ACCERT
ACCREDITATION – CERTIFICATION

Sektör İncelemeleri - 4

Kişisel Verilerin Korunması

Sigortacılık

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 Haziran.2020

ISBN-978-605-06236-2-8

İçindekiler

Önsöz

ACCERT Sektörel İnceleme Raporlarının ilk üçü beklediğimizden daha çok ve daha olumlu geri dönüşler sağladı. Bu da bizleri, yaptığımız bu iş için fazlaca yüreklendirmeye yetti. Benzeri biçimde yenileri için yüreklendirirken de, konu yani sektör açısından beklentileri de gösterdi. İşte bu beklentilere yönelik Sigortacılık sektöründe kişisel verilerin işlenmesi ve korunması üzerine bu inceleme raporunu hazırlayıp yayınlamaya karar verdik. Bu raporda da yine sigortacılık sektörünün kendisine has yasal ve pratik durumunu kişisel veriler ve mahremiyetin korunması açılarından ele alıp ilgili sektöre bir rehberlik sunabilmeyi hedefliyoruz.

Bu raporu hazırlarken de dünya küresel salgınla (*pandeminin*) mücadelesini sürdürüyor. Önceliğimiz bu salgını sağ-salim atlatabilmek. Ama ağır-aksak da olsa, yaşam sürüyor.

Sektörel olarak salgını ve yol açtığı tahribatı en yakından izleyen sektörlerin başında sağlık geliyorsa hemen ardından gelen sektöründen biri de sigortacılıktır. Hem insan hayatı hem de faaliyet alanı açısından sigortacılık da çok ciddi bir sınamadan geçiyor ve geçmeye devam edecek.

Sigortacılık, ana faaliyetleri nedeniyle kişisel veriler, özellikle de özel nitelikli kişisel veriler (*ağırlıklı olarak da kişisel sağlık verileri*) ile uğraşan bir sektör. Bu nedenle, salgın döneminde ve salgından sonra çok daha fazla dikkatli olması gerekmektedir. Küresel anlamda büyük sıkıntı yaşayan kişiler ve şirketler daha alıngan, daha kırılgan olacaklardır.

Yüzyılda bir kez yaşanan küresel salgın, geleneksel iş yapış biçimlerini etkileyip değiştirirken, kapsam ve ölçek olarak sigortacılık sektöründe de bütün varsayımları, bütün algıları değiştirecektir. İşte böyle bir dönemde, böyle bir ortamda sigortacılık sektörü kendisini daha fazla hırpalayacak "boş bulunmalardan" kaçınmalıdır ve kişisel verilerin korunması da bunlardan birisidir.

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 sahip gibi görünse de, kişisel veriler ve mahremiyet konusu yeterince dikkat ve özenle ele alınmazsa, bu durum sigortacılık da dâhil kurumlara duyulan inanç ve güveni ciddi bir biçimde aşındıracaktır.

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.

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.

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
Haziran.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
Birlik	Türkiye Sigorta Birliği (TSB)
BT	Bilişim Teknolojileri
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*)
DSÖ	Dünya Sağlık Örgütü (World Health Organization)
e-Devlet	e-Devlet, vatandaşlara devlet tarafından verilen hizmetlerin elektronik ortamda sunulması
EDPB	Avrupa Veri Koruma Kurulu (*European Data Protection Board*)
GDPR	Avrupa Genel Veri Koruma Tüzüğü (*General Data Protection Regulation)*
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*)
IAIS	Uluslararası Sigorta Denetçileri Derneği (*The International Association of Insurance Supervisors*)
ICO	İngiltere Bilgi Komiseri Ofisi (*Information Commissioner's Office*)
İK	4857 Sayılı iş Kanunu
İlgili Kişi	Kişisel verisi işlenen gerçek kişi
KVKK	6698 sayılı Kişisel Verilerin Korunması Kanunu
KVK Kurumu	Kişisel Verileri Koruma Kurumu
MEDULA	e-Nabız Sistemi
NAIC	A.B.D. Ulusal Sigorta Komisyoncuları Birliği (*National Association of Insurance Commissioners*)
OCR	A.B.D. Sağlık ve İnsan Hizmetleri Bakanlığı Sivil Haklar Ofisi (*Office for Civil Rights*)
OECD	Ekonomik işbirliği ve Kalkınma Teşkilatı (*Organization for Economic Cooperation and Development)*
SBM	Sigortacılık Bilgi ve Gözlem Merkezi
SGK	Sosyal Güvenlik Kurumu
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
TSB	Türkiye Sigorta 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*)

1. Sigortacılık Sektörü ve Kişisel Veriler

Kişisel verilerin hem kamusal hem de ticari açıdan çok kritik önem taşıdığı günümüzde finans ve sigortacılık, kişisel veriler açısından çeşitli ve karmaşık iş yükü ve iş süreçlerine sahip bir sektördür.

5684 sayılı Sigortacılık Kanunu'nda tanımlanan sigorta işlemleri kişilerin, kurum ve kuruluşların çeşitli bilgilerinin toplandığı süreçlerden oluşmaktadır. Sigortacılık toplum ve iş hayatının çok geniş bir kesimini kapsayan faaliyetleri için topladığı büyük ölçekli verilerin içerisinde çok fazla miktarda da kişisel veriler bulunmaktadır. Bunların başında bireysel emeklilik, hayat ve kaza sigortaları gibi işlemleri olmak üzere, sigortacılık **çok çeşitli** kişisel verileri ve bilgileri içeren karmaşıklıktaki iş ve işlemlerden oluşmaktadır.

6698 Sayılı Kişisel Verileri Koruma Kanunu, sigorta sektörü için çok kritik bir yasadır;

- ✓ Sigortacılık mesleğinin **ana iş konusu kişisel veriler** ile ilgilidir.
- ✓ Sigortacılar, yapılan işlerin doğası gereği, **birçok kişi ve kuruma** (*niteliğine bağlı olarak ulusal ve uluslararası*) **bilgi ve veri aktarımı** yapmaktadır.
- ✓ Özellikle sağlık verileri gibi KVKK'da **özel nitelikli kişisel verileri** de işlemektedir.

Hem ulusal hem de uluslararası düzenlemelere bakıldığında, bu alana yönelik önemli tanımlamalar ve düzenlemeler olduğu görülmektedir. Ülkemizde 7.Nisan.2016 tarihinde yürürlüğe giren 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 (*GDPR*) ise kişisel verilerin yanısıra özel nitelikli kişisel veriler ile ilgili *(-ki bunların başında **sağlıkla ilgili veriler**, **genetik veriler** ve **biyometrik veriler** gelmektedir*) daha ayrıntılı düzenlemeler yapılmıştır.

Düzenlemelere göre sigorta şirketleri çoğu durumda doğrudan **veri sorumlusu**, bazı durumlarda da **veri işleyen** niteliğini haiz olmaktadır. Bu sigorta şirketleri 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, sigorta şirketleri tarafından;

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

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

Sigortacılık işlemlerinde KVKK/GDPR düzenlemeleri kapsamında tanımlanmış olan kişisel veriler, ağırlıklı olarak kişilerden olmak üzere, çeşitli kurum ve kuruluştan toplanıp, işlenmekte ve bir kısmı iş gereği bir kısmı da mevzuatlar gereği paylaşılmaktadır. Bu denli geniş bir kapsamda ve büyük miktarda toplanıp işlenen ve paylaşılan kişisel verilerin yönetilmesi elbette zor ve oldukça risklidir. Bunun tabii sonucu olarak, veri ihlalleri ve saçılma riskleri de artmaktadır.

Sigorta işlemleri özellikle sağlık ve hayat sigortalarındaki işlemler, kendi doğası ve ulusal sigorta mevzuatının yapısından dolayı ulusal ve uluslararası alanda, işlenen ve aktarılan yüksek düzeydeki kişisel veriler açısından, bu sigorta şirketlerini daha kırılgan hale getirmektedir.

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 veriler 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. KVK Kurumu, "***veri merkezleri yurtdışında olan platformların kullanılması*** *durumunda yurtdışına veri aktarımı söz konusu olacağından, Kişisel Verilerin Korunması Kanununun 9 uncu maddesinde belirtilen şartlara uygun olmayan aktarımların Kanunun ihlali anlamına gelebileceğini*" belirtmiştir.[1]

Bu örneklerden görüleceği üzere, KVKK uyumluluğu sigortacılık 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 GDPR düzenlemeleri, verilerin nerede tutulduğuna bakılmaksızın, AB yerleşik bireylere ait kişisel verilerin, özellikle de kişisel sağlık verilerinin işlenmesi durumunda AB dışındaki kurum ve kuruluşları da kapsamaktadır.[2] **AB'de yerleşik veri sahiplerine mal ve hizmet sağlayan ya da davranışlarını izleyen** AB üyesi olmayan veri sorumlusu ve/veya veri işleyenleri, dolayısıyla bu işlemleri yapan sigortacılık şirketlerini de kapsayacaktadır.[3]

KVKK sorumluluk ve yükümlülüklerinin yanı sıra, yaptığı iş ve işlemler ile aktardığı veya aktarılan bir takım kişisel verilerden dolayı GDPR kapsamına girecek sigorta şirketlerinin GDPR düzenlemeleri gereğince ek bazı teknik, idari ve cezai sorumluluk ve yükümlülükleri de bulunabileceği, GDPR yaptırımlarının sonuçlarının ise daha ağır olduğu göz önünde bulundurulmalıdır.

Sigortacılık sektörü de bu düzenlemelerden en fazla etkilenecek alanlardan biri olup yeni düzenlemelere en etkili ve verimli biçimde uyumluluk sağlaması gerekmektedir.

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 sigortacılık hizmeti veren kurum ve kuruluşları büyük para cezaları ve itibar kaybı gibi ciddi riskler beklemektedir.

Etkili bir uyumluluk sürecinde yasal yükümlülüklerin yanısıra ticari faydalar da vardır. Müşterilerinin, çalışanlarının ve iş ortaklarının mahremiyetini koruyan ve uygun şekilde hedeflenmiş çalışmalar yürüten sigorta şirketlerinin, iş, personel ve müşteriler için daha güvenli ve tercih edilir olmalarını sağlayacaktır.

[1] https://www.kvkk.gov.tr/Icerik/6723/Uzaktan-Egitim-Platformlari-Hakkinda-Kamuoyu-Duyurusu
[2] Avrupa Genel Veri Koruma Tüzüğü (GDPR) m.3
[3] EDPB Guidelines 3/2018 on the territorial scope of the GDPR (Article 3) - version adopted after public consultation

2. Kişisel Verileri Koruma Kanunu (KVKK)

6698 sayılı Kişisel Verileri Koruma Kanunu (KVKK) 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 sigortacılık sektöründe faaliyet yürüten kurum ve kuruluşlar 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

Kanun, ilgili hükümleri ihlal edilmesi durumunda, ihlalleri niteliğine göre "***suçlar***" ve "***kabahatler***" olarak ayırmış olup, kabahatler için sorumlu kişi veya kurumlara 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

KVKK'na göre 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

KVKK'nın 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 KVKK'nın 14. maddesinin (3). fıkrasına göre "*Kişilik hakları ihlal edilenlerin, genel hükümlere göre* ***tazminat hakkı*** *saklıdır.*"

2.3. KVKK Uygulama Örnekleri

Kurum ve Kurul 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
12.03.2020	İnternet Servis Sağlayıcısı	**300.000**	m. 12/1	Veri Güvenliği için Gerekli İdari ve Teknik Tedbirlerin Alınmaması
27.02.2020	Spor Salonu	**225.000**	m. 12/1 a	Veri Güvenliği için Gerekli İdari ve Teknik Tedbirlerin Alınmaması
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
27.02.2020	Amazon Turkey	**100.000**	m. 10	Aydınlatma Yükümlülüğünü Yerine Getirmemek
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
27.01.2020	Gayrimenkul Şirketi	**50.000**	m. 5	Genel Veri İşleme İlkelerine Uyumsuzluk
6.02.2020	Uçak Bileti Satış Firması	**50.000**	m. 15/5	Kurum Kararını en geç 30 Gün İçinde Yerine Getirmemek
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
7.11.2019	Telekom Şirketi	**50.000**	m. 12/1	Veri Güvenliği için Gerekli İdari ve Teknik Tedbirlerin Alınmaması
16.01.2020	Banka	**50.000**	m. 12/2	Veri Güvenliği için Gerekli İdari ve Teknik Tedbirlerin Alınmaması
14.01.2020	Eğitim Kurumu	**50.000**	m. 12/1 a	Veri Güvenliği için Gerekli İdari ve Teknik Tedbirlerin Alınmaması
14.01.2020	Avukat	**50.000**	m. 12/1	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
27.01.2020	Sigorta Acentası	**22.500**	m. 12	Genel Veri İşleme İlkelerine Uyumsuzluk
31.05.2019	Varlık Şirketi	**20.000**	m. 12/1 a	Genel Veri İşleme İlkelerine Uyumsuzluk
16.01.2020	Çağrı Merkezi	**18.000**	m. 12/1 a	Veri Güvenliği için Gerekli İdari ve Teknik Tedbirlerin Alınmaması
27.01.2020	Mobil Uygulama	**10.000**	m. 10	Aydınlatma Yükümlülüğünü Yerine Getirmemek
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		
16.01.2020	Banka	BDDK'ya İntikal	m. 12	Veri Güvenliği için Gerekli İdari ve Teknik Tedbirlerin Alınmaması

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

3. Avrupa Veri Koruma Tüzüğü (GDPR)

Sigortacılık 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 tarafından, GDPR kapsamında verilecek cezalarının "***etkili, ölçülü ve caydırıcı***" olması öngörülmüş ve bu nedenle söz konusu idari para cezaları da ciddi miktarlara ulaşabilmektedir.

