi amacıyla "*sağlık kurumlarında elektronik ortamda **üretilen verileri, doğrudan üretildikleri yerden, standartlara uygun şekilde toplamayı, toplanan verilerden tüm paydaşlar için uygun bilgiler üreterek** birinci, ikinci ve üçüncü basamak sağlık hizmetlerinde verim ve kaliteyi arttırmayı hedefleyen, entegre, güvenli, hızlı ve genişleyebilen bir bilgi ve iletişim platformu*" olarak Sağlık.NET kurulmuştur.

T.C. Sağlık Bakanlığı'nın, sağlık verilerinin paylaşımı konusu, 21.06.2019 tarihli "*Kişisel Sağlık Verileri Hakkında Yönetmelik*" ile düzenlenmiştir. Buna göre Yönetmelikte belirtilen koşulları yerine getirmeleri durumunda; kişisel sağlık verilerine;

- ✓ Sağlık personeli
- ✓ Bakanlık birimleri
- ✓ Hasta yakınları
- ✓ Avukatları

erişebilmektedir. Çocukların sağlık verilerine ise, ebeveynler, bu verilere çocukların kendisinden herhangi bir onaya ihtiyaç duymaksızın e-Nabız üzerinden erişebilir.

Görüleceği üzere, varlığı Bakanlık altında olmayan, ayrı bir tüzel kişiliğe sahip olan tüm sağlık hizmeti sunucuları da, verdikleri sağlık hizmeti sürecinde topladıkları tüm kişisel veri ile kişisel sağlık verilerini Bakanlıkla paylaşmak zorundadırlar. Bu durum, Bakanlık'ın KVKK ve GDPR açısından hem **veri sorumlusu** hem de **veri işleyen** konumuna getirmektedir.

T.C. Sağlık Bakanlığı'nın yanı sıra, SGK da "*Sosyal Güvenlik Kurumu Verilerinin Kullanımına, Paylaşılmasına Ve Korunmasına İlişkin Usul ve Esaslar*" kapsamında **sağlık verilerinin paylaşımını** gerçekleştirmektedir.

5502 sayılı Kanunun 35. maddesinde "*Kurum, bu Kanun ve diğer kanunlarla verilen görevleri yerine getirmek amacıyla işlediği kişisel veriler ile ticari sır niteliğinde olan verileri, veri sahibinin noter onaylı muvafakati olmadan gerçek veya tüzel kişilerle paylaşamaz.*" hükmü yer almaktadır.

Bu konuya bazı istisnalar getirilmiştir. 5018 sayılı Kamu Malî Yönetimi ve Kontrol Kanununda yer alan bazı hükümlerde, "*kamu idarelerinin kanunlarında belirtilen görevleri yapabilmeleri için ihtiyaç duydukları sağlık verisi dışındaki kişisel veriler ile ticari sır niteliğindeki veriler paylaşılabilir.*" denilmektedir. Ayrıca "*bunların dışındaki gayri maddi hakları ile kimliği belirli veya belirlenebilir bir gerçek veya tüzel kişiyle ilişkilendirilemeyecek şekilde anonim hâle getirdiği verileri araştırma, planlama ve istatistik gibi amaçlar için kamu idareleri, bilimsel araştırma yapan kamu personeli, bilimsel dernekler, kamu kurumu niteliğindeki meslek kuruluşları veya üniversiteler ile ücretsiz olarak paylaşabilir.*" hükmü yer almaktadır.

Bir diğer istisnai durum ise, "*Anonim hâle getirilen verinin tüzel kişilere ait olması hâlinde bu fıkrada sayılanlar dışındaki gerçek veya tüzel kişilere tüzel kişinin noter onaylı muvafakati alınmak kaydıyla ücretli olarak verilebilir.*" şeklinde düzenlenmiştir.

Ancak bu istisnaların yanında düzenleme kurumlara veri güvenliği konusunda yükümlülükte getirmektedir. Düzenlemede "*Veri paylaşılan kamu idareleri ile gerçek ve tüzel kişiler, **paylaşılan verinin gizliliğinden** ve **güvenliğinden sorumludur**. Bu fıkranın aksine davrananlar hakkında, veri paylaşımı yapılanlar da dâhil olmak üzere 5237 sayılı Türk Ceza Kanunu ile diğer ilgili mevzuat hükümleri uygulanır.*" denilmektedir.

SGK'nın "*Verilerinin Kullanımına, Paylaşılmasına ve Korunmasına İlişkin Usul ve Esaslar*"ında veri sahiplerine de yönelik hükümler yer almaktadır. Bu düzenlemenin 11. Maddesinde veri sahiplerinin haklarına yer verilmektedir. Bu maddede aşağıdaki haklar yer almaktadır. Buna göre herkes, "*Kuruma başvurarak kendisiyle ilgili;*

- *Kişisel sağlık verisinin işlenip işlenmediğini öğrenmek,*
- *Verileri işlenmişse buna ilişkin bilgi talep etmek,*
- *Verilerin eksik veya yanlış olması hâlinde bunların düzeltilmesini istemek*

hakkına sahiptir."

Ayrıca Kurum, kişisel sağlık verilerini;

- Kişinin kendisi veya kişinin **noter onaylı açık rızası** ile diğer **gerçek** veya **tüzel kişiler**,
- **Mahkeme kararı** ile kişinin verilerine **erişim izninde yetkilendirilmiş** kişiler,
- Müvekkili tarafından verilen **vekâletnamede** avukatın kişisel sağlık verilerini talep edebileceğinin belirtilmiş olması şartıyla ilgili **avukatı** ile ücretsiz olarak **paylaşabilir** veya gerekçesini açıklanarak veri taleplerini reddedebilir.

Aynı düzenlemenin 12. Maddesinde, Sözleşmeli sağlık hizmeti sunucularının, sundukları hizmetlere ilişkin veri talepleri konusu yer almaktadır. Bu maddeye göre Sağlık hizmet sunucularının, Kurum Bilgi İşlem Sistemine gönderdiği verilerden mücbir sebeplerle Kuruma faturalandırılamayanlar, "*Veri Paylaşım Komisyonunca değerlendirilerek uygun görülmesi halinde* sadece *ilgili **sağlık hizmeti sunucusu ile paylaşılabilir**.*" hükmü yer almaktadır.

Benzer şekilde düzenlemenin 13. ve 14. maddelerinde 3. taraflarla veri paylaşımı konusu yer almaktadır. 13. madde de Adli mercilerin sağlık verisi talepleri, "*Cumhuriyet savcıları, hâkimlikler veya mahkemeler tarafından talep edilen **her türlü sağlık verisi** ücretsiz olarak karşılanır.*" şeklinde düzenlenmiştir. Benzer şekilde 14. madde de Kamu idarelerinin kanunlarında belirtilen görevleri yapabilmelerine yönelik sağlık verisi talepleri: 5018 sayılı Kamu Malî Yönetimi ve Kontrol Kanununun eki (I), (II), (III) ve (IV) sayılı cetvellerde yer alan kamu idarelerinin kanunlarında belirtilen görevleri yapabilmeleri için ihtiyaç duydukları verilerden;

- Kişisel sağlık verisi hiçbir şekilde paylaşılmaz.

- ✔ Kişisel sağlık verisi içermeyecek şekilde anonim hale getirilmiş veriler ile kişisel sağlık verisi dışındaki ticari sır niteliğindeki veriler ücretsiz paylaşılabilir veya gerekçesi açıklanarak reddedilebilir, şeklinde düzenlenmiştir.

Araştırma, planlama ve istatistik amaçlı sağlık verisi talepleri 15. Maddede yer almaktadır. Bu maddeye göre;

"Kamu idarelerinin araştırma, planlama ve istatistik amaçlı veri talepleri ile bilimsel araştırma yapan kamu personeli, bilimsel dernekler, kamu kurumu niteliğindeki meslek kuruluşları veya üniversitelerin araştırma, planlama ve istatistik amaçlı ihtiyaç duydukları sağlık verisi talepleri;

- ✔ *Veri Paylaşım Komisyonunca değerlendirilerek uygun görülmesi halinde,*
- ✔ *Kişisel sağlık verisi ve ticari sır niteliğinde veri içermemesi,*

şartıyla ücretsiz karşılanır."

Bu maddelerde belirtilen hususlarla ilgili veri paylaşım kriterlerini belirlemek üzere "Veri Kontrol Komisyonu" kurulmuştur.

Veri Kontrol Komisyonu; "*Sağlık verilerinin anonimleştirilmesi için her bir veri talebine yönelik anonimleştirme kurallarının belirlenmesi ve anonimleştirilmiş verilerin gereken gizliliği sağlayıp sağlamadığı açısından kontrol edilmesi konusunda görev ve yetkiye sahiptir*."

Veri Paylaşım Komisyonu, 15. madde kapsamındaki veri talebine esas çalışmanın,

- ✔ Ülkemiz ve Kurum sağlık stratejileri ve hedeflerinin gerçekleştirilmesine katkısı,
- ✔ Genel Sağlık Sigortası uygulamalarının geliştirilmesine etkisi ve Kurumsal öncelikler,
- ✔ Verilerin ayrı veya özel bir çalışma, araştırma, inceleme ya da analiz neticesinde oluşturulabilecek nitelikte olup olmadığı

gibi ölçütlere göre değerlendirerek karar vermektedir.[21]

Yukarıdaki açıklamalardan anlaşılacağı üzere, sağlık hizmeti sunucularının verdikleri sağlık hizmeti sürecinde topladıkları kişisel veriler ile kişisel sağlık verilerini doğrudan veya dolaylı olarak SGK ile paylaşmak durumundadırlar. Bu durum SGK'yı da KVKK ve GDPR açısından hem **veri sorumlusu** hem de **veri işleyen** konumuna getirmektedir.

