KVKK VE GDPR IŞIĞINDA VERİ İHLALİ VE SONUÇLARI

AYŞENUR YILDIZ

MEF ÜNİVERSİTESİ

HAZİRAN 2024

MEF ÜNİVERSİTESİ
SOSYAL BİLİMLER ENSTİTÜSÜ
ÖZEL HUKUK ANABİLİM DALI
ÖZEL HUKUK TEZLİ YÜKSEK LİSANS PROGRAMI

YÜKSEK LİSANS TEZİ

KVKK VE GDPR IŞIĞINDA VERİ İHLALİ VE SONUÇLARI

Ayşenur YILDIZ

ORCID NO: 0009-0004-9021-4922

Tez Danışmanı: Prof. Dr. Kadir Berk KAPANCI

HAZİRAN 2024

AKADEMİK DÜRÜSTLÜK BEYANI

Bu çalışmada yer alan tüm bilgilerin akademik kurallara ve etik ilkelere uygun olarak toplanıp sunulduğunu, çalışmada söz konusu kurallar ve ilkelerin zorunlu kıldığı çerçevede, özgün olmayan tüm bilgi ve belgelere, alıntılama standartlarına uygun olarak referans verilmiş olduğunu beyan ederim.

İsim ve Soy isim: Ayşenur YILDIZ

İmza:

ÖZET

KVKK VE GDPR IŞIĞINDA VERİ İHLALİ VE SONUÇLARI

Ayşenur YILDIZ

Özel Hukuk Tezli Yüksek Lisans Programı

Tez Danışmanı: Prof. Dr. Kadir Berk KAPANCI

Haziran 2024, 100 Sayfa

Kişisel verilerin korunması hukuku, günümüzde teknolojinin kullanımı günlük hayatın ayrılamaz bir parçası haline geldiğinden sürekli gündeme gelen, önemli bir konudur. Bu durum işlenecek kişisel mahiyetteki verilere ilişkin düzenlemelerin getirilmesini zorunlu kılmıştır. Bu ihtiyaç doğrultusunda 24.03.2016 tarihinde 6698 sayılı Kişisel Verilerin Korunması Kanunu yürürlüğe girmiştir. 25.05.2018 tarihinde ise, yine aynı ihtiyaç doğrultusunda Avrupa Birliği sınırları içerisinde uygulanmak üzere General Data Protection Regulation (Genel Veri Koruma Tüzüğü) yürürlüğe girmiştir.

Bu çalışmada, Kişisel Verilerin Korunması Kanunu ve Genel Veri Koruma Tüzüğü uyarınca veri sorumlusunun yükümlülüklerinden biri olan veri güvenliğini sağlama yükümlülüğü incelenecek; veri güvenliği ihlali durumunda ilgili Veri Koruma Kuruluna ve ilgili kişilere bildirim yapma yükümlülüğü üzerinde durulacaktır.

Çalışma üç bölümden oluşmaktadır. İlk bölümde, kişisel verilerin korunması hukukunun temel kavramları tez çalışmasının konusuyla ilgisi bakımından sınırlı olarak incelenmiştir. İkinci bölümde, veri güvenliği kavramı ve veri sorumlusunun veri güvenliğini sağlama yükümlülüğü KVKK, GDPR ve ilgili sair mevzuat ışığında incelenmiştir. Üçüncü bölümde ise veri güvenliği ihlali kavramı incelenmiş, veri güvenliği sonucu olan bildirim yükümlülüğünün üzerinde durulmuş ve karşılaştırmalı bir değerlendirme yapılmıştır.

Anahtar Kelimeler: Kişisel Verilerin Korunması Kanunu, General Data Protection Regulation (Genel Veri Koruma Tüzüğü), veri güvenliği, veri güvenliği ihlali, veri güvenliği ihlalinde Kişisel Verileri Koruma Kuruluna yapılacak bildirim, ilgili kişilere yapılacak bildirim.

Bilim Dalı Sayısal Kodu: 54001

ABSTRACT

DATA BREACH AND ITS CONSEQUENCES IN ASPECT OF KVKK AND GDPR

Ayşenur YILDIZ

LL.M. in Private Law

Thesis Advisor: Prof. Dr. Kadir Berk KAPANCI

June 2024, 100 Pages

Personal data protection law is an important topic that is constantly on the agenda as the use of technology has become an inseparable part of daily life. This has led to the introduction of regulations regarding the personal data to be processed: The Personal Data Protection Law No. 6698 entered into force on 24.03.2016. On 25.05.2018, the General Data Protection Regulation entered into force to be implemented within the borders of the European Union.

In this study, the obligation to ensure data security, which is one of the main obligations of the data controller pursuant to the Personal Data Protection Regulation and the General Data Protection Regulation, will be examined and the obligation to notify the relevant Data Protection Board and the relevant persons in case of data security breach will be emphasized.