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 cezaları (hangi meblağ yüksek ise, o geçerlidir) kesilecektir.*
  - *Veri Koruma Görevlisinin Belirlenmesi*
  - *Veri Koruma Görevlisinin Konumu ve Görevleri*
  - *Onaylı Davranış Kurallarının İzlenmesi*
  - *Veri Koruma Etki Değerlendirmesi (DPIA)*
  - *Ön istişare*
  - *DPIA süreçlerindeki Eksiklik – Yanlışlık: İdari Para Cezası*

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 cezaları*** *(hangi meblağ yüksek ise, o geçerlidir) kesilecektir.*
  - *Rıza koşulları da dâhil olmak üzere işleme faaliyetine ilişkin Temel İlkeler (m.5, 6, 7 ve 9)*
  - *Veri Sahiplerinin Hakları (m.12 ila 22)*
  - *Üçüncü ülkedeki bir alıcıya veya bir uluslararası kuruluşa yönelik kişisel veri aktarımları (m.44-49)*

3.3. Veri Akışının Askıya Alınması

- Üçüncü bir ülkedeki bir alıcıya veya uluslararası bir kuruluşa yönelik **veri akışlarının askıya alınması** yönünde talimat verilmesi söz konusudur.

3.4. Tazminat Hakkı

- Bir diğer risk de, veri ihlalinden zarar görecek kişilere tanınan **tazminat** hakkıdır.

Ayrıca, yol açacağı **ticari zararlar** ve **itibar kayıpları** da göz önünde bulundurulması gereken bir husustur.

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
HIRVATİSTAN	13.03.2020	20.000.000	Banka	m.15 (1), (3)	Veri Sahibi Hakları Sağlanama Yükümlüğünün Tam Sağlanamaması
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
İTALYA	17.01.2020	8.500.000	Eni Gas e Luce S.p.A. (Elektrik ve Gaz)	m.5, m.32	Gizlilik politikalarının yetersizliği
İSVEÇ	11.03.2020	7.000.000	Google LLC	m.5, m.6, m.17	Veri Sahibi Hakları Sağlanama Yükümlüğünün Tam Sağlanamaması
İTALYA	18.01.2020	3.000.000	Eni Gas e Luce S.p.A. (Elektrik ve Gaz)	m.5, m.6; m.7, m.25	Rıza Eksikliği, Veri Güvenliği için Gerekli İdari ve Teknik Tedbirlerin
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
HOLLANDA	30.04.2020	725.000	Bilinmiyor	m.5, m.9	Veri İşleme için Yetersiz Yasal Dayanak
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	Hellenic Telecom Organization (OTE)	m.5 (1) c, m.25	Genel Veri İşleme İlkelerine Uyumsuzluk
YUNANİSTAN	7.10.2019	200.000	Hellenic Telecom Organization (OTE)	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)(2), m.6 (1), m.13 (1)c, m.14	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
FİNLANDİYA	22.05.2020	100.000	Posti Group Oyj	m.12, m.13, m.14, m.15	Veri Sahibi Hakları Sağlanama Yükümlüğünün Tam Sağlanamaması
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
İRLANDA	17.05.2020	75.000	Tusla	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	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 Yerne 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.5 (1) a, m.6	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. Sigortacılık Sektörü ve Kişisel Verilerin Korunması

Sigortacılık, Türkiye Sigorta Birliği (*TSB*) tarafından "*aynı türden tehlikeyle karşı karşıya olan kişilerin, belirli bir miktar para ödemesi yoluyla toplanan tutarın, sadece o tehlikenin gerçekleşmesi sonucu fiilen zarara uğrayanların zararını karşılamada kullanıldığı, bir risk transfer sistemi*"[4] olarak tanımlanmıştır.

Sigortanın temel işlevi, zararı ekonomik açıdan önemsiz bir duruma getirmektir. Kişiler tek başına karşılayamayacakları zararları bir organizasyon aracılığıyla aralarında paylaşmaktadırlar.

"*Modern sigortacılığın doğuşuna deniz, kara sigortacılığına yangın, kaza sigortacılığına tren kazaları ile ilişkin bireysel kazalar öncülük ederken, sanayinin gelişmesiyle yaşanan büyük teknik hasarlar, mühendislik sigortalarının gelişimine yol açmıştır.*

20. yüzyılın başlarında sigorta şirketleri her türlü sigorta ihtiyacına cevap verebilecek şekilde örgütlenmelerini tamamlamış kuruluşlar olarak etkin hizmet verebilecek düzeye ulaşmışlardır."[5]

Kişilerin mahremiyeti ve kişisel verilerin korunması ile **meşru iş fırsatları** arasındaki denge her zaman tartışma konusu olmuştur.

Nitekim Sigortacılık sektörünün ana faaliyetlerinin odak konusu olan kişisel verilerin işlenmesi, AB düzenlemelerinde de tartışma konusu olmuştur. GDPR metninin başında yer alan Açıklamalar (*Recitals*) bölümünde bu konuda özel açıklamalar yer almaktadır.

> *(52) Birlik veya Üye Devlet yasalarında öngörüldüğü ve kişisel verilerin ve diğer temel hakların korunmasına yönelik yeterli önlemlerin alınması koşuluyla, özellikle iş hukuku alanındaki kişisel verilerin işlenmesi, emekli aylıkları ve sağlık güvenliği dâhil olmak üzere sosyal koruma kanunu, izleme ve uyarı amacıyla, bulaşıcı hastalıkların ve diğer sağlığa yönelik ciddi tehditler önlenmesi veya kontrolü için özel kişisel veri kategorilerinin işlenmesine ilişkin yasağın kaldırılmasına izin verilemelidir. Bu tür bir istisna, halk sağlığı ve sağlık hizmetleri hizmetlerinin yönetimi de dâhil olmak üzere sağlık amaçları için yapılabilir, **özellikle sağlık sigortası sisteminde hak ve hizmetlere ilişkin taleplerin çözümünde kullanılan prosedürlerin kalitesinin ve maliyet etkinliğinin sağlanması** amacıyla veya kamu yararına, bilimsel veya tarihi araştırma amaçlarına veya istatistiksel amaçlarla arşivlemek amacıyla kullanılabilir. İstisna, mahkeme işlemlerinde ya da idari ya da mahkeme dışı işlemlerde olsun, yasal iddiaların oluşturulması, uygulanması ya da savunulması için gerektiğinde bu tür kişisel verilerin işlenmesine de izin vermelidir.*
>
> *(53) Daha yüksek korumayı hak eden özel kişisel veri kategorileri, sağlıkla ilgili amaçlar için, özellikle de sağlık yönetimi bağlamında, gerçek kişilerin ve toplumun yararına bu amaçlara ulaşmak için gerekli olduğunda işlenmelidir. ... Üye devletlerin, genetik verilerin, biyometrik verilerin veya sağlıkla ilgili verilerin işlenmesiyle ilgili sınırlamalar da dâhil olmak üzere başka koşulları sürdürmelerine veya sunmalarına izin verilmelidir. Bununla birlikte, bu şartlar bu tür verilerin sınır ötesi işlemesi için geçerli olduğunda Birlik içindeki kişisel verilerin serbest akışını engellememelidir.*
>
> *54) Özel veri kategorilerinin işlenmesi, veri sahibinin rızası olmadan, halk sağlığı alanlarındaki kamu yararı için gerekli olabilir. Bu tür işlemler, gerçek kişilerin hak ve özgürlüklerini korumak için uygun ve özel önlemlere tabi tutulmalıdır. .... **Kamu yararı nedeniyle sağlıkla ilgili verilerin bu şekilde işlenmesi, kişisel verilerin işverenler veya sigorta ve bankacılık şirketleri gibi üçüncü şahıslar tarafından başka amaçlar için işlenmesiyle sonuçlanmamalıdır.***

Sigorta şirketlerinin işlediği özel nitelikli kişisel veriler, KVKK'nın 6. maddesinde öngörülmüş olan özel işleme şartlarına tabidirler. Şirket çalışanlarının, kişisel verilerin korunmasına ilişkin genel bilincin ötesinde bu gibi detayları ayırt edebilecek durumda olmaları gerekmektedir. Her türlü sağlık bilgisi "**özel nitelikli kişisel veri**"dir.

> ***Özel nitelikli kişisel verilerin işlenme şartları***
>
> ***MADDE 6-*** *(1) 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 özel nitelikli kişisel veridir.*

[4] https://tsb.org.tr/sigorta-tanimlari.aspx?pageID=648
[5] https://tsb.org.tr/sigortanin-tarihi.aspx?pageID=438

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

(3) Birinci fıkrada sayılan sağlık ve cinsel hayat dışındaki kişisel veriler, kanunlarda öngörülen hâllerde ilgili kişinin açık rızası aranmaksızın işlenebilir. 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 işlenebilir.

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

KVK Kurulu, *"Özel Nitelikli Kişisel Verilerin İşlenmesinde Veri Sorumlularınca Alınması Gereken Yeterli Önlemler"* ile aşağıdaki açıklamaları içeren bir karar almıştır;

"6698 sayılı Kişisel Verilerin Korunması Kanununun (Kanun) 6 ncı maddesinin (4) numaralı fıkrasında, "Özel nitelikli kişisel verilerin işlenmesinde, ayrıca Kurul tarafından belirlenen yeterli önlemlerin alınması şarttır." hükmü yer almaktadır.