Veri sorumlusu sıfatıyla sağlık hizmeti sunucuları Kişisel Verilerin Korunması Kanunu'nda sayılan "*ilkeler*"e ve "*veri işleme şartları*"na eksiksiz uymakla yükümlüdürler. Kanun'da sayılan istisnai işleme şartlarından herhangi birinin bulunmaması halinde ise ilgili kişinin verisinin işlenebilmesi ve özellikle **paylaşılabilmesi** için gerekli aydınlatmaların çok dikkatli bir biçimde yapılması ve gerekli durumlarda ilgili kişinin **açık rızasının** alınması bir zorunluluktur.

2014 tarihli Sağlık Çalışanları ile ilgili Yönetmelikte tüm sağlık çalışanlarının "*Mesleki uygulamalar sırasında edindiği kişisel verileri ve sağlık ile ilgili özel bilgileri, ilgili mevzuat gereği rapor düzenleme ve hastanın ya da diğer kişilerin hayati tehlikesi söz konusu olduğu durumlar hariç,* ***muhafaza eder ve üçüncü kişilerin eline geçmemesi için gerekli tedbirleri*** *alır.*" hükmü yer almaktadır.

KVKK 6. Maddesinin (3). Fıkrasında; "*Sağlık ve cinsel hayata ilişkin kişisel veriler ise ancak kamu sağlığının korunması, koruyucu hekimlik, tıbbî teşhis, tedavi ve bakım hizmetlerinin yürütülmesi, sağlık hizmetleri ile finansmanının planlanması ve yönetimi amacıyla,* ***sır saklama yükümlülüğü*** *altında bulunan kişiler veya yetkili kurum ve kuruluşlar tarafından ilgilinin açık rızası aranmaksızın işlenebileceğine."* hükmedilmiştir.

GDPR düzenlemelerinde, başta doktorlar olmak üzere sağlık hizmeti sunanlar "***mesleki gizlilik yükümlülüğü***" meslek grubunda yer alan kişiler olarak[22], kişisel sağlık bilgilerini "*tıbbi tanı, sağlık veya sosyal bakım hizmetlerinin veya tedavinin sağlanması ya da sağlık veya sosyal bakım sistemleri ve hizmetlerinin yönetilmesi*

[21] Veri Paylaşımı, Op.Dr.Mustafa Öztürk SGK Genel Sağlık Sigortası Genel Müdürlüğü 2 Haziran 2016
[22] Avrupa Genel Veri Tüzüğü (GDPR), m.9 (3)

açısından işleme faaliyetinin gerekli olması"[23] durumunda, veri sahibinden rıza almadan işleyebilecekler arasında tanımlanmıştırlar.

KVKK, sağlık mevzuatında yer alan ***sır tutma*** sorumluluklarına ek olarak bir dizi yeni yükümlülükler getirmiştir.

Ardından Bakanlık'ın "*Kişisel Sağlık Verileri Hakkında Yönetmelik*" KVKK'da belirtilen "*özel nitelikli kişisel veriler*" kapsamındaki "***kişisel sağlık verilerini***" özel olarak düzenlemiştir.

Veri sorumlusunun yükümlülükleri, koşulları oluştuğunda kişisel verilerin "silinmesi", "yok edilmesi" veya "anonim hale getirilmesi"ni de içermektedir. Keza, Kanun kişisel verilerin yurt içinde veya yurt dışına aktarılması bakımından (*örneğin, doktorlar arasında, hastaneler arasında, kamu-özel üçüncü kişiler arasında, başka ülkelere (konsolosluklara) veri gönderilmesi esnasında*) ek yükümlülükler getirmekte, hatta belirli durumlarda Kişisel Verilerin Korunması Kurulu'nun iznini şart koşmaktadır.

Sağlık hizmeti sunucuları kişisel verileri işlenen gerçek kişilere *(ilgili kişi*) yönelik doğrudan yükümlülükleri de bulunmaktadır. İlgili kişilerin kendileriyle ilgili olarak işlenen veriler bakımından tam ve doğru şekilde doktor veya diğer yetkililer tarafından işleme öncesinde (*en geç veri işlemesi esnasında*) aydınlatılması gerekir. Bu sorumluluğun yerine getirilmemesi veya gereği gibi yerine getirilmemesi doktorların, hastanelerin ve benzeri kurumların doğrudan sorumluluğunu doğurur. Aynı şekilde ilgili kişilerin KVKK ile özel olarak koruma altına alınmış olan haklarına doktor veya diğer sağlık sektörü çalışanları tarafından riayet edilmemesi de aynı şekilde hukuki sorumluluklar doğuracaktır.

Veri güvenliğinin Kanun'da öngörülen çerçevede tesis edilmesi sağlık hizmeti sunanlar için başlı başına bir yükümlülüktür. Bu yükümlük sadece teknik tedbirler alınmasını gerektirmemekte, aynı zamanda çeşitli idari (*yönetsel*) tedbirlerin alınmasını zorunlu kılmaktadır.

Ülkemizdeki sağlık kurumlarınca verilen hizmetlerin sadece ülkemiz vatandaşları ile sınırlı olmadığı göz önüne alındığında veri güvenliğine ilişkin alınması gereken tedbirlerin de sadece bu sağlık kurumlarınca ve yine sadece ülke sınırlarında alınması gereken tedbirlerden ibaret olmadığı açıktır.

Ayrıca aşağıda Bakanlık'ın VERBİS yükümlülüğü ile ilgili duyurusu yer almaktadır.

> *6698 sayılı Kanun hükümleri uyarınca Bakanlığımız; merkez teşkilatı ve taşra teşkilatı ile Bakanlığımız bünyesinde faaliyet göstermekte olan kamu hastaneleri, aile hekimlikleri, halk sağlığı ve toplum sağlığı merkezleri ve sair Bakanlığımıza bağlı sağlık hizmeti sunucuları bakımından tek bir veri sorumlusu olarak kabul edilmektedir ve veri sorumlusu Bakanlığımızın kamu hukuku tüzel kişiliğidir. Veri Sorumluları Sicili Hakkında Yönetmeliğin 11 inci maddesinin beşinci fıkrası uyarınca Bakanlığımız adına Sicile (VERBİS'e) kayıt yükümlülüğü, Genel Müdürlüğümüz tarafından yerine getirilecektir.*
>
> *Dolayısı ile 6698 sayılı Kanun kapsamında Veri Sorumluları Siciline,* ***Bakanlığımız adına Genel Müdürlüğümüz tarafından yapılacak bildirim dışında herhangi bir bildirim <u>YAPILMAMASI</u> gerekmektedir.***
>
> *Kamu ve vakıf üniversitesi hastanelerinin, bünyesinde faaliyet göstermekte oldukları üniversitenin kamu hukuku tüzel kişiliği tarafından VERBİS'e yapılacak olan kayıt yükümlülüğü kapsamında değerlendirilmesi; her türlü özel sağlık kuruluşunun ise bünyesinde faaliyet göstermekte olduğu özel hukuk tüzel kişiliği tarafından yapılacak olan kayıt yükümlülüğü kapsamında değerlendirilmesi gerekmektedir. Muayenehane işleten hekimlerin VERBİS'e kayıt yükümlülükleri ise ilgili hekimler tarafından yerine getirilmelidir.*[24]

Düzenlemelere göre sağlık hizmeti sunucuları, Bakanlık ve SGK çoğu durumda doğrudan **veri sorumlusu**, bazı durumda da **veri işleyen** niteliğini haiz olmaktadır. Bu durum, ilgili tarafların gerek doğrudan **veri sorumlusu**, gerekse de **veri işleyen** niteliği ile hem kendisinin eylemlerinden **<u>doğrudan</u>** hem de kişisel verileri paylaştıkları tarafların işleyeceği eylemlerden dolayı **müştereken sorumluluklar** doğurmaktadır.

[23] Avrupa Genel Veri Tüzüğü (GDPR), m.9 (2) h

[24] https://kisiselveri.saglik.gov.tr/TR,62249/verbis-hakkinda-duyuru.html

Bu durum, KVKK uyarınca bu sağlık hizmeti sunucuları tarafından, yapılan işlemler ile ilgili çok kapsamlı ve detaylı bir "**envanter**" çıkarılmasını ve "**risk/etki analizlerinin**" yapılmasını gerektirmektedir.

Kişisel verilerin gerek yurtiçinde gerekse de yurtdışına aktarılmasında "*yeterli önlemlerin*" alınması, belirli durumlarda "*yeterli bir korumayı yazılı olarak taahhüt edilmesi*" gibi ek önlemlerin de alınması gerekmektedir.

Zira bazı sorumlulukların yerine getirilememesi veya yükümlülüklerin ihlal edilmesi **TCK 135-140** ile düzenlenmiş suçlar bakımından **hapis cezası gerektirmektedir**. Benzer biçimde KVKK 18. maddesindeki kabahatleri işleyen şirketlere **idari para cezaları** uygulanması riski de bulunmaktadır.

İdari para ve disiplin cezaları ile hapis cezalarının yanı sıra 6698 sayılı kanunun 14. maddesinin (3). fıkrasına göre "*Kişilik hakları ihlal edilenlerin, genel hükümlere göre **tazminat hakkı** saklıdır*."

Benzeri biçimde GDPR düzenlemelerine göre de "*bir ihlal sonucu **maddi veya manevi zarar gören** herhangi bir kişi, yaşanan zarara ilişkin olarak veri sorumlusu veya veri işleyenden **tazminat alma hakkına** sahiptir*."