The study consists of three parts. In the first part, the basic concepts of personal data protection law are examined in a limited manner in terms of their relevance to the subject of the thesis. In the second part, the concept of data security and the obligation of the data controller to ensure data security are examined in the light of the Personal Data Protection Law, all other relevant legislation and GDPR. In the third part, the concept of data security breach is examined, the obligation of notification as a result of data security is emphasized and a comparative evaluation is made.

Keywords: Personal Data Protection Law, General Data Protection Regulation (GDPR), data security, data security breach, notification to the Personal Data Protection Board in case of data security breach, notification to data subjects.

Numeric Code of the Field: 54001

TEŞEKKÜR

Yol göstericiliği için kıymetli tez danışmanım Prof. Dr. Kadir Berk KAPANCI'ya, her daim olduğu gibi eğitim hayatımda da desteklerini esirgemedikleri için sevgili annem Meral YILDIZ, babam Mustafa YILDIZ, kardeşlerim Ahsen ve Deniz YILDIZ'a ve sevgili eşim Mehmet Erdi KOCA'ya teşekkürlerimi sunarım.

İÇİNDEKİLER

ÖZET ..... **İ**
ABSTRACT ..... **İİİ**
TEŞEKKÜR ..... **V**
İÇİNDEKİLER ..... **Vİ**
KISALTMALAR ..... **İX**
GİRİŞ **1**
A. Konunun Takdimi 1
B. Konunun Sınırlandırılması 4
1. KVKK VE GDPR KARŞILAŞTIRMASIYLA KİŞİSEL VERİLERİN KORUNMASI HUKUKUNUN TEMEL ÖGELERİ **5**
1.1. Kişisel Verilerin Korunması Hukukuna İlişkin Temel Kavramlar 5
1.1.1 Kişisel Veri Kavramı 5
1.1.2. Özel Nitelikli Kişisel Veriler 12
1.1.3. Genel Nitelikli Kişisel Veriler 15
1.1.4. Kişisel Verilerin İşlenmesi 15
1.1.4.1. Hukuka ve Dürüstlük Kuralına Uygun Olmak 18
1.1.4.2. Doğru ve Gerektiğinde Güncel Olmak 19
1.1.4.3. Belirli, Açık ve Meşru Amaçlar İçin İşlenmek 20
1.1.4.4. İşlendikleri Amaçla Bağlantılı, Ölçülü ve Sınırlı Olmak 21
1.1.4.5. İlgili Mevzuatta Öngörülen veya İşlendikleri Amaç İçin Gerekli Süre Kadar Saklanmak 22
1.1.4.6. GDPR Uyarınca Hesap Verilebilirlik İlkesi 23
1.1.5. Veri Sorumlusu ve Veri İşleyen 23
1.1.5.1. Veri Sorumlusu 23
1.1.5.2. Veri İşleyen 26
1.2 Veri Sorumlusunun Yükümlülükleri 28
2. KVKK VE GDPR KARŞILAŞTIRMASIYLA VERİ SORUMLUSUNUN VERİ GÜVENLİĞİNE İLİŞKİN YÜKÜMLÜLÜKLERİ **29**
2.1. Genel Olarak 29
2.1.1. Veri Güvenliği 31
2.1.2. Bilgi Güvenliği 32
2.2. Veri Sorumlusunun Veri Güvenliğine İlişkin Sorumluluğunun Hukuki Kaynakları 33

2.3. Veri Sorumlusunun Veri Güvenliğine İlişkin Yükümlülükleri 36
2.3.1. Hukuka Aykırı İşlemenin Önlenmesi 38
2.3.2. Kişisel Verilere Hukuka Aykırı Olarak Erişilmesinin Önlenmesi 42
2.3.3. Kişisel Verilerin Muhafazasını Sağlamak 44
2.3.4. Teknik ve İdari Tedbir Alma Yükümlülüğü 45
2.3.4.1. Kişisel Veri Güveliğine İlişkin İdari Tedbirler 47
2.3.4.1.1. Mevcut Risk ve Tehditlerin Belirlenmesi 49
2.3.4.1.2. Çalışanların Eğitilmesi ve Farkındalık Çalışmaları 49
2.3.4.1.3. Kişisel Veri Güvenliği Politikalarının Oluşturulması 51
2.3.4.1.4. Kişisel Verilerin Mümkün Olduğunca Azaltılması 51
2.3.4.1.5. Veri İşleyenler ve Müşterek Veri Sorumluları ile İlişkilerin Yönetimi 52
2.3.4.2. Kişisel Veri Güveliğine İlişkin Teknik Tedbirler 54
2.3.4.2.1. Siber Güvenliğin Sağlanması 55
2.3.4.2.2. Kişisel Veri Güvenliğinin Takibi 57
2.3.4.2.3. Kişisel Verilerin Bulunduğu Ortamların Güvenliğinin Sağlanması 57
2.3.4.2.4. Kişisel Verilerin Yedeklenmesi 58
2.3.4.3. Veri Sorumlusunun Denetim Yükümlülüğü 58
2.3.4.4.Kanuna Aykırı Başkasına Açıklama ve İşleme Amacı Dışında Kullanım Yasağı 59
3. VERİ GÜVENLİĞİ İHLALİNİN TESPİTİ VE VERİ SORUMLUSUNUN BİLDİRİM YÜKÜMLÜLÜĞÜ 61
3.1. Veri Güvenliği İhlali 61
3.1.1. Veri İhlali Kavramı 61
3.1.2. Veri İhlalinin Tespiti 64
3.2. Veri Sorumlusunun Bildirim Yükümlülüğü 66
3.2.1. Veri Koruma Otoritesine Yapılacak Bildirim 68
3.2.2. İlgili Kişiye Yapılacak Bildirim 71
3.2.3. GDPR Bakımından Risk Değerlendirilmesi 73
3.3. Veri Güvenliğine İlişkin Yükümlülüğün Yerine Getirilmemesinde Sorumluluk 75
3.3.1. Sözleşme Sorumluluğu 76