Bu çerçevede, Kanunun 22 nci maddesinin (1) numaralı fıkrasının (ç) ve (e) bentleri uyarınca özel nitelikli kişisel veri işleyen veri sorumluları tarafından alınması gereken yeterli önlemler Kişisel

Verileri Koruma Kurulu tarafından aşağıdaki şekilde belirlenmiştir:

1- *Özel nitelikli kişisel verilerin güvenliğine yönelik sistemli, kuralları net bir şekilde belli, yönetilebilir ve sürdürülebilir ayrı bir politika ve prosedürün belirlenmesi,*
2- *Özel nitelikli kişisel verilerin işlenmesi süreçlerinde yer alan çalışanlara yönelik,*
   a) Kanun ve buna bağlı yönetmelikler ile özel nitelikli kişisel veri güvenliği konularında düzenli olarak eğitimler verilmesi,
   b) Gizlilik sözleşmelerinin yapılması,
   c) Verilere erişim yetkisine sahip kullanıcıların, yetki kapsamlarının ve sürelerinin net olarak tanımlanması,
   ç) Periyodik olarak yetki kontrollerinin gerçekleştirilmesi,
   d) Görev değişikliği olan ya da işten ayrılan çalışanların bu alandaki yetkilerinin derhal kaldırılması. Bu kapsamda, veri sorumlusu tarafından kendisine tahsis edilen envanterin iade alınması,
3- *Özel nitelikli kişisel verilerin işlendiği, muhafaza edildiği ve/veya erişildiği ortamlar, elektronik ortam ise;*
   a) Verilerin kriptografik yöntemler kullanılarak muhafaza edilmesi,
   b) Kriptografik anahtarların güvenli ve farklı ortamlarda tutulması,
   c) Veriler üzerinde gerçekleştirilen tüm hareketlerin işlem kayıtlarının güvenli olarak loglanması,
   ç) Verilerin bulunduğu ortamlara ait güvenlik güncellemelerinin sürekli takip edilmesi, gerekli güvenlik testlerinin düzenli olarak yapılması/yaptırılması, test sonuçlarının kayıt altına alınması,
   d) Verilere bir yazılım aracılığı ile erişiliyorsa bu yazılıma ait kullanıcı yetkilendirmelerinin yapılması, bu yazılımların güvenlik testlerinin düzenli olarak yapılması/yaptırılması, test sonuçlarının kayıt altına alınması,
   e) Verilere uzaktan erişim gerekiyorsa en az iki kademeli kimlik doğrulama sisteminin sağlanması,
4- *Özel nitelikli kişisel verilerin işlendiği, muhafaza edildiği ve/veya erişildiği ortamlar, fiziksel ortam ise;*
   a) Özel nitelikli kişisel verilerin bulunduğu ortamın niteliğine göre yeterli güvenlik önlemlerinin (elektrik kaçağı, yangın, su baskını, hırsızlık vb. durumlara karşı) alındığından emin olunması,
   b) Bu ortamların fiziksel güvenliğinin sağlanarak yetkisiz giriş çıkışların engellenmesi,
5- *Özel nitelikli kişisel veriler aktarılacaksa;*
   a) Verilerin e-posta yoluyla aktarılması gerekiyorsa şifreli olarak kurumsal e-posta adresiyle veya Kayıtlı Elektronik Posta (KEP) hesabı kullanılarak aktarılması,
   b) Taşınabilir Bellek, CD, DVD gibi ortamlar yoluyla aktarılması gerekiyorsa kriptografik yöntemlerle şifrelenmesi ve kriptografik anahtarın farklı ortamda tutulması,
   c) Farklı fiziksel ortamlardaki sunucular arasında aktarma gerçekleştiriliyorsa, sunucular arasında VPN kurularak veya sFTP yöntemiyle veri aktarımının gerçekleştirilmesi,
   ç) Verilerin kâğıt ortamı yoluyla aktarımı gerekiyorsa evrakın çalınması, kaybolması ya da yetkisiz kişiler tarafından görülmesi gibi risklere karşı gerekli önlemlerin alınması ve evrakın "gizlilik dereceli belgeler" formatında gönderilmesi gerekir.

6- *Yukarıda belirtilen önlemlerin yanı sıra Kişisel Verileri Koruma Kurumunun internet sitesinde yayımlanan Kişisel Veri Güvenliği Rehberinde belirtilen uygun güvenlik düzeyini temin etmeye yönelik teknik ve idari tedbirler de dikkate alınmalıdır.*

Kişisel veri güvenliğine ilişkin belirlenecek doğru ve tutarlı politika ve prosedürler, veri sorumlusunun çalışma ve işleyişine uygun şekilde entegre edilmelidir. Veri sorumlularınca politika ve prosedürler iyi bir şekilde ve zamanında hazırlanamadığında, sorunlu alanlar belirlenemediğinde veya mevcut güvenlik önlemleri kullanılamadığında kişisel veri güvenlik seviyesi yeteri kadar sağlanamamaktadır.[6]

Bilindiği gibi, sigorta sektöründeki hızlı tempolu değişim ve yenilik döneminde, veri ve teknolojinin birleşimi her iş alanı ile giderek iç içe geçmektedir. Her ne kadar KVKK/GDPR düzenlemelerinin daha zor bir uygulama getirdiği doğru olsa da veri koruma mevzuatı, ihlallere yönelik ciddi cezalar öngörürken bunun yanında yeni fırsatlar da sağlamaktadır. Uyumluluk, kişisel verilerin şeffaf bir şekilde işlenmesini ve verilerin güvende kalmasını sağlayan sistemlerin bulunmasını zorunlu hale getirirken, müşteri güvenini artıracak ve rekabette olumlu etkiler sağlayacaktır.

4.1. Kişisel Sağlık Verileri

Kişisel sağlık verileri, hem KVKK hem de GDPR düzenlemelerinde üzerinde hassasiyetle durulan konulardan birisidir. 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 ile ilgili olan üç tür kişisel veri tanımlanmıştır:[7]

- ***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.[8]

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 (*tıbbi kayıtlar)*[9] kişisel sağlık verisi olarak değerlendirilmektedir.

Hem KVKK hem de GDPR düzenlemelerinde, kişisel sağlık verilerine özel önem atfedilmekte olup, bu verileri işlenme ve korunma bakımından kritik bir veri türü haline getirmektedir. Bu da, bazı sigorta hizmetlerinde toplanan, işlenen ve paylaşılan kişisel sağlık verilerinden dolayı sigortacılık sektörünün düzenlemelere uyumluluğunu diğer sektörlere göre biraz daha fazla kritik bir noktaya taşımaktadır.

[6] Kişisel Veri Güvenliği Rehberi (Teknik ve İdari Tedbirler) s.11
[7] 2016/679 Sayılı Avrupa Genel Veri Tüzüğü (GDPR) m.4: Tanımlar
[8] 21 Haziran 2019 tarihli T.C. Sağlık Bakanlığı, Kişisel Sağlık Verileri Hakkında Yönetmelik
[9] TSE, Hastane Akreditasyon Tasarısı 1996

4.2. Türkiye Sigorta Birliği

Sigortacılık Kanunu'nun 24. maddesinde Türkiye Sigorta Birliği'nin sigortacılık mesleğinin geliştirilmesi, şirketler arasında dayanışma sağlanması ve haksız rekabetin önlenmesi amacıyla kurulan, tüzel kişiliği haiz kamu kurumu niteliğinde meslek kuruluşu olduğu hükmü yer almıştır.

Kanununda 29.Haziran.2012 tarihinde yapılan değişiklikle Birlik çatısı altına emeklilik şirketleri de dâhil edilmiş ve Birliğin unvanı "*Türkiye Sigorta, Reasürans ve Emeklilik Şirketleri Birliği*" olarak değiştirilmiştir. Bu değişimden sonra Birliğin logosu değiştirilmiş ve logo ile birlikte "*Türkiye Sigorta Birliği*" (*TSB*) ibaresinin kullanılması kararlaştırılmıştır.

Bugün itibariyle Birlik'in 40'ı hayat dışı, 17'si hayat ve emeklilik, 6'i hayat ve 3'u reasürans şirketi olmak üzere aktif olarak 66 üyesi faaliyette bulunmaktadır.[10]

TSB, KVKK kapsamında aşağıdaki veri sahiplerine ait kişisel verileri işlemektedir:[11]

- ✓ *Sigortalı/Sigorta Ettiren (Müşteri)*
- ✓ *Potansiyel Sigortalı/Sigorta Ettiren (Potansiyel Müşteriler)*
- ✓ *Eski Çalışan / Emekliler*
- ✓ *İş Ortağı Hissedarları, Yetkilileri, Çalışanları*
- ✓ *Tedarikçi Hissedarları, Yetkilileri, Çalışanları*
- ✓ *Çalışan ve Stajyer Adayları*
- ✓ *İş Ortağı Adayları*
- ✓ *Tedarikçi Adayları*
- ✓ *Ziyaretçiler*
- ✓ *Basın*
- ✓ *Üçüncü Kişiler*

TSB, kişisel verileri ve özel nitelikli kişisel verileri;

- ✓ *Birlik tarafından dış kaynak kullandığı süreçlerde hizmet alımını temin amacıyla tedarikçilere,*
- ✓ *İş ortaklığının amaçlarının yerine getirilmesini temin amacıyla iş ortaklarına,*
- ✓ *Hukuki yetkileri çerçevesindeki talep edilen bilgilerle sınırlı olarak Hukuken yetkili kamu kuruluşları ve hukuken yetkili özel kişi veya kuruluşlara*

aktarıldığını belirtmektedir.[12]

4.2. Sigorta Bilgi ve Gözetim Merkezi

Sigorta Bilgi ve Gözetim Merkezi (SBM), Sigortacılık Kanunu'nun 31/B maddesinin birinci fıkrasına istinaden kurulmuştur. Temel görevleri arasında, "*sigortacılık sektöründe **risk değerlendirmesine esas bilgileri toplamak** ve bu bilgileri sigortacılık faaliyetinde bulunan şirketler ile T.C. Hazine ve Maliye Bakanlığı'nın belirlediği **kişilerle paylaşılmasını sağlamak***" yer almaktadır.[13]

SBM'nin görevi, sigorta sektörü verilerini tek merkezde toplayarak, bu verileri güvenlikli bir şekilde saklamaktır. Ayrıca bilgi ve istatistik üretip sunmak, aldığı tedbirlerle sigorta sistemine olan güveni artırmak ve kamu gözetim-denetiminin etkinleştirilmesine yardımcı olmaktır.

Bu amaçla, ilgili tüm taraflar SBM tarafından istenilen "***her türlü bilgiyi vermekle yükümlüdür***". Benzer biçimde SBM de "***topladığı her türlü bilgiyi, Müsteşarlığa istenen biçim ve sürede vermekle yükümlüdür***." Ayrıca, SBM tarafından "*söz konusu bilgiler, sahibinin açık rızasının bulunması durumunda **belirlediği kişiye** belli bir ücret karşılığında verilir.*"

[10] https://www.tsb.org.tr/hakkimizda.aspx?pageID=657
[11] https://tsb.org.tr/images/Documents/TSB_KVK_Veri_Isleme_Politikasi.pdf
[12] https://tsb.org.tr/images/Documents/TSB_KVK_Veri_Isleme_Politikasi.pdf
[13] https://www.sbm.org.tr/tr/sayfa/sbm-hakkinda-63

Diğer taraftan SBM, Araç Sorgulama Hizmetleri için 11890.com.tr hizmetinin sunumunda Pluss Telekom ile işbirliği yaparak müşterilerine hizmet sunarken, kişisel verileri toplama ve kaza sorgulamalarına ait bilgileri de yine bu şirket sistemleri aracılığıyla iletmektedir.[14]

Yine benzeri biçimde SMS5664 hizmetini de mevcut 3 mobil iletişim şirketleri üzerinden sağlamaktadır; [15]

> *"Turkcell, Türk Telekom, Vodafone ile anlaşmalı olarak devreye alınmış olan SMS projesi ile kişiler mesaj atarak arabalarının hasar geçmişlerini, araç detay bilgilerini, eksper raporuna göre değişen parçalarını Turkcell, Türk Telekom, Vodafone "5664"e mesaj atarak sorgulayabilirler."*

SBM, kişisel veriler açısından çeşitli ve karmaşık iş yükü ve iş süreçleri içeren bu hizmetlerin sunumunda, **birçok kişi ve kuruma bilgi ve veri aktarımı** yapmaktadır. Bu da verilerin saçılma riskini de artırmaktadır.

4.3. KVKK/GDPR ve Sigortacılık Sektöründeki Yükümlülükler

Düzenlemelere göre sigorta şirketleri, TSB ve SBM çoğu durumda işledikleri kişisel veriler (*örneğin, personel kayıtları ve müşteri kayıtları*) ile ilgili olarak doğrudan **veri sorumlusu**, üçüncü taraflardan alarak kendi bilişim sisteminde kaydedip saklamakta olduğu kişisel veriler için de **veri işleyen** niteliğini haiz olmaktadırlar. Bu durum, ilgili tarafların gerek doğrudan **veri sorumlusu**, gerekse de **veri işleyen** niteliği ile hem kendisinin eylemlerinden **doğrudan** hem de kişisel verileri paylaştıkları tarafların işleyeceği eylemlerden dolayı **müştereken sorumluluklar** doğurmaktadır.

Veri koruma düzenlemeleri, sigorta şirketlerinin iş süreçlerinde ilgili kişilerin kişisel verilerinin güvenliğinin sağlanması yönelik bir takım yükümlükler getirmiştir. Sigorta sektörünün bu yeni düzenleme ve yükümlülüklere uyum zorunluluğu vardır. Bu durum, KVKK uyarınca bu sigorta şirketleri ve SBM tarafından, yapılan işlemler ile ilgili çok kapsamlı ve detaylı bir **uyumluluk çalışmalarının** (*"**veri envanteri**" hazırlanması ve "**risk/etki analizleri**" gibi*) 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.