Yurtdışına aktarılacak kişisel sağlık verileri ise, KVKK düzenlemelerindeki koşullara ve yerine göre KVK Kurulu'nun iznine tabiidir. Bu nedenle yurtdışına veri aktarımı gerektiren tüm işlem süreçleri de KVKK düzenlemelerine uyum bakımından gözden geçirilmelidir.

4.5. KVKK/GDPR ve Sağlık Sektöründeki Riskler

KVKK/GDPR düzenlemeleri kişisel verileri işleyen her kuruluşu etkileyecektir. Ancak, aşağıdaki kişisel verilerin toplanıp, işlenmesi ve diğer taraflara aktarılmasından dolayı sağlık sektörü özellikle etkilenecektir.

Sektörün karmaşık ve küresel doğası gereği büyük ölçeklerde veri toplanmakta, işlenmekte ve paylaşılmaktadır. Hem ulusal anlamda hem de uluslararası veri paylaşımının da olduğunu göz önünde bulundurulduğunda bu kadar geniş kapsamlı bir sistemin güvenliğinin sağlanması oldukça zor bir süreç olduğu daha kolay görülmektedir. Günümüzde siber saldırganların hedefindeki sektörler içerisinde sağlık sektörü ilk sıralarda yer alırken, veri ihlalleri konusunda da 2. sırada yer aldığı gerçeğinden hareketle konu değerlendirildiğinde sağlık sektöründeki kişisel veri, özellikle de kişisel sağlık verilerinin güvenliği konusu büyük riskler taşımaktadır. Bu risklerin başında tüm kişisel sağlık verilerinin aktarıldığı ve barındırıldığı Bakanlık merkezi bilgi sistemi altyapısı yer almaktadır. Bir diğer önemli risk ise, kişisel sağlık verilerinin çok fazla sayıda 3. tarafa aktarılıyor olmasıdır. (*Eczane, Sigorta Şirketleri, SGK ve İşyerleri vb*). Ayrıca Sağlık Turizmi kapsamında toplan kişisel sağlık verileri ise başta AB ülkeleri olmak üzere ilgili tüm dünya ülkelerine aktarılması konudur.

Tüm bunlar göz önünde bulundurulduğunda böylesine geniş bir ağ ve sistemi yönetmenin zorluğu ve karmaşıklığı yanında önemli güvenlik riskleri de söz konusudur. Bu sistemin içerisinde veri ihlali riskleri ihmal edilemeyecek kadar büyüktür. Bu durum başta Bakanlık olmak üzere ilgili tüm taraflara KVKK/GDPR düzenlemelerine karşı çok ciddi yükümlülük ve sorumluluklar getirmektedir.

Dünyada ve ülkemizde gelişmelere bakıldığında birçok siber saldırı ve veri ihlali olaylarının meydana geldiği görülmektedir. Bu tür veri ihlalleri, kuruluşlar için iş, üretkenlik ve itibar üzerinde çok ciddi olumsuzluklara ve maddi zararlara yol açmaktadır.

Aşağıdaki veriler bu riskleri daha da açık bir şekilde ortaya koymaktadır. İngiliz Kişisel Veri Koruma Otoritesi ICO tarafından yayınlanan raporda, veri ihlallerinden;[25]

- ✓ **%18** oranla en büyük mağduriyetin **Sağlık Sektöründe** yaşandığını, bunu
- ✓ **%16** ile belediye ve kamu kurumlarının,
- ✓ **%12** ile eğitim kurumlarının,
- ✓ **%11** ile adli kurumların ve
- ✓ **%9** ile finans sektörünün izlediğini belirtmiştir.

[25] https://www.healthcareitnews.com/news/europe/statistics-reveal-healthcare-sector-most-affected-personal-data-breaches

ICO'nun raporunda, sağlık hizmetlerindeki veri ihlallerin çoğunun **çalışanlarla ilişkili** olduğu belirtilmektedir.

Verizon tarafından yayınlanan "*2019 Veri İhlali Araştırma Raporu*"na göre ise;[26]

- ✔ **%16** oranla en büyük mağduriyetin belediye ve kamu kurumlarının yaşandığını, bunu
- ✔ **%15** ile **Sağlık Sektörünün**,
- ✔ **%10** ile finans sektörünün izlediğini belirtmiştir.

Yaşanan 466 olayın 304'sında onaylanmış veri saçılması gerçekleşmiştir. Sağlık sektöründeki veri ihlallerinin çoğunlukla **yetkinin kötüye kullanımı** ile **web uygulamalarından** kaynaklanmaktadır. (**%81**)

Bu raporda da, veri ihlallerinin ağırlıklı biçimde çalışanlardan (**%59**) kaynaklanması, ICO tarafından tespiti de teyit etmektedir. Saçılan verilerin büyük bölümünü sağlık verileri (**%72**) oluştururken, diğer ağırlıklı veriler ise kişisel veriler (**%34**) oluşturmaktadır.

Raporda ayrıca veri ihlallerindeki temel nedenin finansal (**%83**) motivasyon olduğu belirtilmektedir.

Sağlık sektöründeki **veri ihlallerinin ortalama toplam maliyeti 6,45 milyon $** veya **veri ihlalinin ortalama toplam maliyetinden %65 daha yüksektir**. Aynı zamanda kayıt başına **429 $** maliyet ile yine sağlık kuruluşları en yüksek bedele katlanmaktadır.[27]

Bunlara ek olarak, sağlık sektörü, finansal hizmetler ve farmasötikler ile birlikte bir veri ihlalinden sonra müşterilerini elinde tutmak konusunda diğer sektörlerden daha fazla sorun yaşamaktadır.[28]

Finansal kuruluşlarının veri ihlallerini tanımlamaları ve gerekli önlemleri almaları **233 gün** sürerken, sağlık sektöründeki kuruluşlar için bu süreç **329 güne** çıkmaktadır.[29]

Aynı raporda, **sağlık sektörünün güvenlik otomasyonu konusunda da sıkıntılar yaşadığını** belirtmektedir. Güvenlik otomasyonunu tümüyle kuran sağlık kurumlarının oranı **%15** iken, kısmen kuranların oranı **%35**, güvenlik otomasyonuna sahip olmayanların oranı ise **%50**'dir.[30]

Sağlık sektörünün veri ihlallerine en fazla maruz kalan sektörlerden biri olması, özellikle kişisel sağlık verilerinin niteliği göz önüne alındığında oldukça ciddi bir probleme dönüşmektedir.

A.B.D.'deki sağlık sektörüne yönelik olarak yapılan araştırmada yer alan tablo, sağlık sektörünün tüm veri ihlalleri arasında **%35,64**'lük oranla 2. sırada yer aldığı göstermektedir. Saçılan verilerin %23.91 oranında hassas veri olması da dikkat çekicidir. Benzeri biçimde, saldırı ve ihlallerde kullanılan yöntemler açısından da sağlık sektörü 2. sırada yer almıştır.

Sektör	İhlal Sayısı	İhlal %'si	Saçılan Hassas Veri	Saçılan Hassas Veri %'si	Saçılan Kişisel Veri	Saçılan Kişisel Veri %'si
İş/Ticaret	644	43,72%	18.824.975	11,43%	705.106.352	99,99%
Sağlık	525	35,64%	39.378.157	23,91%	1.852	0,00%
Eğitim	113	7,67%	2.252.439	1,37%	23.103	0,00%
Banka/Finans	108	7,33%	100.621.770	61,10%	20.000	0,00%
Kamu/Askeriye	83	5,64%	3.606.114	2,19%	22.747	0,00%
Aylık Toplam	**1.473**	**100,00%**	**164.683.455**	**100,00%**	**705.174.054**	**100,00%**

Tablo.6. A.B.D.'deki aylık veri ihlalleri[31]

[26] https://enterprise.verizon.com/resources/executivebriefs/2019-dbir-executive-brief-emea.pdf
[27] IBM Security, Cost of a Data Breach Report 2019
[28] A.g.e.
[29] A.g.e.
[30] A.g.e
[31] 2019 End of Year Data Breach Report, ITRC, Cyberscout

Veri ihlal yöntemlerinin sektörlere göre dağılımına bakıldığında, sağlık sektörünün diğer sektörler içerisinde 2. sırada yer aldığı görülmektedir. Bunun temel sebeplerinden birisi, sağlık sektöründeki bilişim altyapılarındaki güvenlik önlemlerinin yetersizliği ve dolayısıyla saldırganlar için kolay bir hedef olmasıdır. İkinci önemli husus ise, kişisel sağlık verilerinin maddi, manevi ve bazı durumlarda da stratejik anlamda ciddi bir kıymet ifade etmesidir. Bu aynı zamanda bir ulusal güvenlik sorununa da dönüşmektedir.

Yöntem	Bankacılık	Eğitim	İş/Ticaret	Kamu	Sağlık	TOPLAM
Korsanlık/İşgal (Oltalama, Fidye, Kötücül)	31	29	291	35	191	577
Yetkisiz Erişim	45	59	223	15	196	538
Çalışan Hatası / İhmal / Kayıp	12	15	42	19	73	161
İnternet Kazası / İnternet Saçılması	12	7	44	8	17	88
Fiziki Hırsızlık	2	0	17	2	32	53
Kurumiçi Hırsızlık	6	2	12	3	10	33
Gönderimde Saçılma	0	1	15	1	6	23

Tablo.7. Veri İhlal Yöntemlerinin Sektörlere Göre Dağılımı[32]

Sağlık hizmeti sunucuları için teknolojik yeniliklerin hızına ayak uydurmak oldukça hayati bir öneme sahiptir. Buna rağmen birçoğu, güvenli dijital ve mobil sağlık hizmetlerine yönelik altyapı konusunda yetersiz durumdadır. Sağlık sistemleri teknolojilerini güncel tutamayan kurumların güvenlik risklerinin yanında, hastalarının, doktorlarının ve personelinin daha rekabetçi sağlık kurumlarına geçme riski bulunmaktadır.