3.3.2. Haksız Fiil Sorumluluğu 77
3.3.3. Kişisel Verilerin Korunması Mevzuatlarına Dayalı Sorumluluk 80
3.4. Veri Güvenliğine İlişkin Yükümlülüğün Yerine Getirilmemesi Kabahati 83
SONUÇ 87
KAYNAKÇA 91
KARARLAR 96

KISALTMALAR

95/46/ECU Sayılı Direktif	**:** Kişisel Verilerin İşlenmesi ve Bu Tür Verilerin Serbest Dolaşımına Dair Bireylerin Korunması Hakkındaki Avrupa Birliği Konseyi ve Avrupa Parlamentosu Direktifi
AB	**:** Avrupa Birliği
agm.ne.	**:** Adı Geçen Eser
a.g.m.	**:** Adı Geçen Makale
AİHM	**:** Avrupa İnsan Hakları Mahkemesi
AİHS	**:** Avrupa İnsan Hakları Sözleşmesi
AY	**:** Anayasa
Bkz.	**:** Bakınız
dn.	**:** dipnot
EC	**:** European Commission (Avrupa Komisyonu)
EDPB	**:** European Data Protection Board (Avrupa Veri Koruma Kurulu)
EU	**:** European Union (Avrupa Birliği)
e.t.	**:** Erişim Tarihi
GDPR	**:** General Data Protection Regulation (Genel Veri Koruma Tüzüğü)
İÜHFM	**:** İstanbul Üniversitesi Hukuk Fakültesi Mecmuası
Kurul	**:** Kişisel Verileri Koruma Kurulu
Kurum	**:** Kişisel Verileri Koruma Kurumu
KVKK	**:** Kişisel Verilerin Korunması Kanunu
m.	**:** Madde
RG	**:** Resmi Gazete
Rehber	**:** Kişisel Veri Güvenliği Rehberi
s.	**:** Sayfa
ss.	**:** Sayfa Sayısı
S.	**:** Sayı
Tüzük	**:** Genel Veri Koruma Tüzüğü
vd.	**:** ve devamı

GİRİŞ

A. Konunun Takdimi

Bu tez çalışmasının konusunu 6698 sayılı Kişisel Verilerin Korunması Kanunu ("KVKK" ya da "Kanun")[1] ve 2016/679 sayılı Genel Veri Koruma Tüzüğü ("GDPR" ya da "Tüzük")[2] ışığında veri ihlali ve sonuçları oluşturmaktadır.

Kişisel verilerin korunması, Türk hukukunda 2010 yılında Anayasa'nın[3] "Özel hayatın gizliliği" başlıklı 20. maddesinin 3. fıkrası ile gittikçe önem kazanmıştır. Türkiye Cumhuriyeti, Avrupa Konseyi tarafından 28.01.1981 tarihinde imzaya açılmış olan "Kişisel Verilerin Otomatik İşleme Tabi Tutulması Karşısında Bireylerin Korunması Sözleşmesi"ni (108 no'lu Sözleşme) imzalayan ülkelerdendir; ancak 108 Nolu Sözleşme'nin iç hukuka dâhil edilmesi 17.03.2016 tarih ve 29656 sayılı Resmi Gazete'de yayımlanması ile gerçekleşmiştir.