Veri sorumlusu sıfatıyla sigorta şirketleri ve SBM Kişisel Verilerin Korunması Kanunu'nda sayılan "*ilkeler*"e ve "*veri işleme şartları*"na eksiksiz uymakla yükümlüdürler. Örneğin, kanunlarda "*açıkça*" öngörülen haller dışında kişisel verilerin sahibinden *(ilgili kişi)* "açık rıza" almadan veri işleyemezler.

Kişisel verilerin aktarılması, paylaşılması, silinmesi, yok edilmesi ve işlenmesi, sağlık ve hayat sigortalarının uygulamalarında düzenlemeler açısında bir takım zorlukları beraberinde getirmektedir. Kişilerin sağlık verilerinin sigorta şirketleri tarafından biliniyor olması, sağlık sigortaların düzenlemesi noktasında, ilgili kişinin sigortalanması açısından sıkıntılara yol açacak veya sağlıklı bir kişiye göre çok daha yüksek miktarda bir poliçe bedelini gündeme getirecektir.

Diğer taraftan sigortacılık işlemlerinde kullanılan kişisel sağlık verileri, sigortacılık işlemleri gereği bizzat sigorta şirketleri tarafından toplanmaktadır. Sigorta şirketleri ve SBM verdikleri hizmetler sürecinde topladıkları kişisel veriler ile kişisel sağlık verilerini doğrudan veya dolaylı olarak bir takım kişi veya kurumlarla paylaşmaktadırlar.

Kanun'da sayılan istisnai işleme şartlarından herhangi birinin bulunmaması halinde, 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.

Ayrıca T.C. Sağlık Bakanlığı, "*Kişisel Sağlık Verileri Hakkında Yönetmelik*" ile KVKK'da belirtilen "*özel nitelikli kişisel veriler*" kapsamındaki "***kişisel sağlık verilerini***" özel olarak düzenlemiştir.

[14] 11890.com.tr / 11890 Çağrı Merkezi Hizmeti, Sigorta Bilgi ve Gözetim Merkezi ve Pluss Telekom İletişim Ticaret A.Ş işbirliği ile sunulmaktadır.
[15] https://www.sbm.org.tr/tr/sayfa/sms-sorgulamalari-7

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, sigorta şirketleri ile SBM arasında, kamu-özel üçüncü kişiler arasında, başka ülkelere veri gönderilmesi gibi*) ek yükümlülükler getirmekte, hatta belirli durumlarda Kişisel Verilerin Korunması Kurulu'nun iznini şart koşmaktadır.

Sigorta şirketlerinin ve SBM'nin kişisel verileri işlenen gerçek kişilere *(ilgili kişi*) yönelik doğrudan yükümlülükleri de bulunmaktadır. İlgili kişilerin kendileriyle ilgili olarak işlenen veriler bakımından tam ve doğru şekilde veri sorumlusu tarafından işleme öncesinde (*en geç veri işlemesi esnasında*) aydınlatılması gerekir. Bu sorumluluğun yerine getirilmemesi veya gereği gibi yerine getirilmemesi sigorta şirketlerinin veya SBM'nin doğrudan sorumluluğunu doğurur. Aynı şekilde ilgili kişilerin KVKK ile özel olarak koruma altına alınmış olan haklarına sigorta sektörü çalışanları tarafından riayet edilmemesi de aynı şekilde hukuki sorumluluklar doğuracaktır.

Veri güvenliğinin Kanun'da öngörülen çerçevede tesis edilmesi sigorta şirketleri ve SBM için başlı başına bir yükümlülüktür. Bu yükümlük sadece hukuki ve idari tedbirlerle sınırlı olmayıp, aynı zamanda çeşitli teknik tedbirlerin alınmasını zorunlu kılmaktadır.

Tüm bunların yanı sıra, banko, gişe, masa gibi hizmet alanlarında kişisel verilerin korunmasına yönelik Kişisel Verileri Koruma Kurulu'nun 21/12/2017 Tarihli ve 2017/62 Sayılı İlke Kararı[16] da hem sigortacılık hem de bankacılık alanında önem taşımaktadır. Karara göre; bankacılık ve sağlık sektörleri başta olmak üzere birden fazla çalışan ile birlikte bitişik düzende hizmet veren posta ve kargo hizmetleri, turizm acenteleri, zincir mağazaların müşteri hizmetleri bölümleri, çeşitli abonelik işlemlerinin yapıldığı kuruluşlar ile belediye, vergi ve nüfus ile ilgili işlemler gibi hizmetlerin verildiği kamu ve özel sektör kurum ve kuruluşlarının, 6698 sayılı Kişisel Verilerin Korunması Kanununun 12 nci maddesi uyarınca kişisel verilerin korunması ile ilgili olarak; banko/gişe/masa gibi bölümlerde yetkisi olmayan kişilerin yer almasını önleyecek ve aynı anda birbirlerine yakın konumda hizmet alanların birbirlerine ait kişisel verileri duymasını, görmesini, öğrenmesini veya ele geçirmesini engelleyecek nitelikte gerekli teknik ve idari tedbirleri alması gerekmektedir.

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

GDPR düzenlemeleri, verilerin nerede tutulduğuna bakılmaksızın, AB yerleşik bireylere ait kişisel verilerin, özellikle de kişisel sağlık verilerinin işlenmesi durumunda AB dışındaki kurum ve kuruluşları da kapsamaktadır.[17] **AB'de yerleşik veri sahiplerine mal ve hizmet sağlayan ya da davranışlarını izleyen** AB üyesi olmayan veri sorumlusu ve/veya veri işleyenleri, dolayısıyla bu işlemleri yapan sigortacılık şirketlerini de kapsayacaktadır.[18] Bu sebepten dolayı sigorta şirketleri ve SBM aynı zamanda GDPR yükümlüsü durumundadırlar.

KVKK sorumluluk ve yükümlülüklerinin yanı sıra, yaptığı iş ve işlemler ile aktardığı veya aktarılan bir takım kişisel verilerden dolayı GDPR kapsamına girecek sigorta şirketlerinin GDPR düzenlemeleri gereğince ek bazı teknik, idari ve cezai sorumluluk ve yükümlülükleri de bulunabileceği, GDPR yaptırımlarının sonuçlarının ise daha ağır olduğu göz önünde bulundurulmalıdır.

Sigortacılık sektörü de bu düzenlemelerden en fazla etkilenecek alanlardan biri olup yeni düzenlemelere en etkili ve verimli biçimde uyumluluk sağlaması gerekmektedir.

Süreç içerisinde etkili veri koruma denetimleri uygulandığında bazı sıkıntı ve zorluklar gelecektir. GDPR düzenlemeleri sonrasında kişisel verilerin toplanması, işlenmesi ve paylaşılması, bu düzenlemeler açısından

[16] https://kvkk.gov.tr/Icerik/4114/2017-62
[17] Avrupa Genel Veri Koruma Tüzüğü (GDPR) m.3
[18] EDPB Guidelines 3/2018 on the territorial scope of the GDPR (Article 3) - version adopted after public consultation

bazı uyumsuzluklara yol açabileceğinden ülkemizde sigortacılık hizmeti veren kurum ve kuruluşları büyük para cezaları ve itibar kaybı gibi ciddi riskler beklemektedir.

Sağlıklı bir uyumluluk süreci, yasal yükümlülüklerin yanısıra ticari faydalar da sağlayacaktır. Müşterilerinin, çalışanlarının ve iş ortaklarının mahremiyetini koruyan ve uygun şekilde hedeflenmiş çalışmalar yürüten sigorta şirketlerinin, iş, personel ve müşteriler için daha güvenli ve tercih edilir olmalarını beraberinde getirecektir.

4.4. KVKK/GDPR ve Sigortacılık Sektöründeki Riskler

Sigortacılık, kişisel veriler açısından çeşitli ve karmaşık iş yükü ve iş süreçlerine sahip bir sektör olup, **birçok kişi ve kuruma** (*niteliğine bağlı olarak ulusal ve uluslararası*) **bilgi ve veri aktarımı** yapmaktadır. Sigortacılık sektöründe toplanan, işlenen ve paylaşılan verilerin önemli bir kısmını da kişisel sağlık verileri gibi KVKK'da **özel nitelikli** veriler kapsamında değerlendirilen veriler oluşturmaktadır.

Bütün bu verilerin miktarı ve çeşitliliğinden kaynaklanan risklerin sonucu olarak bilgi güvenliği konusunda farkındalığın en yüksek olduğu sektörlerin başında sigortacılık sektörü gelmektedir.

Sigorta sektörü, özellikle temel siber güvenlik farkındalığı açısından bilişim ve iletişim firmalarından (*%31'e karşılık, tüm işletmeler arasında %13*) sonra ikinci sırada (*%24*) yer almaktadır.[19]

Bu nedenle, siber güvenliğe öncelik veren iş sektörleri arasında finans ve sigortacılık ilk sırayı almaktadır:[20]

- ✔ Finans ve Sigorta (*%71*, tüm işletmelerin ortalaması *%40*)
- ✔ Bilgi ve İletişim (*%57*)
- ✔ Sağlık, Sosyal Hizmetler ve Sosyal Bakım (*%56*).

Benzer biçimde finans ve sigorta sektörü (*%70*) ve bilgi ve iletişim firmalarının (*%53*) siber güvenlik temel bilgisine sahip yönetici sayısı ortalamanın (*%37*) üzerindedir.[21]

Diğer taraftan aynı araştırma, özel işletmeler arasında, müşteriler hakkında **kişisel verileri toplama ve saklama oranının en yüksek** olduğu sektörlerin başında da finans ve sigortacılık sektörlerinin geldiğini göstermektedir:[22]

- ✔ Finans ve Sigorta (*%77, Genel Olarak %55*)
- ✔ Yönetim ve gayrimenkul (*%70*)
- ✔ Sağlık, sosyal hizmet ve sosyal bakım (*%68*).

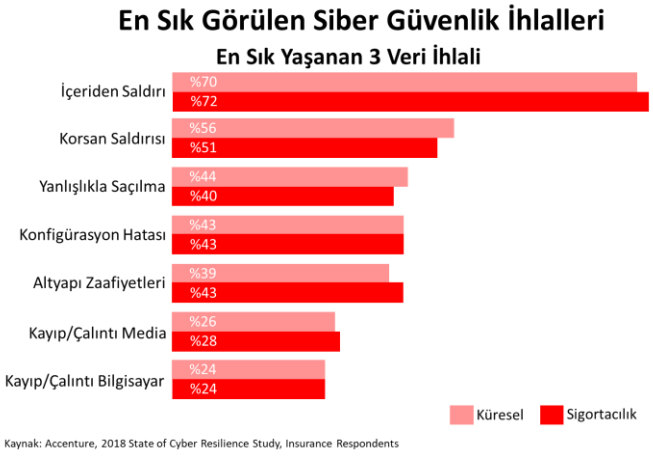
"Tüm sigorta şirketleri, büyüklük, karmaşıklık veya iş kollarından bağımsız olarak, çeşitli üçüncü taraflarla (örn. Hizmet sağlayıcılar, aracılar ve reasürörler) bazı durumlarda ***sağlıkla ilgili hassas bilgiler olmak üzere önemli miktarda özel ve gizli poliçe sahibi verisi toplar, depolar ve paylaşır****. Sigorta şirketlerinin verilerinin gizliliğinin, bütünlüğünün ve kullanılabilirliğinin korunması büyük önem taşımaktadır. Siber suçla sigorta şirketlerinden elde edilen bilgiler gasp, kimlik hırsızlığı, fikri mülkiyetin kötüye kullanılması veya diğer suç faaliyetleriyle finansal kazanç için kullanılabilir. Kişisel verilerin yanlışlıkla veya kasıtlı olarak ihlale maruz kalması, etkilenen poliçe sahiplerine ciddi ve kalıcı zarar vermenin yanı sıra sigortacı sektör katılımcılarına itibar zararıyla da sonuçlanabilir. Benzer şekilde, sigortacının kritik sistemlerine yönelik kötü amaçlı siber saldırılar, iş yapma yeteneğini engelleyebilir."*[23]

Sigorta şirketleri **işledikleri kişisel verilerin niteliği ve yüksek hacmi nedeni ile yüksek risk grubu içerisinde bulunmaktadır**.