Amerika'da yapılan bir araştırmada, 220 sağlık BT karar vericisinden sadece **%11**'i kendisinin sayısal dönüşüm kapsamında uyum sağladığını ifade ederken, üçte ikisi kendilerini bu konuda geç kalanlar olarak değerlendirmektedir. BT altyapılarının iyileştirilmesi konusunda erken davrananlar, aşağıda sıralanan konularda açık avantajlara sahip olduğu görülmektedir:[33]

- Azalan bakım maliyetleri (**%87**)
- Gelişmiş iş akışı verimliliği (**%83**)
- Daha fazla hasta memnuniyeti (**%82**)
- İyileştirilmiş hasta sonuçları (**%78**)

Diğer taraftan, aynı araştırmaya göre şu anda sağlık sektöründeki bilişim altyapılarının iyileştirmesinde karşılaşılan en büyük engeller aşağıdaki gibidir:

- Eski sistemleri yeni dijital/mobil teknolojilerle entegre etme
- Yeni çözümlerin iş akışlarına entegre edilmesine klinisyen direnci
- Yeni teknolojileri hem kurmak hem de sürdürmek için yetenekli BT personeli bulmak
- Gizlilik ve güvenlik endişeleri

Siber saldırganların sağlık hizmetleriyle ilgili sistemlere sızması halinde, hasta adları, adresleri, telefon numaraları, tıbbi durumlar, tedaviler, ilaç bilgileri ve sigorta kayıtları da dâhil olmak üzere birçok özel nitelikli kişisel bilgileri ele geçirmeleri söz konusudur. Bu bilgilerin günümüzde çok değişik amaçlarla kullanıldığı bilinmektedir. Bu durum siber âlemde ticari bir sektör haline gelmiştir.

KVKK'nın 17. maddesinde işaret edildiği üzere, **TCK 135 ile 140** arasında düzenlenmiş olan suç ve cezalar öncelikle kişisel verilerin korunmasını ihlal eden fiilleri kapsar. Kişisel verilerin korunması ile ilgili suç teşkil eden fiilleri işleyenleri, her bir fiil için 1 yıldan 6 yıla kadar hapis cezaları öngörülmektedir. Örneğin, kişisel verileri hukuka aykırı olarak bir başkasına veren bir sağlık hizmetleri yöneticisi veya çalışanları, TCK 136'daki **suçun nitelikli halini işlemiş olacağından** 3 ile 6 yıl arasında bir hapis cezasına çarptırılacaktır.

KVKK'nın 18. maddesinde çeşitli kabahatler tanımlanmıştır. Bu kabahatleri işleyen veri sorumlularına **5.000 TL ile 1.000.000 TL** arasında idari para cezaları uygulanır. Her bir ihlal bakımından ayrı ayrı söz konusu olacak olan bu cezalar kişisel verilerin korunmasına ilişkin yükümlüklerini yerine tam olarak getirmeyen

[32] A.g.e.
[33] https://www.healthcareitnews.com/news/majority-healthcare-providers-lagging-their-digital-health-readiness

sağlık hizmetleri sunucuları bakımından önemli bir risktir. Örneğin, veri güvenliğine ilişkin yükümlülüklerinin yerine getirilmemesi nedeniyle **1.000.000 TL**'sına kadar idari para cezası verilmesi mümkündür.

Son olarak kişisel verilerin korunmasına ilişkin yükümlüklerin ihlali beraberinde özel hukuk hükümlerine göre sağlık hizmeti sunucularının sorumluluğunu doğuracaktır. KVKK 14. maddesinde bu hususa *"Kişilik hakları ihlal edilenlerin, genel hükümlere göre tazminat hakkı saklıdır"* demek suretiyle işaret etmektedir. Kişisel verilerin korunması bilinci yaygınlaştıkça, her geçen gün sayısı artarak devam edecek olan tazminat taleplerine muhatap olacaklardır.

Ayrıca, KVKK'nın kapsamına sadece otomatik olarak işlenen kişisel veriler değil, bir veri kayıt sisteminin parçası olmak kaydıyla otomatik olmayan yollarla işlenen veriler de girmektedir. Bu nedenle basılı veya dijital ortamda işlenip işlenmediğine bakılmaksızın sağlık hizmetlerinin sunulması sürecinde işlenen ve kişisel veri niteliği taşıyan, kişisel sağlık verileri de dâhil her türlü veriler bakımından KVKK tarafından belirlenmiş yükümlükler ve bu uygulamalara bağlı riskler mevcuttur.

Avrupa yerleşik kişilere yönelik işlemlerden dolayı da ayrıca GDPR düzenlemeleri kapsamında bazı idari ve hukuki yükümlülükler ile ciddi idari para cezası riskleri söz konusudur.

4.6. Uyumluluğa Yönelik Adımlar

Günlük çalışma süreçlerine etkili veri koruma denetimleri uygulamak büyük bir zorluktur, ancak KVKK ve GDPR düzenlemeleri yürürlüğe girdiğinden bu yana, kişisel verilerin toplanması, işlenmesi ve paylaşılması, bu düzenlemeler açısından bazı uyumsuzluklara yol açabileceğinden sağlık sektöründeki kurum ve kuruluşları büyük para cezaları ve itibar gibi ciddi riskler beklemektedir. Etkili bir uyumluluk sürecinde ise ticari faydalar da vardır: yolcularının, çalışanlarının ve iş ortaklarının mahremiyetini koruyan ve uygun şekilde hedeflenmiş sağlık hizmetlerini sunan sağlık işletmelerinin iş, personel ve hastalar için daha cazip olmaları ve bunları elinde tutması daha olasıdır.

Sağlık sektöründe faaliyet gösteren kurum ve kuruluşların KVKK/GDPR düzenlemelerine uyumluluk için yapması gereken iş ve işlemler temel aşağıdaki gibidir:

Farkındalık

Sağlık hizmeti sunanların KVKK/GDPR uyumluluk projelerini ve bu düzenlemeler göre nelere ihtiyacı olduğu ve kendi kuruluşları için önemli risklerin ne olduğu konusunda özellikle üst yönetim arasında farkındalığı artırarak başlatmaları çok önemlidir.

Kurumun gerekli zamanı ve kaynakları taahhüt etmesini ve mahremiyete saygı duyan bir kültür geliştirmesini sağlamak için doğru insanları en üst yönetim seviyesine dâhil etmek gerekir.

Eğitim

KVKK/GDPR uyumluk projesinin başlangıcında farkındalığa yönelik ve daha uyumluluk politika ve planlarının uygulanmasına yönelik tüm personele ve mürettebata gerekli eğitimler verilmelidir.

Gemilerde seyahat belgeleri ve diğer kişisel veriler tutulmaktadır. Bu nedenle gemideki görevlilere belirli aralıklarla ve uygun ölçüde eğitimlerin verilmesi de önemlidir.

Veri Koruma Takımının Oluşturulması

KVKK/GDPR uyumluluk projesini yürütmek için yönetimin tam desteğiyle, risk, yasal ve bilişim teknolojileri çalışanlarından oluşacak bir ekip kurmaları gerekir.

Güvenilir harici danışman desteği; teknik uzmanlık, maliyet ve zaman kazanmanıza yardımcı olacaktır.

Hesap Verebilirlik ve Yönetişim Çerçevesi

KVKK/GDPR uyumluluğu, üstyönetim düzeyinde destek gerektirir. Bu nedenle üstyönetimin KVKK/GDPR düzenlemelerinin gereklerini, yükümlülüklerini, risklerini ve sonuçlarını iyi anlaması gerekmektedir. KVKK/GDPR uyumluluğunun sağlanması ve daha da önemlisi sürdürülebilmesi için gerekli kaynakların uygunluğu sağlamak ve sürdürmek için gereken kaynakların tahsis edilmesi üstyönetimin bu konudaki bilgisi ile yakından ilgilidir.

Veri İşleme Envanterinin Hazırlanması

Veri işleme faaliyetlerini belirlemesi ve veri işleme envanterinin hazırlanması ciddi bir iş yükü getirir ancak özellikle sağlık alanında faaliyet gösteren tüm kurum ve kuruluşlar için yasal bir zorunluluk niteliğindedir.

Veri işleme envanterinin hazırlanması, her faaliyet için veri toplamadan yok etmeye kadar tüm veri yaşam döngüsünün anlaşılmasını ve hazırlanmasını sağlar.

Fark Analizi ve Uyumluluk Planı

Kişisel verilerin işlenmesi sürecinde kuruluşlar veri akışlarındaki bir dizi zayıflık ve kırılganlıkların oluşması olasıdır. KVKK/GDPR uyumluluk çalışmaları kapsamında bu zayıflıklar ve kırılganlıklar dikkatlice aranmalı ve bunların yol açacağı olası riskler değerlendirmelidir. Daha sonra bu riskleri kabul edilebilir bir seviyeye indirgeyecek veya ortadan kaldıracak pratik eylem planları oluşturulmalıdır.

Zayıflıkları uzun soluklu izlenmesi ve yeni kırılganlıkların oluşmasını engellemek için uygulama planları ve prosedürler belirlenmelidir.