2016 yılında Türkiye'de yürürlüğe giren KVKK, günümüzde kişisel verilerin korunması hukukundaki birçok yasal düzenlemelerin temelini oluşturan 95/46/EC sayılı ve 1995 tarihli Kişisel Verilerin İşlenmesi ve Bu Tür Verilerin Serbest Dolaşımına Dair Bireylerin Korunması Hakkındaki Avrupa Birliği Konseyi ve Avrupa Parlamentosu Direktifi ("95/46/EC Sayılı Direktif" veya "Direktif")[4] temel alınarak düzenlenmiştir.[5] 95/46/EC sayılı Direktif, üye AB devletleri için bir tüzük gibi bağlayıcı olmayıp, üye devletlerin Direktif'e uyarak iç hukuklarında düzenlemeler yapmaları beklenmekteydi.[6] Başka bir deyişle Direktif, ulaşılmak istenen temel bir hedefi ifade etmiş ve nasıl ulaşılacağını üye devletlerin kendi iç yapısına bırakmıştı.[7]

---

[1]Yayımlanma Tarihi: RG 07.04.2016, S. 29677.
[2]Kişisel verilerin işlenmesine ilişkin olarak gerçek kişilerin korunması ve bu tür verilerin serbest dolaşımına ilişkin ve 95/46/EC sayılı Direktifi yürürlükten kaldıran 27 Nisan 2016 tarihli ve 2016/679 (AB) sayılı Avrupa Parlamentosu ve Konsey Tüzüğü, OJ 2016 L 119/1.
[3]2709 Sayılı Türkiye Cumhuriyeti Anayasası, Yayımlanma Tarihi: RG 18.10.1982, S. 17863.
[4]Directive 95/46/EC of the European Parliament and of the Council. Avrupa Birliği Resmi Gazetesi: L281, T. 23.11.1995.
[5]Murat Volkan Dülger, **Kişisel Verilerin Korunması Hukuku**, Hukuk Akademisi Eğitim ve Yayıncılık Ltd. Şti, 1. Baskı, İstanbul, Ocak 2019, s. 2.
[6]Ufuk Dal, **Avrupa Birliği Genel Veri Koruma Tüzüğü'nün Ülke Dışı Uygulama Yetkisi ve Bu Yetkinin Uluslararası Hukukta Meşruiyeti**, Kişisel Verileri Koruma Dergisi, Cilt 1, Sayı 1, 2019, s. 23.
[7]Dülger, s. 66.

Gelişen teknoloji ile kişisel verilerin korunması alanında yetersiz kalması üzerine 95/46/EC sayılı Direktif yerini 25.05.2018 tarihinde yürürlüğe giren GDPR'a bırakmıştır. GDPR iki bileşenden oluşur; bunlar, yasal gereklilikleri oluşturan maddeler ve maddeleri tamamlayan, ek bilgi ve destekleyici açıklamalar sağlayan resitallerdir. Resitaller GDPR'a ne zaman ve nasıl uyulacağını açıklar. GDPR'ın 173 paragraflık resital bölümü ve 99 maddeden oluşan temel tüzük metni bulunur ve oldukça kapsamlı bir veri koruma çerçevesi sunar.[8] GDPR, Direktif'in aksine yol gösterici bir nitelikte ortaya çıkmamıştır ve bağlayıcıdır. [9]

GDPR'ın AB tarafından düzenlenmiş olması, ilgili hükümlerin sadece AB içerisinde yerleşik faaliyet gösteren veri işleyicileri ve veri sorumluları açısından bağlayıcı olduğu anlamına gelmez. Nerede yerleşik faaliyet gösterdiği ayırt edilmeksizin AB vatandaşları ve GDPR'ın uygulama alanına dâhil herkese yönelik bir kişisel verilerin korunması güvencesi sağlamaktadır.[10]

Türkiye'de KVKK'nın uygulanmasını sağlamak ve kişisel verilerin korunmasını gözetmek amacıyla gerekli düzenleyici ve denetleyici işlemlerde bulunan kurum Kişisel Verileri Koruma Kurumu'dur ("Kurum"). Avrupa Veri Koruma Kurulu ("EDPB") ise GDPR'ın uygulanmasını sağlamak ve AB'nin veri koruma makamları arasında işbirliğini teşvik etmek için görevli olan, tüzel kişiliğe sahip bağımsız AB organıdır. EDPB, 25 Mayıs 2018 tarihinde veri koruma ve gizlilik konusunda bağımsız bir Avrupa Birliği danışma organı olan Madde 29 Çalışma Grubu'nun yerini almıştır.