[19] https://www.gov.uk/government/publications/cyber-security-breaches-survey-2020/cyber-security-breaches-survey-2020
[20] https://www.gov.uk/government/publications/cyber-security-breaches-survey-2020/cyber-security-breaches-survey-2020
[21] https://www.gov.uk/government/publications/cyber-security-breaches-survey-2020/cyber-security-breaches-survey-2020
[22] https://www.gov.uk/government/publications/cyber-security-breaches-survey-2020/cyber-security-breaches-survey-2020
[23] IAIS, Issues Paper on Cyber Risk to the Insurance Sector (August 2016)

Nitekim bu konuda yapılan araştırmalar, siber saldırılardan en fazla zarar görenlerden birisi sigortacılık sektörüdür. Siber saldırıların sigortacılık sektörüne ortalama ihlal maliyeti her geçen yıl artmaktadır;[24]

Özellikle sigortacılık sektöründe yaşanan veri ihlallerindeki iç tehditlerin sayısının harici saldırganlara göre daha fazla olması, çalışanlar ve yüklenicilerde büyük bir iş gücüne sahip olması nedeniyle sigorta şirketlerini risklerini daha da artmaktadır. [25]



Türkiye özelinde bu risklere teknolojik altyapı eksikliğinden kaynaklanan sorunlar da eklenmektedir.

> *Gerçekleştirilen görüşmeler doğrultusunda; B ve C tipi acentelerin çoğunlukla geleneksel yöntemler ile satış yaptıkları ve teknolojik altyapılarını yeteri kadar geliştirmedikleri gözlenmiştir. Acenteler, potansiyel müşterilerini ilgilenebilecekleri ürünlerden ve fırsatlardan haberdar etmeli, müşteri portföylerini genişletmenin yollarını aramalıdır. Her tip satış kanalı kurgusunu kendi bünyesinde bulundurabilen, altyapıları güçlü acenteler özellikle ilerleyen yıllarda diğer acentelerden ayrılacak ve müşterilerine daha kaliteli hizmet sundukları için yüksek prim üretimlerine ulaşabileceklerdir. Altyapı kısıtları olan ve gerekli yatırımı yap(a)mamış acenteler ile prim üretimi ve sermayesi yüksek olup ya da sigorta şirketinin desteğiyle donanımlarını kuvvetlendirmiş, operasyonel iş yüklerini en aşağı seviyeye çekip verimliliğini arttırmış acenteler arasındaki farkın giderek açılması beklenmektedir.*[26]

Olası para cezası yaptırımının yanı sıra, söz konusu şirketlerin **marka imajının ciddi şekilde zedelenmesi, yani itibar kaybı ile müşteri kaybı da** para cezasından daha etkili sonuçlara yol açmaktadır.

[24] The Cost Of Cybercrime, Ninth Annual Cost Of Cybercrime Study, Unlocking The Value Of Improved Cybersecurity Protection, Accenture Security, 2019
[25] Insuring the Future, 2018 State of Cyber Resilience for Insurance, Accenture Consulting s.9
[26] TOBB Sigorta Acenteleri İcra Komitesi / Sigorta Acenteleri Dünya Uygulamaları Araştırma ve 2023 Vizyonu Belirleme Deloitte, 2016

Bu kapsamda, örnek olarak veri ihlali deneyimlemiş **aynı sektördeki** iki şirket olan **Target** ve **Home Depot**'un verileri aşağıda sunulmaktadır:[27]

	Target	Home Depot
Etkilenen Kişi Sayısı	40 milyon	56 Milyon
Fark Etme Süresi	Haftalar	Günler
Tepki Kalitesi	Düşük	Yüksek
ABD'deki aynı mağaza satışlarındaki fark (%QoQ)	-%0,4	+%5,8
Üç aylık kazançlardaki fark	-%46	+%14
Hisse Fiyatı	-%11,9	+%4,3
Yönetici Kaybı	CEO+CIO	Yok

Bu doğrultuda ihlal sonrası dönemi **başarılı bir şekilde yönetebilen** Home Depot'un gelirinin **%14 oranında arttığı** ve şirketten herhangi bir üst düzey yetkilinin ayrılmadığı gözlenmiş ancak **ihlal sonrası aksiyon almakta başarısız olan** Target firmasının gelirinin **%46 oranında azaldığı** ve **CEO ve CIO pozisyonunda yer alan üst düzey yetkililerinin görevden ayrılmak zorunda** kaldıkları görülmüştür.

Diğer yandan, Sigortacılık Kanunu *"sigorta brokerleri (m.21/5), sigorta eksperleri (m.22/15), sigorta acenteleri (m.23/17), Birlik yönetim ve denetiminde yer alanlar (m.25/20) ile bunların yanlarında çalışanların, tahkim Komisyonunda görev alanlar, hakemler ve raportörlerin, (m.30/19)* ***işleri dolayısıyla öğrendikleri bilgi ve sırları*** *ilgililerin izni olmaksızın açıklayamayacaklarına"* hükmetmektedir. Ayrıca, "bu *Kanunun uygulanmasında ve uygulanmasının denetiminde görev alanlar, bu Kanuna tâbi kuruluşların görevlileri ve yetkilileri, bu Kanuna tâbi kişiler ile bunların yanında çalışanlar ve dışarıdan hizmet alımı yoluyla sigortacılık sektöründe iş görenler, ...* ***sigorta sözleşmesi ile ilgili kişilere ait sırları bu konuda kanunen açıkça yetkili kılınan mercilerden başkasına açıklayamaz****. (m.31/A-1)"*

Ancak, *"gizlilik sözleşmesi yapılması ve sadece risk değerlendirmesi amacıyla kullanılmak üzere sigorta şirketi, reasürans şirketi ve emeklilik şirketlerinin kendi aralarında doğrudan doğruya ya da Sigorta Bilgi ve Gözetim Merkezi vasıtasıyla yapacakları her türlü bilgi ve belge alışverişi sırasında sigorta şirketi, reasürans şirketi ve emeklilik şirketlerine ya da sigorta sözleşmesi ile ilgili kişilere ait, yanlış sigorta uygulamaları dâhil,* ***sır niteliğindeki bilgilerin öğrenilmesi ve paylaşımı sır saklama yükümlülüğü dışında*** *(m.31/A-2)"* bırakılmıştır.

KVKK, sigorta mevzuatında yer alan **sır tutma** sorumluluklarına ek olarak bir dizi yeni yükümlülükler getirmiştir. Ayrıca, Sigortacılık Kanunda yer alan sır tutma muafiyeti, **KVKK açısından bir muafiyet sağlamamaktadır**. Dolayısıyla, Sigortacılık Kanunu gereği sır tutma muafiyeti getiren "*sadece risk değerlendirmesi amacıyla*" ile yapılan kişisel verilerin paylaşımları, KVKK açısından **kurumların idari para cezasına**, **kişilerin ise doğrudan hapis cezasına** çarptırılma risklerini doğurmaktadır.

Mevcut Sigortacılık Mevzuatı KVKK bağlamından bakıldığında, veri güvenliği ve bilgi gizliliği konularına yer verilmiştir. Hâlbuki KVKK veri güvenliği dışında işleme şartları ve işleme ilkeleri koymuş ve bunlara uyumu zorunlu kılmıştır. Nitekim kişisel veri ihlallerinden dolayı kesilen cezaların çoğu "*gerekli idari ve teknik tedbirlerin*" eksikliğinden kaynaklanmaktadır.

Günümüzde siber saldırganların hedefindeki başlıca sektörler içerisinde yer alan sigortacılık, kişisel veri, özellikle de kişisel sağlık verilerinin güvenliği konusu büyük riskler taşımaktadır. Bu risklerin başında birçok kişisel verilerinin aktarıldığı ve barındırıldığı SBM merkezi bilgi sistemi altyapısı yer almaktadır.

> *(2) Bu maddenin birinci fıkrasında belirtilen şirketler, Sigorta Bilgi ve Gözetim Merkezine üye olmak zorundadır. Üye kuruluşlar, Sigorta Bilgi ve Gözetim Merkezince istenilen* ***her türlü bilgiyi vermekle yükümlüdür****.*
>
> *(3) Sigorta Bilgi ve Gözetim Merkezi kuruluş amaçları doğrultusunda, özel hukuk tüzel kişileri ile kamu kurum ve kuruluşlarından, kamu kurumu niteliğinde meslek kuruluşları ve bunların üst kuruluşlarından, ilgili mevzuatla kurulmuş diğer bilgi merkezlerinden bilgi talep etmeye ve bunlarla Müsteşarlığın uygun görüşüne istinaden bilgi*

[27] https://www.linkedin.com/pulse/gdpr-banks-breaches-billion-euro-fines-why-72hr-risk-thomas

alışverişine yönelik sözleşmeler imzalamaya yetkilidir. Söz konusu kurum ve kuruluşlar Sigorta Bilgi ve Gözetim Merkezi tarafından ***talep edilen bilgileri vermekle yükümlüdür****. Sigorta Bilgi ve Gözetim Merkezinde toplanan bilgilerin bilgi sahibinin kendisi veya onay vermesi durumunda bu madde uyarınca Sigorta Bilgi ve Gözetim Merkezi ile bilgi alışverişine ilişkin sözleşme yapan özel hukuk tüzel kişileri, kamu kurum ve kuruluşları ile kamu kurumu niteliğinde meslek kuruluşları ve bunların üst kuruluşlarıyla anılan sözleşmeler çerçevesinde* ***paylaşılması*** *bu Kanunun 31/A maddesinin ikinci fıkrası kapsamında değerlendirilir.*

(5) Sigorta Bilgi ve Gözetim Merkezinin ***bütün işlem*** *ve* ***kayıtları gizlidir****. Sigorta Bilgi ve Gözetim Merkezi* ***topladığı her türlü bilgiyi, Müsteşarlığa istenen biçim ve sürede vermekle yükümlüdür****. Söz konusu bilgiler, sahibinin açık rızasının bulunması durumunda* ***belirlediği kişiye*** *belli bir ücret karşılığında verilir.*

(6) Sigorta Bilgi ve Gözetim Merkezi nezdinde bulunan sır niteliğindeki bilgileri, bu konuda kanunen yetkili kılınan mercilerden başkalarına açıklayanlar, hukuka aykırı olarak kendisi ya da başkası yararına kullananlar, yayanlar, verenler, aktaranlar veya ele geçirenler hakkında 35 inci maddenin dokuzuncu ve onuncu fıkraları hükümleri uygulanır. Bu fıkrada tanımlanan suçların bir tüzel kişinin faaliyeti çerçevesinde işlenmesi halinde, ilgili tüzel kişi hakkında 26/9/2004 tarihli ve 5237 sayılı Türk Ceza Kanununun ***tüzel kişilere özgü güvenlik tedbirlerine*** *hükmolunur.*

Bir diğer önemli risk ise, sigortacılıkta toplanan kişisel sağlık verileri de dâhil olmak üzere tüm kişisel verilerin **çeşitli üçüncü tarafa aktarılıyor** olmasıdır. (*SBM, Denetleme, Tahkim vb*).

m.28 (4) Sigorta denetleme uzmanları, sigorta denetleme aktüerleri ile bunların yardımcıları; sigorta şirketleri ve reasürans şirketleri ile bunların bağlı ortaklıkları, iştirakleri, şubeleri ile temsilciliklerinden, aracılar ve bankalar da dahil olmak üzere diğer kişilerden bu Kanun ve diğer kanunların sigortacılıkla ilgili hükümleri bakımından gerekli görecekleri bilgileri istemeye ve bunların tüm defter, kayıt ve belgelerini incelemeye yetkilidir.

m.30 (15) Sigortacılık yapan kuruluşla uyuşmazlığa düşen kişinin Komisyona başvurusu, öncelikle raportörler tarafından incelenir. Raportörler en geç onbeş gün içinde incelemelerini tamamlamak zorundadır. Raportörler tarafından çözümlendirilemeyen başvurular sigorta hakemine iletilir. Uyuşmazlığa hangi sigorta hakeminin bakacağı, Komisyon tarafından sigorta hakemi listesinden seçilir. Komisyon, işin niteliğine bağlı olarak en az üç sigorta hakeminden oluşan bir heyet oluşturulmasına karar verebilir.