Veri Koruma ve Gizlilik Politikalarının Hazırlanması

Belirli eylem planı tamamlandığında, uyumluluk için uygulama aşamasına geçebilir. Bu normalde gizlilik politikalarında değişiklik yapılmasını, personel acenteleriyle yapılan sözleşmeleri, liman acentelerine, personele ve mürettebata bilgi bildirimlerinin yanı sıra uygun rıza formlarının hazırlanmasını içerir.

Uygulama, manuel prosedürler, BT güvenliği (*güvenlik duvarları, şifreleme vb.*) ve iş sürekliliği ile olağanüstü durum kurtarma planındaki değişiklikleri de içermelidir.

Dış danışmanlar uygulamanın çeşitli yönlerini yerine getirmeye yardımcı olabilir, fakat aynı zamanda çabayı yönetmeye de yardımcı olabilirler.

Veri İhlal Süreçlerinin Hazırlanması

Sağlık sektöründeki işletmeler, ihlal durumunda Kişisel Verileri Koruma Kurumuna ve veri sahiplerine (*veri ihlalinin tespitinden itibaren 72 saat içinde*) söz konusu ihlali ve olası etkileri ile ilgili bildirimde bulunmak zorundadırlar.

Bildirimin zamanında gönderilebilmesi için yapılması gereken ayrıntılı eylemleri içerecek bir Olay Raporu Planı tasarlaması çok önemlidir. Plan, önceden belirlenmiş net bir dizi ardışık eylem ve bu eylemler için açık bir sorumluluk tahsisi ve bildirim şablonları, araştırma gereksinimleri, raporlama, medya ve iletişim yönetimi vb. İçermelidir. Sağlık sektöründe faaliyet sunanlar ayrıca ayrıntıları içeren bir olay günlüğü tutacak teknik altyapıyı da hazırlamalıdırlar.

Risk Değerlendirmesi

Gizlilik ve veri güvenliği alanında çok sayıda "risk" tanımı ve kavramı olmasına rağmen, KVKK/GDPR kapsamında sadece verileri işlenen kişiler için gündeme gelecek olan riske odaklanılmaktadır.

KVKK/GDPR düzenlemeleri, veri sorumlularının belirli proje ve faaliyetlerde bulunan riske uygun bir güvenlik düzeyi sağlamasını gerektirir. Sağlık sektöründe faaliyet gösteren bir kurum veya kuruluş, kişisel verilere, özellikle de kişisel sağlık berilerine yönelik riski azaltmak için uygun seviyede teknik ve idari önlemleri uygulamadan önce riski belirlemek için gerekli çalışmaları yapmalıdırlar.

Veri sorumluları karşılaşacakları tek riskin sistemlerine girmeye çalışan siber suçlular olduğunu düşünmemelidirler, kişisel verilerin kazara veya kasıtlı imha, kayıp veya ifşaya karşı savunmasız olduğunu da göz önünde bulundurmalıdır.

Kişisel Verilerin Güvenliğine Yönelik Teknik Önlemlerin Alınması

KVKK/GDPR düzenlemelerinin öngördüğü teknik ve idari önlemlerin alınması, idari ve hukuki önlemlerin tamamlayıcı ve zorunlu tamamlayıcısı durumundadır.

Bunun için var olan bir bilgi güvenliği politikalarına ek olarak kişisel verilerin korunmasına yönelik politika ve süreçlerin tanımlanması gerekmektedir.

Ayrıca, kişisel verilere erişim içim yetki matrisinin de hazırlanması, veri keşif ve kişisel verilerin sınıflandırılması ile veri korumaya yönelik şifreleme, anonimleştirme ve bulanıklaştırma (*pseudonymization*) tekniklerinin uygulaması, KVKK/GDPR uyumluluk sürecinin zorunlu parçalarıdır.

İzleme ve Raporlama

KVKK/GDPR düzenlemeleri gereğince sağlık hizmeti sunan kurum ve kuruluşların gerektiğinde politikalarını ve prosedürlerini güncelleyerek, personelini ve mürettebatını eğitmeli ve gerekli resmi belgelerini ve anlaşmalarını güncelleyerek uyumluluklarını sürekli olarak izlemelidirler.

Ayrıca olası bir denetim için bu uyumluluk altyapılarını da gösterebilmelerinin en sağlıklı yolu da düzenli olarak ilgili raporların üretilmesi ve arşivlenmesidir.

Yönetişime Yönelik Bir Kültürün Geliştirilmesi

Bir sağlık hizmeti sunan kurum ve kuruluşun iç denetim ortamında kişisel verilerin korunmasına yönelik güvenlik tedbiri, etkili risk azaltma yöntemleri her zaman sonunda insanların bu önlemleri ne kadar iyi anladıkları ve uyguladıklarına bağlı olacaktır.

Sağlık sektöründe faaliyet gösteren kurum ve kuruluşlar kendilerini aktif olarak korumaları için yönetişim odaklı bir kültürün oluşturulması ve sürdürülmesi gerekmektedir. Bu kişisel verilerin saçılma tehditlerine karşı çok daha etkili bir kalkan oluşturur.

Sağlık hizmeti sunan kurum ve kuruluşlar, gerçekten risk odaklı, etkili ve verimli bir şekilde uyumluluk çalışmaları ile hem uyumluluk maliyetlerini hem de olası riskleri ve etkilerini en aza indirgemelidirler.

5. Sağlık Sektöründeki Yaptırım Örnekleri

Sağlık verileri, genetik ve biyometrik veriler KVKK düzenlemelerine göre "***özel nitelikli kişisel veri***"lerdir. Aynı zamanda sağlık sektöründeki düzenlemelere göre ise "***kişisel sağlık verileri***"dir.

Bu kişisel verilerin işlenmesi, gerek KVKK gerekse TCK kapsamında bir takım hukuki, idari ve cezai yaptırımlar ile güvence altına alınmıştır. KVKK uyumunun gereği yükümlülükleri yerine getirmeyenler de gerek ceza hukuku (TCK) gerek idare hukuku (KVKK) gerekse özel hukukta (*MK, BK ve diğer kanunlarda*) öngörülen yaptırımlara maruz kalacaklardır.

Diğer taraftan, gerek KVKK gerek GDPR gerekse de dünyanın diğer bölgelerindeki benzeri düzenlemeler kişisel sağlık verilerinin saçılması konusunda ağır yaptırımlar uygulamaktadırlar.

5.1. KVKK Uygulama Örnekleri

6698 sayılı KVKK ile kurulan Kişisel Verileri Koruma Kurumu ve Kurulu bugüne kadar bir dizi ikincil mevzuatı düzenleyip uygulamaya koymuştur. Bu düzenlemeler gereğince birçok inceleme yapmış ve yaptırımları da uygulamaya başlamıştır.

KVK Kurulu'nun 03/08/2018 Tarihli Karar Özeti

*İlgili kişiye ait özel nitelikli kişisel veri olan sağlık raporunun, bir **Hastane** nezdinde hastaların tedavi sürecinde yer alan **hekimler tarafından**, veri sorumlusuna ait mobil olarak kullanılan bir uygulamadan alınan ekran görüntüsünün başka bir cihaz tarafından çekilmesi suretiyle internet ve sosyal medya mecralarında paylaşılması ve bu itibarla özel nitelikli bir kişisel verinin sosyal medya aracılığıyla geniş bir kitleye ifşa edilmiş olduğu dikkate alınarak, Kurulca yapılan resen inceleme neticesinde;*

*6698 sayılı Kişisel Verilerin Korunması Kanununun 12 nci maddesinin (1) numaralı fıkrasının (c) bendi kapsamında kişisel verilerin muhafazasını sağlamak amacıyla **uygun güvenlik düzeyini temin edemeyen** veri sorumlusu hakkında Kanunun 18 inci maddesi uyarınca **idari para cezası** uygulanmıştır.*[34]

KVK Kurulu'nun 05/12/2018 Tarihli ve 2018/143 Sayılı Karar Özeti

*Bu kapsamda, doktor kontrolünde ilaç kullanan ilgili kişinin sağlığı ile ilgili özel nitelikli kişisel verilerinin, ilaçları temin ettiği eczane tarafından 6698 sayılı Kişisel Verilerin Korunması Kanununun 8 inci maddesinde **sayılan şartlar sağlanmadan üçüncü kişiyle paylaşılmasının** Kanunun 12 nci maddesinin (4) numaralı fıkrasına aykırılık teşkil etmesi nedeniyle veri sorumlusu eczane hakkında Kanunun 18 inci maddesi uyarınca **idari para cezası** uygulanmıştır.*[35]

KVK Kurulu'nun 07/11/2019 Tarihli ve 2019/332 Sayılı Karar Özeti

*"İlgili kişinin veri sorumlusu **Doktor** hakkındaki başvurusunda yer alan iddialar ile ilgili olarak Kurulun 11/04/2019 tarihli ve 2019/98 sayılı Kararı ile başlatılan inceleme kapsamında veri sorumlusundan konuya ilişkin gerekli bilgi ve belgelerin istenilmesine ilişkin Kurumumuzun 18/06/2019 tarihli yazısının 20/06/2019 tarihinde aynı konutta bir yakınına teslim edilmesine rağmen, bugüne kadar herhangi bir cevap verilmediği de dikkate alınarak, veri sorumlusu **Doktor tarafından** ilgili kişinin açık rızası veya Kanunun 5 inci maddesinin (2) numaralı fıkrasında sayılan diğer işleme şartları olmaksızın cep telefonuna reklam amaçlı mesaj gönderilmesi suretiyle kişisel verilerinin işlenmesi nedeniyle adı geçen veri sorumlusu hakkında Kanunun 12 nci maddesinin (1) numaralı fıkrasının (a) bendi kapsamında kişisel verilerin hukuka aykırı işlenmesini önlemek amacıyla uygun güvenlik düzeyini temin etmeye yönelik gerekli teknik ve idari tedbirleri almadığı kanaatine varılmasından ötürü, anılan veri sorumlusu hakkında Kanun'un 18'inci maddesinin (1) numaralı fıkrasının (b) bendi uyarınca **50.000 TL idari para cezası** uygulanmasına karar verilmiştir."*[36]

[34] https://www.kvkk.gov.tr/Icerik/5262/Kisisel-Verileri-Koruma-Kurumu-Karar-Ozetleri#
[35] https://www.kvkk.gov.tr/Icerik/5364/2018-143
[36] https://www.kvkk.gov.tr/Icerik/6624/2019-332

5.2. GDPR Uygulama Örnekleri

AB kişisel verilerin korunması konusunda 1981 yılından bu yana ciddi mevzuat ve uygulamaları hayata geçirmiş, bu mevzuat ve uygulamaları gerek iş hayatının sürekliliği gerekse de kişilerin mahremiyetinin korunması açısından dengeleyecek daha çok tecrübe edinme fırsatı yakalamıştır.