Veri güvenliği kavramı, kişisel verilerin korunması hukukunun oldukça önemli bir parçasıdır ve veri sorumlusunun temel yükümlülüklerinden biri de veri güvenliğini sağlamaktır. Nitekim, 'Amaç' başlıklı KVKK m.1'in gerekçesinde de bu durum "Maddeyle, Kanunun amacı belirlenmektedir. Amaç, kişisel verilerin işlenmesinin disiplin altına alınması ve Anayasada öngörülen başta özel hayatın gizliliği olmak üzere temel hak ve özgürlüklerin korunmasıdır. Son yıllarda önem kazanan kişinin

[8]Ayşe Nur Akıncı, **Avrupa Birliği Genel Veri Koruma Tüzüğü'nün Getirdiği Yenilikler Ve Türk Hukuku Bakımından Değerlendirilmesi,** T.C. Kalkınma Bakanlığı İktisadi Sektörler ve Koordinasyon Genel Müdürlüğü Çalışma Raporu 6, Haziran 2017, s. 19.
[9]Dülger, s. 66.
[10]Akıncı**,** s. 15**;** Dülger, s. 66.

mahremiyet hakkı ile bilgi güvenliği hakkının korunması da bu kapsamda değerlendirilmektedir…"[11] şeklinde ifade edilmiştir. Yine benzer şekilde GDPR m. 5/1-f uyarınca 'verilerin uygun güvenliğinin sağlanarak işlenmesi gerektiği' ifade edilmiştir.

KVKK m. 12/1 uyarınca veri sorumlusunun "kişisel verilerin hukuka aykırı olarak işlenmesini ve kişisel verilere hukuka aykırı olarak erişilmesini önlemek ve kişisel verilerin muhafazasını sağlamak" amacıyla uygun asgari güvenliği sağlamak için her türlü teknik ve idari tedbirleri almak zorunda olduğu belirtilmiştir. İlgili maddenin 5. fıkrasında ise "işlenen kişisel verilerin kanuni olmayan yollarla başkalarınca elde edilmesi halinde veri sorumlusunun bu durumu en kısa sürede ilgilisine ve Kişisel Verileri Koruma Kuruluna bildireceği, Kurul'un gerekmesi halinde bu durumu kendi internet sitesinde ya da uygun göreceği başka bir yöntemle ilan edebileceği" düzenlenmiştir.

Veri güvenliğinin ihlal edildiği durumlarda ise hem KVKK hem de GDPR veri sorumlularına ilgili kurumlara ve ilgili kişilere bildirimde bulunmayı zorunlu kılmıştır. Veri güvenliği ihlali kavramı, GDPR hükümlerinde bildirim yükü KVKK'ya göre daha detaylı düzenlenmiştir. Ancak iki mevzuatta da birtakım usuller ve süreler ifade edilmemiş, örneğin ihlal türleri detaylandırılmamıştır.[12]

Veri sorumlusunun veri güvenliği ihlali durumundaki bildirim yükümlülüğünü yerine getirebilmesi için öncelikle kişisel veri denildiğinde ne anlaşılması gerektiği ve veri güvenliği kavramları açıklığa kavuşturulmalıdır. Bu nedenle, bu tez çalışmasında, öncelikle kişisel verilerin korunması hukukundaki temel kavramlar KVKK ve GDPR ışığında ele alınacaktır. İkinci bölümde veri güvenliği kavramı ve veri sorumlusunun veri güvenliğine ilişkin yükümlülükleri incelenecektir. Son bölümde ise veri güvenliği ihlali kavramı karşılaştırmalı mevzuat ve ilgili kararlar ışığında değerlendirilecek, veri sorumlusunun bildirim yükümlülüğü detaylıca incelenecektir.

[11]Kişisel Verilerin Korunması Kanunu Gerekçesi. *Bkz*. https://www.lexpera.com.tr/mevzuat/gerekceler/kisisel-verilerin-korunmasi-kanunu-madde-gerekceleri/1 (E.T. 02.01.2024).

[12]Nur Sena Sevindi, Muhammed Emin Ordu, **AB Ve Türk Hukukunda Veri İhlalinin Tespiti Ve Bildirim Süresinin Karşılaştırmalı Değerlendirmesi**, Kişisel Verileri Koruma Dergisi, Cilt 5, Sayı 1, 2023, s. 12.

B. Konunun Sınırlandırılması

Bu tez çalışması üç bölümden oluşmaktadır. Tez planı olarak öncelikle birinci bölümde kişisel verilerin korunması hukukundaki temel kavramlar incelenecektir. İkinci bölümde veri sorumlusunun veri güvenliğine ilişkin yükümlülüğü incelenecektir. Son bölümde ise veri ihlali durumunda veri sorumlusunun bildirim yükümlülüğü incelenecektir. Tüm değerlendirmeler asıl inceleme konusu ile bağlantılı olarak, amaç ile sınırlanarak incelenmiştir.

Bu nedenle ilk bölümde ele alınacak olan kişisel verilerin korunması hukukuna ilişkin ilgili mevzuatlara ilişkin açıklamalar ve temel kavramlar; amaç ile sınırlandırılarak değerlendirilmiştir. İkinci bölümde, veri güvenliği kavramından ve veri sorumlusunun veri güvenliğini sağlama yükümlülüğünden bahsedilmiştir. Son bölümde ise veri sorumlusunun veri güvenliği ihlali durumundaki bildirim yükümlülüğünden bahsedilmiştir ve kısaca sorumluluk halleri ile veri güvenliğini sağlamama kabahatine değinilmiştir.