Ayrıca bazı kişisel verilerin de başta AB ülkeleri olmak üzere ilgili diğer ülkelere aktarılması söz konusudur.

Mütekabiliyet çerçevesinde ve bu Kanunun uygulanması ile ilgili olarak ***yabancı ülke kanunlarına göre denetime yetkili mercilerin****, kendi ülkelerindeki sigortacılık sektöründe faaliyet gösteren kuruluşların bu Kanuna tâbi* ***Türkiye'deki teşkilât veya ortaklıklarında denetim yapma ve bilgi isteme*** *taleplerinin yerine getirilmesi Müsteşarlığın iznine tâbidir. Bu mercilerce istenen bilgiler, açıklanmaması kaydıyla Müsteşarlık tarafından verilebilir. Müsteşarlık, yabancı ülkelerin denetime yetkili mercileri ile yapacağı anlaşmalar çerçevesinde* ***sigortacılıkla ilgili her türlü işbirliği ve bilgi alışverişinde*** *bulunabilir. (m.29 (2))*

Tüm bunlar göz önünde bulundurulduğunda böylesine geniş bir ağ ve sistemi yönetmenin zorluğu ve karmaşıklığı yanında önemli güvenlik riskleri de bulunmaktadır. 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.

Siber saldırganların sigortacılık 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 mümkündür. Bu bilgilerin günümüzde çok değişik amaçlarla kullanıldığı bilinmektedir. Bu durum siber ortamda ticari bir sektör haline gelmiştir.

Hem siber sigortanın sigortacıları hem de finans sektöründeki katılımcılar olarak sigortacılar, siber güvenlik olaylarının yıkıcı potansiyeline veya finansal etkisine karşı bağışık değildir.[28]

"*Siber risk, sigorta sektörü için büyüyen bir zorluk teşkil etmektedir ve [Sigorta Temel İlkeleri] uyarınca denetçilerin ele almak zorunda olduğu bir sorundur.* ***Sigortacılar önemli miktarlarda gizli kişisel ve ticari***

[28] OECD, Enhancing the Role of Insurance in Cyber Risk Management (December 2017)

***bilgi toplar, depolar ve yönetir**. Bu veri rezervuarları nedeniyle sigortacılar, daha sonra gasp, kimlik hırsızlığı veya diğer suç faaliyetleri yoluyla finansal kazanç için kullanılabilecek bilgiler arayan **siber suçlular için başlıca hedeflerdir**. Ayrıca, sigorta şirketleri küresel finans sektörüne önemli katkılarda bulunduğundan, siber güvenlik olayları nedeniyle sigorta sistemlerinin kesintilerinin çok geniş etkileri olabilir. "*[29]

Sigorta şirketlerinin müşterileri hakkında kredi kartı ve ödeme verileri de dâhil büyük miktarda kişisel veriye sahip oldukları için bilgisayar korsanları (*hackers*), kimlik hırsızları ve dolandırıcıları tarafından daha fazla saldırıya uğramaktadır. Siber saldırıların giderek sayısı artan yüksek profilli veri ihlali *(ABD Personel Yönetimi Ofisi, Anthem, Premera Blue Cross, Target, JP Morgan Chase, Neiman Marcus, Hone Depot ve Equifax vb*) A.B.D. hükümetinin siber güvenlik konusundaki incelemesini hızlandırdı. Bu, bir siber saldırının yol açtığı sayısız riske yol açmaktadır; [30]

1) Kimlik hırsızlığı,
2) İş kesintisi,
3) İtibar kaybı,
4) Veri onarım maliyetleri,
5) Müşteri listelerinin veya ticari sırlarının çalınması,
6) Donanım ve yazılım onarım maliyetleri,
7) Etkilenen tüketiciler için kredi izleme hizmetleri ve
8) Dava masrafları.

A.B.D.de son yıllarda sağlık sigortası bilgilerine yönelik iki büyük veri ihlali olmuştur; Anthem ve Premera Blue Cross. Bu durum, sigorta sektöründeki siber güvenlik tedbirleri konusunda ciddi tereddütler doğurmuştur.

A.B.D. Ulusal Sigorta Komisyoncuları Birliği (NAIC) sigorta şirketlerinde ve NAIC'de barındırılan bilgilerin korunması, sigortacılar tarafından toplanan tüketici bilgilerinin korunması ve piyasada yayınlanan siber sorumluluk politikaları hakkında bilgi toplayarak NAIC'a tavsiyelerde bulunmak ve siber güvenlik konusundaki çalışmaları koordine etmek üzere bir Görev Gücü (*Task Force*) kurmuştur.[31]

Bu durumun dünyada nasıl etkin sonuçlar doğurduğu ve ne denli önemli önlemler alındığı görülmektedir.

Ülkemizde dünya uygulamalarına göre yeni yürürlüğe giren kişisel veri koruma düzenlemeleri 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 sigorta 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.

KVKK'nın 17. maddesinde işaret edildiği üzere, **TCK 135 ile 140** arasında düzenlenmiş olan suç ve cezalar öncelikle kişisel verilerin korunmasını ihlal eden fiilleri kapsamaktadır. Kişisel verilerin korunması ile ilgili suç teşkil eden fiilleri işleyenlere, her bir fiil için 1 yıldan 6 yıla kadar hapis cezaları öngörülmektedir.

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 sigorta şirketleri ve SBM bakımından önemli bir risktir.

Kişisel verilerin korunmasına ilişkin yükümlüklerin ihlali beraberinde özel hukuk hükümlerine göre sigorta şirketleri ve SBM'nin sorumluluğunu doğuracaktır. KVKK 14. maddesinde bu hususa "*Kişilik hakları ihlal edilenlerin, genel hükümlere göre tazminat hakkı saklıdır*" demek suretiyle işaret edilmektedir. Kişisel verilerin

[29] IAIS, Issues Paper on Cyber Risk to the Insurance Sector (August 2016)
[30] https://content.naic.org/cipr_topics/topic_cybersecurity.htm
[31] http://live-naic-static.pantheonsite.io/Releases/2014_docs/insurance_regulators_establish_cybersecurity_task_force.htm

korunması bilinci yaygınlaştıkça, her geçen gün sayısı artarak devam edecek olan tazminat taleplerine muhatap olacaklardır.

İdari para ve disiplin cezaları ile hapis cezalarının yanı sıra KVKK'nın 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*."

Özellikle Avrupa yerleşik kişilerin sağlık verisi gibi özel nitelikli verilerini işleyen veri sorumlularının, her şeyden önce Avrupa'da kurulu bir temsilci atamaları ve işledikleri sağlık verileri gibi hassas veriler için "*Veri Koruma Etki Değerlendirmesi*" (*DPIA*) yapmaları gerekmektedir. Bu ve benzeri önkoşulları yerine getirmeyenler için bir önceki mali yılın yıllık **dünya çapındaki cirosunun %2**'sine kadar veya **10.000.000 €**'ya kadar (*hangi meblağ yüksek ise, o geçerlidir*) **idari para cezası** uygulanma riski bulunmaktadır.

Bir veri ihlali durumunda ise; bir önceki mali yılın yıllık **dünya çapındaki cirosunun %4**'üne kadar veya **20.000.000 €**'ya kadar (*hangi meblağ yüksek ise, o geçerlidir*) **idari para cezası** uygulanma riski vardır.

GDPR düzenlemelerinin sigorta sektörü için diğer bir ağır yaptırım ise üçüncü bir ülkedeki bir alıcıya veya uluslararası bir kuruluşa yönelik **veri akışlarının askıya alınması** durumudur.

Özel Bir Durum: Telematik Sigortacılık ve Bağlı Araçlar (Connected Vehicle)

Telematik sistem, araçlara takılan bir cihaz ile gerçek zamanlı veri aktarımı sağlayan bir sürüş izleme teknolojisidir. Bu teknoloji, hız limiti aşımı, frenleme, hızlanma, dönüş, kasis veya çukur geçişi ve sürüş süresi gibi sürücü davranışlarını analiz eder ve kişiye özel bir sürücü profili oluşturur.[32]

Sürücü profilini ve skorunu çıkaran sistem aracılığıyla sigorta şirketleri sürücüye özel indirim fırsatları sağlarlar. Bu sayede iyi sürücüler ödüllendirilir ve trafikte güvenli sürüş davranışları teşvik edilir.

Telematik sigortacılık ise, sürücünün araç kullanım davranışlarının yanısıra kullanım süresine bağlı (*Pay As You Drive/Usage Based Insurance*) olarak özel prim ve indirim olanakları da sağlar. Bu işlemler ise oldukça çeşitli ve fazla miktarda kişisel verilerin toplanmasını gerektirmektedir.

Teknolojik gelişmeler araçları değiştirirken, bu değişiklikler de araçların kullanımı ve araçlara yönelik hizmetleri de etkilemektedir. Bu anlamda en fazla etkilenecek sektörlerin başında sigortacılık gelmektedir.

Sigortacılık sektörünü etkileyen bir diğer gelişme de Avrupa Veri Koruma Kurulu (*EDPB*) tarafından 28.Ocak.2020 tarihinde yayınlanan bağlı araçlar (*connected vehicles*) için kişisel verilere yönelik rehber taslağı ile gündeme geldi.[33] Bu taslak kişisel veriler ile ilgili veri sorumlusu, ortak veri sorumlusu, veri sahibi, kişisel veriler, aydınlatma, rıza ve bunların uygulamalarına yönelik birçok kavramsal tartışmayı da beraberinde getirmiştir.

AB 2002/58 sayılı eGizlilik Direktifi (*ePrivacy Directive*), bir kişinin veri depolanan veya bilgiye erişilmesini sağlayan donanımını terminal ekipmanı olarak tanımlamış olup, bu kapsamda bağlı araç ve ona bağlı herhangi bir cihaz EDPB tarafından da "***terminal ekipmanı***" olarak kabul edilmiştir. Bu nedenle de günümüzde araçlar geleneksel bir araç gibi değil, bir cep telefonu, tablet veya dizüstü bilgisayar gibi değerlendirilmektedir.

Bir şirket araç havuzundaki araçları ve bu araçları kullanan değişik şirket çalışanları göz önüne alındığında ise, araba ile ilgili "*teknik veriler*" bile birden fazla gerçek kişinin verilerini içerecektir. Bu durumda, aydınlatmanın yapılıp yapılmayacağı, kimler tarafından ve nasıl yapılacağı, ne zaman yapılacağı oldukça zor ve karmaşık bir hal almakta, hatta genellikle de imkânsız olmaktadır. Benzer biçimde, aydınlatmanın usulüne

[32] https://www.sigortadunyasi.com.tr/2020/01/04/generaliden-telematik-hakkinda-merak-edilen-sorulara-yanit/
[33] EDPB Bağlı Araçlar Ve Mobilite İle İlgili Uygulamalar Bağlamında Kişisel Verilerin İşlenmesine İlişkin 7/2020 Numaralı Yönergeler Taslağı, 28.Ocak.2020

uygun yapıldığı varsayılsa bile rızanın alınması kendi başına soruna dönüşecektir. Rızanın kimden, ne zaman ve nasıl alınacağı, ne kadar süreyle veya hangi durumlarda geçerli olacağı yine bir probleme dönüşecektir.

TSB'nin de üyesi olduğu Avrupa Sigorta ve Reasürans Federasyonu (*Insurance Europe*) bu konuda sigortacıların aşağıdaki genel endişelerini dile getirmektedir;[34]

- *Uygulamada aracın sahibiyle ilgili olmayan sürücüler ve yolcular için rıza alınmasının zordur. Tüzük, yolcuların tanımlanamazlarsa rızanın gerekli olmaması gerektiğini açıklığa kavuşturmalıdır. Bu bağlamda, rıza almak imkânsızdır. Bu, veri koruma düzeyini düşürecek bir sonuç ortaya çıkartacak, bu da yolcuların kimliğiyle ilgili veri elde edilmesini gerektirecektir.*
- *Motorlu telematik sigortası, ancak sürücüler sürüş davranışlarıyla ilgili yanlış derecelendirmeleri düzeltebiliyorsa adil kabul edilebilir. Örneğin, trafik sıkışıklıkları genellikle ani hızlanma ve frenleme gerektirir ve bu tür davranışlar normal şartlar altında kötü sürüş olarak kabul edilir. Trafik durumunu doğrulamak için sürekli konum belirleme olmadan, sürücüler uygun sürüş davranışını kanıtlayamayacak ve sonuç olarak motorlu sigorta poliçeleri için haksız yere daha yüksek bir prim ödeyecektir. Telematik ve kullanıma dayalı sigorta poliçeleri bağlamında, kullanıcı için adil bir prim sağlamak için otomatik ve sürekli coğrafi konum belirlemeye izin verilmelidir.*

Dolayısıyla bağlı araçlar böyle değerlendirildikleri zaman da birkaç konu olağan kapsamlarından farklı olarak değerlendirilmelidir.