Bu kapsamda, kişisel verilerin korunması konusunda yeterli hassasiyeti göstermeyen çok büyük ölçekli uluslararası firmalar ve birçok kamu kurumlarına çeşitli yaptırımlar uygulamıştır. Aşağıda bu idari para cezaları uygulamalarından bazı örnekler verilmiştir.

Portekiz – Centro Hospitalar Barreiro Montijo Hastanesi

Portekiz Denetim Otoritesi (CNPD), yetkisiz personelin hastane bilgisayarına giriş yapmak için sağlık çalışanlarının profillerini kullanarak, tüm gizli hasta bilgilerine erişebildiğini tespit etti.[37]

Hastanede çalışan 296 sağlık personeline karşılık hastanenin bilgisayarında 985 tıbbi profil tespit edildi.

Hastane yönetiminin bu konuda daha önce uyarılmasına rağmen bu durumu düzeltmek için hiçbir şey yapmadığı için **400.000 €** tutarında iki **idari para cezası** kesildi.

- ✔ Hastanın verilerine erişimin ve gizlilik ihlallerinin sınırlanamaması nedeniyle **300.000 €**
- ✔ Tedavi sistemleri ve hizmetlerinin gizliliğini, bütünlüğünü, kullanılabilirliğini ve kalıcı esnekliğini sağlamak için **100.000 €.**

Almanya'da Bir Hastane

Hastanın kabulü sırasında hastaya yanlış fatura verilmesiyle sonuçlanan ve hastanenin uğraştığı daha ciddi mahremiyet sorunlarını ortaya çıkaran birkaç **GDPR ihlali meydana geldi**.[38]

Bu, Almanya'da inceleme anına kadar en yüksek para cezası olmasa da, kişisel sağlık verilerini içeren tıbbi ve hastane kayıtlarına ilişkin ihlallerin nasıl ele alındığı konusunda önemli bir gösterge oldu.

Hollanda - Haga Hastanesi

Hollanda Lahey'deki Haga Hastanesi, birçok çalışanının ünlü bir hastanın kayıtlarına eriştiği bir veri ihlali sonrasında GDPR kapsamında **460.000 € idari para cezasına** çarptırıldı.[39]

Hollanda Veri Koruma Dairesi tarafından yapılan soruşturmada, Haga Hastanesi'nin *"hasta kayıtlarının iç güvenliğinin bulunmadığını"* ve *"iki faktörlü kimlik doğrulama ve günlük dosyalarının düzenli olarak gözden geçirilmesi gereksinimlerini karşılamadığını tespit etti. "*

Hastaneye, GDPR tarafından talep edilen gerekli iyileştirmeleri yapmak için verilen süreden sonra, iki haftada bir **100.000 €**'ya kadar, en fazla **300.000 €**'ya kadar para cezası kesileceği bildirildi. Haga Hastanesi, güvenlik durumunu iyileştirmek için ek güvenlik önlemleri uygulamayı kabul etti.[40]

Macaristan'da Bir Sağlık Tesisi

Bir sağlık tesisi, eski bir çalışanın özel e-postalarını silmediği ve bu nedenle kişisel verileri yasal bir dayanak olmadan işlediği için **1.500 € idari para cezasına** çarptırıldı.[41]

[37] https://dataprivacymanager.net/top-5-gdpr-fines/
[38] https://dataprivacymanager.net/gdpr-fine-germany-e105000-fine-for-a-hospital/
[39] https://www.fairwarning.com/blog/monthly-healthcare-news-roundup-gdpr-compliance-fines-for-a-netherlands-hospital-healthcares-number-one-financial-issue-and-more/
[40] https://www.hipaajournal.com/netherlands-hospital-hit-with-e460000-gdpr-data-breach-fine/
[41] https://easygdpr.eu/gdpr-incident/hungary-1500-euro-fine-for-healthcare-facility/

İngiltere - Doorstep Dispensaree Ltd

Hasta verilerini güvenli olmayan bir biçimde saklayan ilaç firmasına GDPR ilkelerine aykırı davranmaktan dolayı idari para cezası kesildi. Firma, müşterilere ve bakım evlerine ilaç tedarik etmektedir. İlaçlar ve Sağlık Ürünleri Düzenleme Kurumu, Londra merkezli eczane Doorstep Dispensaree Ltd. şirketinde güvenli olmayan şekilde depolanmış belgeler buldu ve bir soruşturma başlatan ICO'yu (Bilgi Komiseri Ofisi) uyardı.

ICO, Haziran.2016 ve Haziran.2018 tarihleri arasında kilitli dolaplarda hastalar ile ilgili yaklaşık 500.000 belge buldu. Bu belgeler isim, adres, doğum tarihleri, NHS numaraları, tıbbi bilgiler ve çok sayıda kişinin reçetelerini içeriyordu. Bazı belgelerin, eksik koruma nedeniyle suya maruz kalıp hasar gördüğü belirlendi. Eczaneye **318,563 € idari para cezasına** kesildi.[42]

Bulgaristan'da Bir Doktor Muayenehanesi

Doktorunu ziyaret ederken, bir kişi daha önce hiç orada bulunmamış olmasına rağmen, farklı bir doktora atandığını fark etti. Sonuç olarak, DPA'ya şikâyette bulundu.

Soruşturma sırasında kişinin daha önce başka bir aile doktoru olduğu tespit edildi. Doktorunu değiştirdikten sonra hasta eski aile doktorunun yazılımında "etkin değil" olarak ayarlandı. Ancak işlemler, hasta transferinin bir parçası olarak, sadece aktif hastalara değil, yanlışlıkla tüm aktif olmayan hastalara da uygulandı.

DPA, GDPR'ın ihlal edildiğini belirledi ve 08.04.2019 tarihinde yaklaşık **1.000 € idari para cezası** verdi.[43]

Güney Kıbrıs'ta Bir Hastane

Bir hasta, söz konusu hastaneden, veri sahibinin erişim hakkından yararlanarak hastanede saklanan tüm kişisel verilerini istedi. Hastane, hasta dosyası kaybolduğundan talebi olumlu yanıtlayamadı. Sonuç olarak, kişi Kıbrıs'taki veri koruma yetkilisine şikâyette bulundu.

Soruşturma sırasında, DPA veri korumanın, sadece yetkisiz erişime karşı korumayı değil, aynı zamanda kişisel verilerin kaybolmamasını da kapsadığını açıkladı. Bu nedenle 15.02.2019 tarihinde hastaneye GDPR düzenlemelerini ihlal ettiği için **5.000 € idari para cezası** verildi.[44]

Almanya - Baden-Württemberg

Baden-Württemberg (Almanya) Veri Koruma Kurumu, 12.01.2019 tarihinde bazı kişisel sağlık verilerinin yanlışlıkla internette yayınlandığı için ilgili veri sorumlusuna **80.000 € idari para cezası** kesti.[45]

İdari para cezasının, GDPR m.25. "*Tasarım ve varsayılan olarak verilerin korunması*", m.5. "*Kişisel verilerin işlenmesine ilişkin ilkeler*", m.6. "*İşlemenin yasallığı*" ve m.9. "*Özel kişisel veri kategorilerinin işlenmesi*" maddelerinin ihlalinden dolayı kesildiği belirtilip daha fazla ayrıntı verilmemiştir.

[42] https://easygdpr.eu/gdpr-incident/gdpr-fine-after-careless-storage-of-health-data/
[43] https://easygdpr.eu/gdpr-incident/punishment-against-doctors-office/
[44] https://easygdpr.eu/gdpr-incident/strafe-wegen-verlorener-krankenakte/
[45] https://easygdpr.eu/gdpr-incident/strafe-wegen-irrtuemlicher-veroeffentlichung-von-gesundheitsdaten/

5.3. A.B.D. Örnekleri

A.B.D.'de 2019 yılında sağlık verisi ihlallerinde büyük bir artış görülmüştür. 2018 yılında veri ihlali **13.947.909** kayıta ulaşırken, bu sayı 2019 yılında **41.335.889**'a kadar yükselmiştir. 2019 yılında, A.B.D. nüfusunun **%12,5**'inin sağlık kayıtları çalıntı veya ifşa yoluyla veri saçılmasına maruz kalmıştır.