1. KVKK VE GDPR KARŞILAŞTIRMASIYLA KİŞİSEL VERİLERİN KORUNMASI HUKUKUNUN TEMEL ÖGELERİ

1.1. Kişisel Verilerin Korunması Hukukuna İlişkin Temel Kavramlar

Veri güvenliği durumunda veri sorumlusunun bildirim sorumluluğunun anlaşılabilmesi için kişisel verilerin korunması hukukundaki temel kavramların içeriklerinin detaylıca açıklanması önemlidir. Bu kapsamda ilk bölümde KVKK ve GDPR uyarınca kişisel veri, kişisel verilerin işlenmesi, veri sorumlusu ve veri işleyen kavramları konuyla ilişkili olarak sınırlı biçimde incelenecektir.

1.1.1 Kişisel Veri Kavramı

Kişisel verilerin korunması hukukunu anlayabilmek için en önemli adım kişisel veri kavramının tanımını kavrayabilmektir. Kişisel veri bizi biz yapan veriler bütünüdür. Diğer bir ifadeyle kişisel veri, bir kişinin ayırt edilmesini sağlayan her türlü bilgidir.[13] Kişisel veri dendiğinde akla ne gelmesi gerektiği keskin sınırlarla belirli değildir.[14] Yine de, ulusal ve uluslararası birçok metinde kişisel veri benzer şekillerde tanımlanmaktadır.[15]

95/46/EC Sayılı Direktif uyarınca kişisel veri, "fiziksel, fizyolojik, zihinsel, ekonomik, kültürel veya sosyal kimliğine özel bir veya daha fazla faktöre veya bir kimlik numarasına atıf başta olmak üzere doğrudan veya dolaylı olarak tespit edilebilen bir tespit edilebilir kişi; tespit edilmiş veya tespit edilebilir gerçek kişiye ("veri öznesi) ilişkin herhangi bir bilgi" olarak tanımlanmıştır ve bu şekilde birçok metne uyarlanmıştır.[16] Direktif aslında sadece gerçek kişiye yönelik bir tanımlamada

[13]Murat Uçak, **Civil Liability Of Data Controller For Unlawful Processıng Of Personal Data,** Yüksek Lisans Tezi, İstanbul Medeniyet Üniversitesi, 2019, s. 2; Çiğdem Ayözger Öngün**, Kişisel Verilerin Korunması Hukuku Elektronik Haberleşme Sektörüne İlişkin Özel Düzenlemeler Dahil**, Ertem Basım Yayın Dağıtım San. Tic. Ltd. Şti, 2. Baskı, Ankara, 2019, s. 5; Ersan Şen, **Kişisel Verilerin Korunması Kanunu Tasarısı'nın Anayasa ve Türk Ceza Kanunu Hükümleri Çerçevesinde Değerlendirilmesi**, İstanbul Barosu Dergisi, Cilt 83, Sayı 3, 2009, s. 1197.
[14]Dülger, s. 1.
[15]Ayözger Öngün**,** s. 5.
[16]Aygözer Öngün, s. 5.

bulunmuş olsa da, bazı iç hukuklara uyarlanırken tüzel kişilere yönelik tanımlar da eklenmiştir[17] ve geniş tanımlanmış olduğundan yorum farklılıklarına yol açmıştır.[18]

GDPR m. 4/1'de kişisel veri "kimliği tespit edilmiş ya da edilebilir bir gerçek kişiye ilişkin her türlü bilgi" olarak tanımlanmıştır. Aynı şekilde KVKK m.3/d'de da kişisel veri, "Kimliği belirli veya belirlenebilir gerçek kişiye ilişkin her türlü bilgi" olarak ifade edilmiştir. GDPR düzenlemesinde kişisel veri tanımında KVKK'dan esaslı bir farklılık ortaya koymamıştır. Ancak, söz konusu tanım detaylıca yazılmış ve somut örneklerle çeşitlendirilmiştir.[19]

4 Haziran 2021 tarihinde yürürlüğe giren Elektronik Haberleşme Sektöründe Kişisel Verilerin İşlenmesi ve Gizliliğin Korunmasına İlişkin Yönetmelik[20] m. 3/h'de ise "belirli veya kimliği belirlenebilir gerçek ve tüzel kişilere ilişkin bütün bilgileri" ifade etmiştir. KVKK'da yapılan tanımda ise tüzel kişiler tanımın dışında bırakılmıştır. Buradan da ülkemizdeki mevzuatlarda 95/46/EC Sayılı Direktif ile paralel bir tanımlama yapıldığı ve tüzel kişilere ilişkin tanımlamaya elektronik haberleşme sektörüne ilişkin mevzuatlarda yer verildiği görülür. [21]

Bütün bu tanımlar incelendiğinde kişisel veri kavramını oluşturan temellerin "veri", "kimliği belirli ya da belirlenebilir kişi" ve "verinin kişiye ait olması" olduğu anlaşılmaktadır.[22]