- **Veri Sahipleri**; Araç sahibi, Aracın sürücüsü, Araçtaki yolcular, Araç kiralama hizmetlerinde Aracı Kiralayanlar, Şirket araçlarını kullananlar.
- **Veri sorumlusu/Veri işleyenler**; Aracın üreticisi, araçta kullanılan eğlence ve bilgi sisteminin üreticisi, araçta kullanılan emniyet kemeri, hava yastığı, sensörlü lastik ve benzeri aksamların üreticileri, telefon işletmecisi, varsa internet sağlayıcısı, özellikle elektrikli araçlar için elektrik dağıtım şirketleri, **sigorta şirketleri**, bakım-onarım şirketleri.
- **Kişisel Veriler**; Araç sahibinin adı-soyadı, araç kimlik numarası (*VIN*), sürücünün adı-soyadı, yolcuların ad-soyadları, bunlara ait parmak izi, iris-retina bilgileri, **araç sürüş alışkanlıkları, konum bilgileri, araç ve sürüşe ait diğer veriler**.
- **Aydınlatma**; Veri sorumluları tarafından (*Aracın üreticisi, araçta kullanılan eğlence ve bilgi sisteminin üreticisi, araçta üçüncü taraflarca üretilen emniyet kemeri, hava yastığı, sensörlü lastik ve benzeri akşamların üreticisi, telefon işletmecisi, varsa internet sağlayıcısı, elektrik dağıtım şirketleri,* ***sigorta şirketleri****, bakım-onarım şirketleri*) / Veri sahiplerine (*Araç sahibi, aracın sürücüsü, arabadaki yolcular, kiralık araçlarda aracı kiralayanlar, şirket araçlarında aracı kullananlar*)
- **Rızanın Alınma Zamanı**; Araç satıldığında, Aracı kullanmaya başlarken, Araca ait veya arabadaki herhangi bir hizmeti (***sigorta gibi***) kullanmaya başlarken.
- **Yasal Dayanaklar**; Rıza, Yasalar, diğer düzenlemeler (*Genel Güvenlik Yönetmeliği, Euro NCAP gibi*), Hizmeti Kullanımı (*Sürücü Uyuşukluk ve Dikkat Dağınıklığı Uyarısı, Yerleşik Telefon Donanımı, Navigasyon Sistemi, Akıllı Hız Yardımı, Lastik Basınç Uyarısı gibi*), Meşru menfaat **(*Sürdükçe Öde (Pay-As-You-Drive) Sigortaları gibi*)**
- **Saklama Süreleri;** Araç üreticisi, Diğer üreticiler, Servis sağlayıcıları ve sigortacılar (*veri sorumluları*), her bir işleme işleminin amacına bağlı olarak ve yasal veya düzenleyici hükümlere göre ayrı ayrı saklama süresi belirlemesi gerekir.

GDPR düzenlemeleri gerçek kişilerin ilişkilendirilebileceği *"özellikle* ***benzersiz tanımlayıcılar****"dan*[35] *"gerçek kişiyi sağlık amacıyla* ***benzersiz olarak tanımlamak*** *için gerçek kişiye atanmış ... bilgiler"den*[36] *ve "****sadece***

[34] Insurance Europe, Position Paper Response to EDPB draft guidelines on processing personal data in the context of connected vehicles and mobility related applications, 18 March 2020/COB-DAT-20-023

[35] Avrupa Genel Veri Koruma Tüzüğü (GDPR) Recital.30

[36] Avrupa Genel Veri Koruma Tüzüğü (GDPR) Recital.35

kişisel bir kişinin benzersiz bir şekilde tanımlanmasına veya doğrulanmasına izin" [37] özelliklerden bahsetmektedir.

KVKK düzenlemelerinde ise "*Her türlü bilgi deyimi ile aslında sadece* ***bireyin kesin teşhisini sağlayan*** *ad, soyad, doğum tarihi, doğum yeri gibi bilgiler değil; aynı zamanda bireyin belirlenebilir kılınmasını sağlayan fiziki, ailevi, ekonomik, sosyal ve buna benzer özelliklere ilişkin bilgiler de kastedilmektedir.*

Kanunda, kişisel veriler sınırlı sayma yoluyla belirlenmediğinden, ***her somut olayın özelliğine göre kişisel verinin kapsamının genişletilmesinin de mümkün***" olduğu belirtilmektedir.[38]

GDPR düzenlemelerine göre, "*veri sorumlusu, özellikle çevrimiçi hizmetler ve çevrimiçi tanımlayıcılar bağlamında, erişim isteyen bir veri sahibinin kimliğini doğrulamak için tüm makul önlemleri almalıdır. Bir veri sorumlusu kişisel verileri yalnızca potansiyel taleplere yanıt verebilmek amacıyla tutmamalıdır.*" [39]

Gerçi diğer taraftan da; "*Bir veri sorumlusu tarafından işlenen kişisel veriler, veri sorumlusunun gerçek bir kişiyi tanımlamasına izin vermiyorsa, veri sorumlusunun yalnızca herhangi bir hükmüne uymak amacıyla veri sahibini tanımlamak için ek bilgi almak zorunda olmaması gerekir.*" hükmü ile belirli durumlarda "gerçek kişinin" tanımlayamayacağını da kabul etmektedir. [40]

Veri sahibinin "***benzersiz bir biçimde***" tanımlamanın mümkün olmadığı durumlarda GDPR açısından bu belirsizliklerin bir takım sıkıntılara yol açacağı açıktır. Benzer durum KVKK düzenlemeleri için de geçerli gibi görünmektedir.

Gerek düzenlemelerdeki tanımlardan veya boşluklarda, gerekse de bağlı araçlarda ortaya çıkan yeni durumlardan dolayı veri sahibinin, veri işleme sürecinden önce "***benzersiz bir biçimde***" tanımlanması her zaman ya mümkün olmamaktadır yada kolay olmamaktadır.

Bu durum kişisel verileri koruma düzenlemeleri açısından, sigorta hizmetleri için bazı durumlarda daha açık olmasına rağmen, belirli durumlarda ise karışıklığa neden olabilecek niteliktedir. Bu nedenle sigorta sektörünün tüm paydaşları ile birlikte, bağlı araçlar konusu başta olmak üzere, kendi iş alanlarında yeni teknoloji ve gelişmelerin etkisini, özellikle kişisel verilerin korunması açısından dikkatlice değerlendirmek ve buna göre durum ve stratejilerini güncellemek ve nihayet, gerekli hukuki, idari ve teknik önlemleri zamanında ve tam olarak alması gerekmektedir.

4.5. 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 sigorta 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 sigorta şirketlerinin iş, personel ve müşteriler için daha cazip olmaları ve bunları elinde tutması daha olasıdır.

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

Farkındalık

Sigorta şirketlerinin 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.

[37] Avrupa Genel Veri Koruma Tüzüğü (GDPR) Recital.51
[38] Örneklerle Kişisel Verilerin Korunması, KVKK Yayınları No:29
[39] Avrupa Genel Veri Koruma Tüzüğü (GDPR) Recital.64
[40] Avrupa Genel Veri Koruma Tüzüğü (GDPR) Recital.57

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 gerekli eğitimler verilmelidir.

Sigorta şirketleri tarafından çoğu zaman kişisel sağlık verileri de dâhil olmak üzere çok fazla miktarda kişisel veri toplanıp saklanmakta ve paylaşılmaktadır. Bu nedenle tüm çalışanlara 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 sigortacılık 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, acentelerle yapılan sözleşmelerin, personele yapılacak bildirimlerin yanı sıra uygun rıza formlarının da 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

Sigorta 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. Sigortacılık hizmeti 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. Sigortacılık sektöründe faaliyet gösteren bir kurum veya kuruluş, kişisel verilere, özellikle de kişisel sağlık verilerine 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 sigortacılık şirketlerinin gerektiğinde politikalarını ve prosedürlerini güncelleyerek, personelini düzenli olarak 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 sigorta şirketinin 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. Sigorta şirketleri 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.

Sigorta şirketleri, gerçekten risk odaklı, etkili ve verimli bir şekilde uyumluluk çalışmaları ile hem uyumluluk maliyetlerini hem de olası riskleri ve etkilerini en aza indirgemelidirler.

5. Sigortacılık Sektöründeki Yaptırım Örnekleri

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.

Özellikle 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. Özellikle GDPR ve dünyanın diğer bölgelerindeki benzeri düzenlemeler kişisel sağlık verilerinin saçılması konusunda ağır yaptırımlar uygulamaktadırlar.

Kişisel verilerin korunmasına yönelik düzenlemelerin uygulama örnekleri her geçen gün artmakta ve bu konuda diğer kurum ve otoritelere de rehber niteliğine dönüşmektedir. Ayrıca, bu ihlallerin yol açtığı zararlar için verilen tazminat kararları da, bu konunun mağdurları açısından ayrı bir emsal oluşturmaktadır.

5.1. KVKK Uygulamaları

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.

Sigorta Acentesi

Bir şikâyet üzerine yapılan incelemede veri sorumlusu sigorta acentesinin;

- ✓ *Yaptığı sosyal medya paylaşımlarında müşterilerinin adları, adresleri ve maskelenmiş biçimde kimlik numaralarının yer aldığı, bunların dışında bazı hallerde kişisel veri niteliği arz edebilecek plaka numaraları ile birlikte aracın rengi, markası ve modeli, müşterinin ödemesi gereken prim, toplam prim gibi ayrıntılara da yer verildiği,*
- ✓ *Veri sorumlusu tarafından ilgili paylaşımların şahsi Facebook hesabından ve ".....sigorta" adıyla açtığı ve poliçe paylaşımlarıyla birlikte çeşitli özel gün kutlamaları ve şahsi fotoğraflarını da paylaştığı, hesabın açıklama kısmında kendi adına da yer verdiği Instagram hesabından yapıldığı,*

tespit edilmiş ve müşterilerine ait kişisel verileri herkese açık sosyal medya platformlarında müşterilerinden habersiz olarak ve reklam amacıyla paylaşan sigorta acentesine **22.500 TL idari para cezası** verilmiştir.[41]

5.2. GDPR Uygulamaları

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.

Active Assurances

Fransız KVK otoritesi (CNIL) 18.Temmuz.2019 tarihinde web sitesi kullanıcılarının kişisel verileri saçılması sebebiyle araba sigortası şirketi Active Assurances'a **180.000 €** tutarında **idari para cezası** kesmiştir.[42]

Bu ihlalde sürücü belgelerinin kopyaları, araç belgeleri ve banka kimlik bilgileri de dâhil birçok kişisel veri saçılmıştır. Bu olayda, web sitesi kullanıcılarının kişisel verilerinin güvenliğini koruma yükümlülüğüne uyulmaması ve GDPR'ın 32. maddesinin ihlal edildiği gerekçesiyle idari para cezası vermiştir.