Sağlık sektörüne yönelik siber saldırılarda genel olarak ad-soyad, adres, doğum tarihleri, TCKN, sosyal güvenlik numaraları gibi kişisel verilerin yanı sıra ciddi miktarlarda hastalık bilgisi, tıbbi kayıt, tahlil, kemoterapi, röntgen, reçete gibi kişisel sağlık verileri de çalınmaktadır.

Özellikle sağlık sigortası sisteminin çok gelişmiş olduğu A.B.D.'de, HIPAA gibi çok sıkı düzenlemelere rağmen, sağlık sistemlerindeki yetersiz altyapı ve tedbir eksikliğinden kaynaklanan çok fazla sayıda ihlal gerçekleşmektedir.

Yıl	Kurum/Kuruluş	Miktar ($)	Ceza Türü
2019	Rochester Üniversitesi Sağlık Merkezi	3.000.000	Uzlaşma
2019	Touchstone Sağlık Görüntüleme	3.000.000	Uzlaşma
2019	Sentara Hastaneleri	2.175.000	Uzlaşma
2019	Jackson Sağlık Sistemi	2.154.000	İdari Para Cezası
2019	Texas Yaşlı ve Engelli Hizmetleri Bölümü	1.600.000	İdari Para Cezası
2019	Medical Informatics Engineering	100.000	Uzlaşma
2019	Korunda Medical, LLC	85.000	Uzlaşma
2019	Bayfront Health St. Petersburg	85.000	Uzlaşma
2019	West Georgia Ambulance	65.000	Uzlaşma
2019	Elite Dental Associates	10.000	Uzlaşma
2018	Anthem Inc	16.000.000	Uzlaşma
2018	TexasÜniversitesi MD Anderson Kanser Merkezi	4.348.000	İdari Para Cezası
2018	Fresenius Medical Care North America	3.500.000	Uzlaşma
2018	Massachusetts General Hospital	515.000	Uzlaşma
2018	Brigham and Women's Hospital	384.000	Uzlaşma
2018	Boston Medical Center	100.000	Uzlaşma
2018	Filefax, Inc.	100.000	Uzlaşma
2017	Memorial Sağlık Sistemi	5.500.000	Uzlaşma
2017	Dallas Çocuk Sağlık Merkezi	3.200.000	İdari Para Cezası
2017	Cardionet	2.500.000	Uzlaşma
2017	Memorial Hermann Sağlık Sistemi	2.400.000	Uzlaşma
2017	21st Century Oncology	2.300.000	Uzlaşma
2017	MAPFRE Life Insurance Company of Puerto Rico	2.200.000	Uzlaşma
2017	Presense Health	475.000	Uzlaşma
2017	Metro Community Provider Network	400.000	Uzlaşma
2017	St. Luke's-Roosevelt Hospital Center Inc.	387.000	Uzlaşma
2017	The Center for Children's Digestive Health	31.000	Uzlaşma

Tablo.8. A.B.D.'de OCR Tarafından Son 3 Yılda Kesilen İdari Para Cezaları[46]

A.B.D.'de kişisel sağlık veri ihlalleri için kesilen ve **16.000.000 $**'a kadar varan idari para cezalarından bazı örnekler, gerekçeleri ile birlikte aşağıda açıklanmıştır.

Sentara Hastaneleri

OCR, Sentara Hastaneleri'ne, ihlal bildiriminin postalama hatasından etkilenen diğer kişileri de kapsayacak şekilde güncellenmesi gerektiğini söyledi, ancak Sentara Hastaneleri reddetti.

Sentara Hastaneleri, güvenliği sağlanmayan sağlık verilerinin saçılmasıyla sonuçlanan ihlal sonrası HHS'ye doğru şekilde bildirimde bulunmaması nedeniyle, **2,175 Milyon $** idari para cezası ödeme konusunda uzlaşma yoluna gitti.[47]

[46] https://compliancy-group.com/hipaa-fines-directory-year/
[47] https://www.hhs.gov/about/news/2019/11/27/ocr-secures-2.175-million-dollars-hipaa-settlement-breach-notification-and-privacy-rules.html

Jackson Health System

OCR'nin araştırması, Jackson Sağlık Sistemi (JHS)'nin HHS Sekreterine zamanında ve doğru ihlal bildirimi sağlayamadığını, işletme çapında risk analizleri gerçekleştirmediğini, tespit edilen riskleri makul ve uygun bir seviyeye yönetemediğini, bilgi sistemi faaliyet kayıtlarını düzenli olarak gözden geçirmediğini ve işgücü üyelerinin yetkilendirmesini kısıtlamadığını ortaya koydu.

OCR, güvenlik ve veri ihlali nedeniyle JHS'ye **2,15 Milyon $'**lık idari para cezası verdi.[48]

Teksas Yaşlılık ve Engellilik Hizmetleri

Teksas Yaşlılık ve Engellilik Hizmetleri Bölümünün, maruz kaldığı dâhili ihlalin soruşturulması sırasında HIPAA Kurallarını birden fazla ihlal ettiği tespit edilmiş ve **1.600.000 $'**lık idari para cezası kesilmiştir.[49]

OCR yaptığı araştırmada, veri ihlallerine ek olarak, kurumun HIPAA Güvenlik Kuralı'nın gerektirdiği şekilde, işletme çapında bir risk analizi yapmadığını ve bilgi sistemleri ve uygulamaları üzerinde erişim ve denetim kontrolleri gerçekleştiremediğini tespit etti.

Medical Informatics Engineering

Indiana merkezli elektronik tıbbi kayıt yazılımı ve hizmetleri sağlayıcısı olan Medical Informatics Engineering, 2015 yılında NoMoreClipboard iştirakinde büyük bir veri ihlali yaşadı. Bilgisayar korsanları, elde ettikleri bir kullanıcı adı ve şifreyi kullanarak 3,5 milyon kişinin sağlık bilgilerini (PHI) içeren bir sunucuya erişmişlerdir. OCR incelemede, bir risk analizi başarısızlığı tespit etmiş ve **100.000 $** idari para cezası kesmiştir.[50]

Carroll County, West Georgia Ambulance

Carroll County'de faaliyet gösteren West Georgia Ambulance firması, 500 hastanın PHI'sını içeren şifrelenmemiş bir dizüstü bilgisayarın kaybedildiği bildirildi. OCR, bir risk analizi başarısızlığı olduğunu, personel için bir güvenlik bilinci eğitim programı olmadığını ve HIPAA Güvenlik Kuralı politika ve prosedürlerinin uygulanmadığını tespit etti.

West Georgia Ambulance, Inc. **65.000 $** idari para cezasını ödemeyi ve bu ihlalleri gidermek için düzeltici bir eylem planı hazırlamayı kabul etti.[51]

Elite Dental Associates

Elite Dental Associates diş kliniği, hastaların gizli sağlık verilerine ilişkin yaptığı sosyal medya açıklamalarının yol açtığı veri ihlalleri için **10.000 $** idari para cezası ödemeyi ve söz konusu veri ihlalini düzeltmek için gerekli adımları atmayı kabul etti.[52]

Bayfront Health St. Petersburg ve Korunda Medical

HIPAA kuralları sağlık hizmeti sağlayıcılarının veri sahibinin tıbbi kayıtlarının kendisine sağlaması taleplerini, talepten sonraki 30 gün içinde ve makul bir ücret ile yerine getirmesini gerektirmektedir.

OCR, Bayfront Health St. Petersburg, henüz doğmamış bebeği hakkında anneye talep ettiği kayıtlara zamanında erişim sağlayamadığı için, **85.000 $**'lık idari para cezası kesti.[53]

Aynı biçimde, Korunda Medical için de talep edilen bilgileri süresi içinde ve makul bir ücretle sağlamadığı için idari para cezası kesildi.

[48] https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/agreements/jackson/index.html
[49] https://www.hhs.gov/about/news/2019/11/07/ocr-imposes-a-1.6-million-dollar-civil-money-penalty-against-tx-hhsc-for-hipaa-violations.html
[50] https://www.hhs.gov/about/news/2019/05/23/indiana-medical-records-service-pays-100000-to-settle-hipaa-breach.html
[51] https://www.hhs.gov/about/news/2019/12/30/ambulance-company-pays-65000-settle-allegations-longstanding-hipaa-noncompliance.html
[52] https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/agreements/elite/index.html
[53] https://www.heartland.org/news-opinion/news/feds-take-action-against-doctors-who-fail-to-provide-patient-records

Premera Blue Cross

Bir bilgisayar korsanı Kuzeybatı Pasifik'teki en büyük sağlık sigortası olan Premera'nın ağına sızarak, özel sağlık bilgileri, Sosyal Güvenlik numaraları, banka hesap bilgileri, isimler, adresler, telefon numaraları, doğum tarihleri, kimlik numaraları ve e-posta adresleri dâhil hassas kişisel verileri çalmıştı. Bu ihlalden sonra Premera Blue Cross, aleyhine hassas müşteri verilerinin güvenliğini sağlayamamak ve milyonları etkileyen bir veri ihlali öncesinde ve sonrasında tüketicileri yanıltmak suçlarından 30 eyalette dava açıldı.

Premera Blue Cross, ülke çapında 10,4 milyondan fazla kişinin gizli bilgilerin saçılmasıyla sonuçlanan veri ihlali soruşturmasının ardından 30 eyalette **10 milyon $** idari para cezası ödemeyi kabul etti.[54]

Bu ihlallere yönelik **tazminat davaları** devam etmektedir.

Aetna

Sağlık sigortası firması Aetna, 2.460 müşterisine ait HIV ve Afib teşhisi ile ilgili oldukça hassas sağlık verilerini, ön yüzündeki adres pencerelerinden görülebilen zarflarla gönderdiği için aleyhinde açılan **17,2 milyon $**'lık davada **1,15 milyon $**'lık ödeme için uzlaşmayı kabul etti.[55]

Anthem Inc.