KVKK ve GDPR'ın kişisel veri tanımında yer alan "her türlü bilgi" ibaresinin anlaşılması için öncelikli olarak veri ile bilgi kavramlarının üzerinde durulmalıdır. Günlük yaşamda "bilgi" ve "veri" kelimeleri aynı anlama gelecek şekilde birbiri yerine

[17]Aygözer Öngün, s. 5.
[18]Ian J. Lloyd, **Information Texhnology Law,** Oxford University Press, 7. Bası, Oxford 2014, s. 42.
[19]Akıncı, s. 30.
[20]Yayımlanma Tarihi: RG 04.12.2020, S. 31324.
[21]Aygözer Öngün, s. 6.
[22]Dülger, s. 6-9; Mesut Halıcıoğlu**, Türk Hukukunda Veri Sorumlusu,** Yüksek Lisans Tezi, Hacettepe Üniversitesi, Ankara 2019, s. 6; Osman Şahin, **Elektronik Haberleşme Sektöründe Kişisel Verilerin İşlenmesi, Saklanması ve Gizliliğin Korunması**, Bilgi Teknolojileri ve İletişim Kurumu, Bilişim Uzmanlığı Tezi, Ankara, Haziran 2011, s. 5; Noor Talaat Azzat Sahar, **6698 Sayılı Kişisel Verilerin Korunması Kanununda Yer Alan Temel Kavramlar ile Terminoloji**, Selçuk Üniversitesi Adalet Meslek Yüksekokulu Dergisi, 2011, s. 36-38; Aygözer Öngün, s. 7 vd.

kullanılsa da, birbirlerini tam olarak karşılamamaktadır[23]. Bilgi, verinin anlamlandırılmış biçimidir. Bilgi, veriden daha geniş bir anlama sahiptir. İşlenen veri bilgidir.[24] Yine de, kelimelerin arasındaki fark teknik bir farklılığa dair olduğundan[25], bu tez çalışmasında her iki kelime de aynı anlama gelecek şekilde değerlendirilmiştir. Belirtilmelidir ki "Bilgi ve Veri Güvenliği" başlıklı kısımda bu iki kavramın üzerinde bir kez daha durulacak olup kavramlar farklı açılardan ele alınacaktır.

Kanunda hangi bilgilerin kişisel veri olduğu tek tek sınırlıca sayılmamıştır.[26] Bu nedenle de bu kapsamı geniş olarak ele almak gerekir. Nitekim tanımda "her türlü bilgi" ifadesinin kullanılması amacı da bu geniş tanımlamaya yer verebilmektir.[27] Kurul, yayınladığı Kişisel Verilerin Korunması Kanunu Hakkında Sıkça Sorulan Sorular belgesi ile bunu ifade etmiştir.[28] Sıkça Sorulan Sorular belgesinde de ifade edildiği gibi, her türlü bilgi denildiğinde kişinin kimliğini ifade eden ad, soyad, doğum tarihi vb. bilgiler anlaşılabileceği gibi; pasaport, özgeçmiş, fotoğraf, hobiler, aile bilgileri gibi kişiyi doğrudan ya da dolaylı yoldan bulunabilir kılan bütün veriler kişisel veri sayılır. Burada önemli olan şey verinin bir kişiyi işaret etme amacı taşıyıp taşımadığıdır.[29]

Burada üzerinde durulacak bir diğer nokta ise verilerin yalnızca elektronik veri olarak nitelemesinin yapılamayacağıdır. Benzer bir görüşe göre bu durum "Kavramın sadece bir kısmını oluşturduğu için dar bir anlama sahip olan bilgisayar verileri yerine 'elektronik olarak işlenmiş ve saklanmış veriler' terimi tercih edilmelidir" şeklinde ifade edilmiştir.[30] Yine, bir başka görüşe göre, dar bir tanımlama yapılması durumunda kişisel verilerin korunması hakkının koruma alanı da oldukça daralacaktır.[31]