[41] https://www.kvkk.gov.tr/Icerik/6716/2020-58
[42] https://www.jdsupra.com/legalnews/gdpr-new-cnil-fine-of-180-000-euros-for-21215/

Hollanda Kamu Sigorta Şirketi UWV

İşverenlerin hastalık, gebelik veya ebeveyn izni nedeniyle çalışanların devamsızlıklarını işledikleri Hollanda kamu sigorta şirketi UWV'nin portalında yeterli güvenlik tedbirleri alınmadığı için yüksek miktarda sağlık verileri de dâhil kişisel veri sızıntısı yaşanmıştır. Hollanda Veri Koruma Kurumu (AP), UWV'nin çevrimiçi işveren portalına erişimde çok faktörlü kimlik doğrulaması uygulamadığı için söz konusu portalın güvenliğinin yetersiz olduğuna karar verdi. Gerekli tedbirlerin alınması için UWV'ye Ekim.2019'a kadar, bir yıl süre verilmiştir. Bu tarihten sonra sözkonusu tedbirlerin alınmasında her gecikilen ay için de **150.000 €** olmak üzere, en fazla **900.000 €**'ya **idari kadar para cezası** verileceği bildirilmiştir.[43]

Kasım 2019 Güncellemesi

UWV AP'den talep edilen yükün yararlanıcı süresini askıya almasını istedi. Belirli koşullar altında AP, UWV'ye 1.Mart.2020 tarihine kadar bir kez ertelenmiştir. UWV'nin talep edilen tedbirleri sırayla karşılamaması durumunda bir ceza ödemesi gerekir.[44]

G.Kıbrıs Sosyal Güvenlik Hizmetleri

G. Kıbrıs Yönetimi Çalışma Bakanlığı bünyesindeki Sosyal Sigorta Hizmetlerine (YKA) kişisel verilerin sisteminden sızmasına izin verdiği için **9.000 € idari para cezası** verdi.[45]

Slovakya Sosyal Güvenlik Kurumu

Binlerce Slovak, Avusturya, Almanya ve İngiltere gibi Avrupa ülkelerinde hasta veya yaşlılara bakarak para kazanıp Slovakya'da sosyal sigorta primi ödemektedir. Koşulları, yaşı veya hizmet yıllarını sağladıktan sonra, emeklilik maaşı gibi sosyal yardımlar almaya hak kazanmaktadırlar. Slovak vatandaşlarının bu yardımlar için başvuruları Sosyal Sigortalar Kurumu tarafından işlenmekte ve doğrulamaları sırasında yabancı yetkililerle iletişim kurmaktadır. Bu tür bilgi talebinde, bir başvuru sahibinin maluliyet aylığı için kişisel bilgilerini içeren bir mektup kaybedildi. İlgili kişi Slovak Cumhuriyeti Kişisel Verileri Koruma Ofisine başvurdu.

Sosyal Sigortalar Kurumu, kişisel veri koruma kurallarını ihlal ettiği için **50.000 € idari para cezası**na çarptırıldı.[46]

Leave.EU ve Eldon Sigorta Şirketi Veri İhlali

2018 yılında İngiliz KVK Otoritesi (ICO) tarafından, Brexit kampanya grubu Leave.EU ve Arron Bankalarının sahibi olduğu Eldon Insurance'e toplam **135.000 £ idari para cezası** uygulanmıştır. Eldon Insurance'a uygulanan **15.000 £** ara cezasının, 300.000 adet politik pazarlama mesajının gönderilmesi için müşterilerine ait bilgileri hukuka aykırı şekilde kullanması olduğu belirtilirken, yine Eldon Insurance'a uygulanan **45.000 £** tutarındaki idari para cezasının ise Eldon pazarlama kampanyasına ilişkin e-postaları açık rızaları olmadan Leave.EU üyelerine göndermesinden dolayı kesildiği belirtilmiştir. Aynı şekilde, benzer para cezası ise Leave.Eu'ya kesilmiştir.[47]

[43] https://kyc-chain.com/the-5-biggest-gdpr-fines-to-date/
[44] https://autoriteitpersoonsgegevens.nl/nl/nieuws/ap-dwingt-uwv-met-sanctie-gegevens-beter-te-beveiligen
[45] https://cyprus-mail.com/2020/01/13/commissioner-slaps-record-fines-for-data-violations/
[46] https://www.trend.sk/spravy/socialna-poistovna-porusila-gdpr-rekordnu-pokutu-nechce-zaplatit
[47] https://www.theguardian.com/uk-news/2019/feb/01/leave-eu-arron-banks-insurance-company-fined-data-breaches-information-commissioner-audit

Bupa Sigorta Hizmetleri Veri İhlali

Bupa adlı sigorta şirketine, müşterilerinin kişisel verilerini korumak için etkili önlemler almadığı gerekçesiyle İngiliz otoritesi ICO tarafından **175.000 £ idari para cezası** kesilmiştir. [48]

6.Ocak-11.Mart.2017 tarihleri arasında, bir Bupa çalışanı, 547.000 Bupa Global müşterisinin verilerini internette satışa çıkartmıştır. Söz konusu çalışan verilere Bupa'nın müşteri ilişkileri yönetim sisteminden ulaşarak, bilgileri kendi e-postasına aktarmıştır. ICO, Bupa'nın gerekli teknik ve idari tedbirleri almaması nedeniyle söz konusu durumun 1,5 milyon kaydı uzun süre risk altında bıraktığı kanaatine varmıştır.

Royal&Sun Alliance Sigorta Şirketi Veri İhlali

İngiliz otoritesi ICO, 59.592 müşterisinin isim, adres ve banka hesabı bilgilerini içeren belleğin kaybolmasının ardından Royal & Sun Alliance Insurance PLC firmasına (RSA) **150.000 £ idari para cezası** vermiştir.[49]

İlgili ICO soruşturması, 59.592 müşterinin adlarını, adreslerini ve hesap numaraları ve sıralama kodlarını içeren banka hesabı ayrıntılarını içeren bir sabit sürücü cihazının çalındığını tespit etti. Cihazda ayrıca CVC numaraları ve son kullanma tarihlerinden etkilenmese de 20.000 müşterinin sınırlı kredi kartı bilgileri de bulunuyordu. ICO, RSA'nın Batı Sussex'teki ofislerinde hırsızlığın olmasını engelleyerek finansal bilgilerini korumak için uygun önlemlere sahip olmadığını belirledi. Cihaz, şirket personeli veya yüklenici tarafından çalındı, üzerindeki bilgilerin şifrelenmediği tespit edilen cihaz bulunamadı.

[48] https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2018/09/bupa-fined-175-000-for-systemic-data-protection-failures/

[49] https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2017/01/150-000-fine-for-insurance-company-that-failed-to-keep-customers-information-safe/

5.3. A.B.D. Uygulamaları

A.B.D. kişisel verileri koruma uygulamaları kapsamında, kişisel verilerin korunmasına ilişkin sigortacılık sektörü tarafından gerçekleştirilmiş ihlaller ve ihlal bildirimlerine ilişkin çeşitli örnekler bulunmaktadır.

Anthem

ABD Sağlık Sigortası Şirketi Anthem 2015 yılında 79 milyon insanı etkileyen bir ihlal yaşadı. İhlal, isimleri, doğum tarihlerini, sosyal güvenlik numaralarını ve tıbbi kimlikleri içeriyordu. Şirket ABD Sağlık Sigortası Taşınabilirlik ve Hesap Verilebilirlik Yasası (HIPAA) ihlalleri için Sağlık ve İnsan Hizmetleri Bakanlığı tarafından **16 Milyon $ idari para cezasına** çarptırıldı.

Bu para cezasına ek olarak, şirket 2017 yılında ihlale ilişkin bir toplu dava için ayrıca **115 milyon $ tazminat** ödemek zorunda kalmıştır.[50]

Triple-S (1)

20.Eylül.2013 tarihinde Porto Riko Sigorta şirketi Triple S, yaklaşık 70.000 Medicare Advantage müşterisine ait Medicare Sağlık Sigortası Talep Numarasını ("HICN") yayınladığı bir broşürde paylaştığı için, **6,8 Milyon $** tutarında **idari para cezasına** çarptırılmıştır.[51]

Triple-S (2)

Triple-S firması 2015 yılında ikinci bir veri ihlali için de **3,5 Milyon $ idari para cezasına** çarptırılmıştır.[52] Triple-S ayrıca, sahip olduğu verileri korumak için HIPAA uyum programındaki eksiklikleri gidermeye yönelik düzeltici bir eylem planı belirleyerek uygulamayı kabul etmiştir.

Bir Sağlık Sigortası Şirketi

Maryland'deki bir sağlık sigortası şirketi tıbbi kayıt kurallarını ihlal ettiği için **4,3 milyon $** tutarında **idari para cezasına** çarptırılmıştır.[53]

Eylül.2008 ile Ekim.2009 tarihleri arasında 41 hastanın tıbbi kayıtlarına erişimini reddettiği için **1,3 milyon $** idari para cezasına, ayrıca OCR soruşturmasında yeterli işbirliği yapmadığından dolayı da **3 milyon $** ek idari para cezasına çarptırılmıştır.

Mapfre Sigorta Veri İhlali

29.Eylül.2011 tarihinde, 2.209 kişinin isim, doğum tarihi ve sosyal güvenlik numaralarını içeren USB belleğin, şirketin bilgi işlem biriminden çalınması ile gündeme gelen veri ihlali sonucunda Mapfre Sigorta, ABD Sağlık Hizmetleri Bölümü ile bir anlaşma yapmış ve anlaşmaya göre, güvenlik ve gizlilik kurallarına uymaması nedeniyle Mapfre Sigorta **2,2 milyon $** tutarında **idari para cezası** ödemeyi ve bu durumu düzeltecek bir aksiyon planı uygulamayı kabul etmiştir. [54]

EmblemHealth Veri İhlali

New York merkezli sağlık sigortası şirketi EmblemHealth, New Jersey'de bulunan 6.000'in üzerinde müşterisinin kişisel bilgilerini sızdırması nedeniyle New Jersey Eyaleti tarafından **100.000 $ idari para cezasına** çarptırılmıştır. Ayrıca eyalet yetkilileri ve sigorta şirketi arasında yapılan anlaşma sonucunda, sigorta şirketinin kişisel bilgileri korumaya yönelik olarak bir dizi yeni önlem alması da kararlaştırılmıştır.[55]

[50] https://www.csoonline.com/article/3316569/biggest-data-breach-penalties-for-2018.html#slide4
[51] https://www.hldataprotection.com/2014/02/articles/health-privacy-hipaa/puerto-rico-hits-insurer-with-record-6-8-million-fine-for-hipaa-breach/
[52] https://www.databreachtoday.com/puerto-rico-insurer-fined-35-million-in-hipaa-settlement-a-8715
[53] https://thehill.com/policy/healthcare/145533-health-insurer-fined-43m-for-hipaa-violation
[54] https://www.databreaches.net/ocr-settles-charges-against-mapfre-life-insurance-for-2-2-million/
[55] https://www.databreaches.net/nj-fines-health-insurance-provider-100k-for-personal-information-breach/

Hampton-Haddon Pazarlama Şirketi Veri İhlali

Hampton-Haddon adlı bir hediye dağıtım şirketi, Willis of Tennessee Inc. ve Willis Towers Watson PLC adlı global sigorta şirketine, siber risklere karşı uyarmadığı ve bunlara ilişkin bir sigorta imkanı bulunduğunu belirtmediği için dava açmıştır. [56]

RxAmerica ve Accendo Sigorta Veri İhlali

RxAmerica ve Accendo adlı şirketler, yaklaşık 175,000 adet müşterisinin isim, üyelik numarası, ilaç adı ve doğum tarihi bilgilerinin kişilere gönderilen mektuplarda, mektup zarfından görülebilir olması nedeniyle veri ihlalinde bulunduğunu kamuoyuna açıklamıştır. [57]

Hartwig Moss Sigorta Şirketi Veri İhlali

Hartwig Moss adlı sigorta şirketi, yaklaşık 1,100 müşterisinin kişisel verilerinin ihlale konu olabileceğini açıklamıştır. Ancak söz konusu verilerin büyük çoğunluğunun basit nitelikli olduğu, yalnızca küçük bir kısım müşterinin sağlık verilerine erişilmiş olabileceği belirtilmiştir. [58]

[56] https://www.databreaches.net/you-should-have-told-us-company-says-email-was-hacked-sues-its-insurance-broker-for-not-advising-it-to-get-computer-fraud-insurance/

[57] https://www.databreaches.net/rxamerica-and-accendo-insurance-notify-175000-medicare-beneficiaries-that-mailing-error-exposed-their-medication-name-date-of-birth-and-member-id/

[58] https://www.databreaches.net/hartwig-moss-insurance-agency-discloses-data-breach-affecting-1100-customers/

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 verilerin 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 kuruluşlardan 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-978-605-06236-2-8

ACCERT