Anthem Inc. Sağlık sigortası firması tarafından 79 milyon kişiye ait adları, doğum tarihlerini, tıbbi kimlikleri veya Sosyal Güvenlik numaralarını, sokak adreslerini ve e-posta adreslerini içeren kişisel veriler ifşa edildi.

Bu veri ihlalleri nedeniyle Anthem Inc. firmasına açılan **tazminat** davasında **115 milyon $**'lık bir uzlaşmaya varıldı.[56]

5.4. A.B.D.'de Sağlık Verileri İhlalleri ile ilgili Teşhir Uygulaması

HHS Utanç Duvarı

HHS Utanç Duvarı (*HHS Wall of Shame*) son 24 ay içinde bildirilen tüm HIPAA ihlallerini listeler. HHS yetkisi altında kurulmuş bir web sitesidir. Utanç Duvarı, şu anda Sivil Haklar Dairesi tarafından soruşturma altında olan ihlalleri göstermektedir. HITECH Yasası'nın 13402 (e) (4) bölümünün bir parçası olarak HHS Sekreterinin, 500 veya daha fazla kişiyi etkileyen güvenliği sağlanmamış ve korunması gerekli sağlık bilgilerinin ihlallerine ait listeleri göndermesi zorunludur.

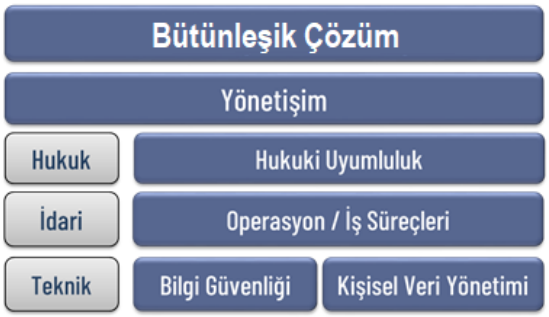
HIPAA İhlali Raporu

Paubox HIPAA İhlali Raporu HHS Utanç Duvarı'na bildirilen 500 veya daha fazla insanı etkilemiş kişisel veri ihlallerini inceler.

[54] https://www.databreaches.net/premera-blue-cross-pays-states-10-million-over-data-breach/
[55] Nursing Informatics for the Advanced Practice Nurse, Susan McBride, PhD, RN-BC, CPHIMS, Mari Tietze, PhD, RN-BC, FHIMSS s.343
[56] https://healthitsecurity.com/news/judge-gives-final-ok-to-115m-anthem-data-breach-settlement

6. Uyumluluk ve Denetim

Kişisel verilerin korunmasıyla tutarlı bir uygulama için tüm bu yapıları uçtan uca kapsayacak uygulama projesine gerek vardır. Bu, KVKK ve GDPR için uygulama projesinin tüm bileşenlerini kapsayan sürecin izlenmesi ve değerlendirilmesi için **tam bir çözüm** olmalıdır.



Bu nedenle; Kişisel Verilerin Korunmasına yönelik gerçekleştirilecek bir çalışmada hukuki, idari ve teknik olmak üzere üç farklı eksenli çalışmalarının bütünleşik olarak hep birlikte yapılması zorunludur.

6.1. Hukuki Çalışmalar

Hukuki değerlendirmeler;

- ✓ Aydınlatma ve açık rıza metinlerinin düzenlenmesi,
- ✓ Çalışanlar, tedarikçiler, müşteriler, işortakları ve benzeri 3. taraflarla düzenlenen sözleşmelerin gözden geçirilip KVKK /GDPR mevzuatına uyumlu hale getirilmeleri,
- ✓ Kişisel verilerle çalışan personel ile yine mevzuata uygun sözleşmelerin düzenlenmesi,
- ✓ Veri sahiplerinin KVKK/GDPR kapsamındaki taleplerinin incelenmesi ve değerlendirilmesi,
- ✓ KVKK/GDPR ilgili diğer konulardaki hukuki değerlendirmelerin yapılması konularını içerir.

6.2. İdari Çalışmalar

İdari değerlendirmeler;

- ✓ Veri koruma ve güvenlik politikalarının belirlenmesini,
- ✓ Risk yönetimini,
- ✓ Proje metodolojisini ve değişim/uyum sürecinin KVKK/GDPR düzenlemelerine göre yönetilmesini içerir.

Ayrıca,

- ✓ KVKK/GDPR mevzuatına göre kişisel verilerin korunmasına yönelik gerekli kurum içi organizasyonun oluşturulması,
- ✓ Görev ve sorumluluk matrisinin hazırlanması ve süreçlerin düzenlenmesi
- ✓ KVKK/GDPR kurumları ile iletişim ve başvurularda gerekli desteklerin sağlanması konularını da içerir.

Bu kapsamda yapılacak uyumluluk çalışmaları;

- ☑ KVKK Önleyici ve Düzeltici Danışmanlık
- ☑ Politikalar / Süreçler / Belgeler
- ☑ Gizlilik ve Mahremiyet Politikaları
- ☑ Veri Koruma Etki Analizi
- ☑ Eğitim

kapsamaktadır.

6.3. Teknik Çalışmalar

Müşteri verilerinin teknik kontrolü, uyumluluğunun anahtarıdır;

- ✓ Yapılandırılmış (*veritabanları*), yarı yapılandırılmış (*Excel vb.*) ve yapılandırılmamış (*dokümanlar, PDF vb.*) veri analizi uygulamaları,
- ✓ Kullanılan uygulamalar ve veri tabanları,
- ✓ Veri merkezi, güvenlik duvarı sistemi, veri depolama,
- ✓ Bulut servisi, e-posta hizmetleri ve güvenlik sistemlerini içerir.

Ancak tümü bunlarla sınırlı olmayıp, KVKK/GDPR zorunlu kıldığı analizlerin ve değerlendirmelerin yapılması ve Müşteri tarafından kullanılan diğer özel uygulamalar da bu sürece dâhil edilmektedir. *(Kişisel Veri Yönetişimi, Müşteri Talep Yönetimi, Şifreleme vb.)*

KVKK/GDPR Uyumluluk çözümünün ikinci aşaması, idari ve hukuki süreçlerin belirlenen tespitlerin gözden geçirilmesi ve tamamlanması ile tüm teknik altyapının uyum otomasyonunu sağlayarak ***bütünleşik çözümü*** gerçekleştirecek bir aşamadır. Bu teknik uygulama süreçlerini tamamlamak, düzenli ve sürekli bir süreç otomasyonu ile uyum için hazır hale gelinmesinin ön koşuludur. Bu kapsamda;

- ☑ Yapılandırılmış / Yapılandırılmamış Ortamlarda Veri Keşfi
- ☑ Veri Sınıflandırılması / Süreç Yönetimi / Veri Yönetişimi
- ☑ Şifrelendirme / Anonimleştirme / Silme / Yok Etme
- ☑ Veri Sahibi Talep Yönetimi
- ☑ Risk Yönetimi / Veri Koruma Etki Analizi
- ☑ Uyumluluk
- ☑ Denetim

çalışmaları "İkinci Aşamada" gerçekleştirilmesi gereken ve temel bir teknik altyapıyı gerektiren iş ve işlemlerdir.

Kişisel verileri korumanın ve korumada sürekliliğin sağlanması ancak uçtan-uca izleme ve denetleme olanağı sağlayan teknik bir çözüm ile mümkündür ve **bu da KVKK/GDPR uyumluluğunun gerçek anahtarıdır.**

■

ACCERT A.Ş.

ACCERT A.Ş. 2018 Yılında sadece Kişisel Verilerin Korunması ile ilgili çalışmalar yapmak için kurulmuştur.

Kurucuları: Bilişim Teknolojileri, Bilgi Güvenliği ve Regülasyon alanında 30 yılın üzerinde deneyimli uzman ve akademisyenlerden oluşmaktadır.

Vizyonu: Kişi, kurum ve kuruluşları ulusal ve uluslararası kişisel verilerinin korunması süreçlerine hazırlamaktır.

Misyonu: Kişilerin gizlilik hakları ile meşru iş fırsatları arasında adil denge kurmak için en uygun çözümleri sunmaktır.

Kişisel Verilerin Korunması Kanunu (*KVKK*) ve Avrupa Veri Koruma Tüzüğü (*GDPR*) gereklilikleri ve yükümlülükleri ile kurum ve kişiler arasında adil denge kurmak için farkındalığı artırmak ve güven ortamının devamlılığını sağlamak amacıyla bütünsel çözümler sunmaktır.

ACCERT A.Ş. Vizyon ve Misyonuna bağlı olarak konusunda uzman ulusal ve uluslararası kuruluşlar ile işbirliği yaparak kişisel verilerin korunması konusunda çözüm sunma çalışmalarını ilerletmiştir.

KVKK ve GDPR düzenlemelerine yönelik uyumluluk çalışmalarında danışmanlık, denetim ve eğitim hizmetleri sunmaktadır.

Bugün iş ortakları ile bu alanda uçtan uca çözüm sunabilen Türkiye'deki öncü kuruluşlarından biridir.

ACCERT Sertifikasyon, Belgelendirme, Danışmanlık, Eğitim ve Denetim A.Ş.

Uğur Mumcu'nun Sokağı No:39/7
Büyükesat Mahallesi, Çankaya / Ankara

Telefon : + 90 (312) 436 41 93
E-Posta : accert@accert.com.tr

ISBN-978-605-06236-0-4

ACCERT