---

[23]Oğulcan Özkan, **Kişisel Verilerin Korunması**, Yüksek Lisans Tezi, Ankara Üniversitesi, Ankara 2020, s. 5.
[24]Aygözer Öngün, s. 8.
[25]Elif Küzeci, **Kişisel Verilerin Korunması, Oniki Levha Yayınları**, 4. Baskı, İstanbul 2018.**,** s. 14; Dülger, s. 7 dn. 19.
[26]Özkan, s. 9.
[27]Mehmet Semih Öztekin, **Kişisel Veri Güvenliğine İlişkin Yükümlülüklerin Yerine Getirilmemesi Kabahati**, Yüksek Lisans Tezi, Galatasaray Üniversitesi, İstanbul, Haziran 2023, s. 6; Çiçek Ersoy Kekevi, **Genel Kavramlar, Kişisel verilerin Korunmasına Akademik Bakış KVKK Akademi Derleme Çalışması**, Kişisel Verilerin Koruma Kurumu, Yayın No: 42, Ankara 2023, s. 103
[28]Kişisel Verileri Koruma Kurumu, **Kişisel Verilerin Korunması Kanunu Hakkında Sıkça Sorulan Sorular**, KVKK Yayınları, Ankara, 2019, s. 21 **["KVKK, Sıkça Sorulan Sorular"].**
[29]Aygözer Öngün, s. 9.
[30]Veli Özer Özbek, **Elektronik Ortamda Saklı Bulunan Verilerin Ceza Muhakemesinde Delil Niteliği ve Değerlendirilmesi**, İÜHFM, Cilt 59, Sayı 1 -2, 2001, s. 197.
[31] Dülger**,** s. 7.

Kişisel veri açısından bilginin nesnel ya da öznel oluşu bir ayrım ifade etmemektedir. Bilginin doğruluğunun kanıtlanmış olması dahi bir ayrım oluşturmamaktadır.[32] Nitekim kişisel veri koruma kuralları zaten verinin yanlış olma ihtimalini öngörür ve ilgili kişiye veriye erişme ve uygun çözüm yöntemleriyle bu verinin yanlışlığına itiraz etme hakkı sağlar.[33]

KVKK'da sınırlı bir tanımlama yapılmadığından, her somut olayın özelliğine göre kişisel verinin kapsamının genişletilmesini de mümkün görmek yanlış olmayacaktır.

GDPR Resital 30 "kişisel veri sadece kişisel tercihler, yer veya eylemler değil, IP adresi, çerezler, belirteçler, sosyal bağlantılar, e-mail sağlayıcılar, arama motorları, tıklama dizileri, ad banner reklamları, javascript gibi unsurları da kapsayacaktır."[34] ifadesi ile kişisel verilerin kapsamını belirtmiştir.

Kişisel veri kavramını oluşturan bir diğer temel ise "kimliği belirli ya da belirlenebilir bir kişinin varlığı" dır. Kişinin kimliğinin belirli ya da belirlenebilir olması denildiğinde öncelikle kişi ibaresinden ne anlaşılması gerektiği değerlendirilmelidir. Tüzel kişilerin ulusal ve uluslararası kaynaklarda kabul görmüş tanımlar uyarınca kapsam dâhilinde olup olamayacağı hususu bu açıdan gündeme gelir.[35]

Tezcan, özel yaşamın korunması esasının gerçek kişiye ait bir kavram olduğunu, ancak tüzel kişiler için de ticari gizliliğin korunmasının söz konusu olabileceğini ifade etmiştir ve gerçek kişilerin özel yaşamının bilgisayar karşısında korunmasıyla yetinilmenin yerinde olduğu görüşünde bulunmuştur.[36] Dülger, kişisel

[32]Dülger, s. 8; Özlem Budak, **Kişisel Verilerin KVKK ve GDPR Kapsamında Yurt Dışına Aktarılması**, Yüksek Lisans Tezi, Marmara Üniversitesi, İstanbul, 2023, s. 11; Article 29 Data Protection Working Party Opinion 4/2007 on the Concept of Personal Data, Haziran 2007, 01248/07/EN, WP 136, s. 6; Ersoy Kekevi, s. 103; Kişisel Verileri Koruma Kurumu, **100 Soruda Kişisel Verilerin Korunması Kanunu**, KVKK Yayınları, Ankara, 2019, s. 18 **["KVKK, Soru Cevap"].**

[33]Article 29 Data Protection Working Party Opinion 4/2007 on the Concept of Personal Data, s. 6.

[34]Dal, s. 26.

[35]Budak, s. 13.

[36]Durmuş Tezcan, **Bilgisayar Karşısında Özel Hayatın Korunması**, Anayasa Yargısı, Ankara 1991, s. 389; Engin Dinç, **Kişisel Verilerin Korunmasında Uluslararası Düzenlemeler Ve Türkiye'nin Durumu**, Yüksek Lisans Tezi, Dicle Üniversitesi, Diyarbakır 2006, s. 16.

verilerin korunması hakkının insan hakkı olması ve amacın bireyin temel hak ve özgürlüklerinin sağlanmak olduğunu söyleyerek buradan anlaşılması gerekenin gerçek kişi olduğunu vurgulamıştır.[37]

KVKK m. 3'teki tanımlama da bu hususta açıktır, kanun lafzı uyarınca KVKK kapsamında yalnızca gerçek kişinin kişisel verileri korunmaktadır. Tüzel kişiye ait bir veri, gerçek kişiyi belirler ya da belirlenebilir kılarsa bu da Kanun kapsamında korunur. KVKK kapsamında tüzel kişilere ait verilerin korunması hiçbir şekilde düzenlenmemiştir. [38] Tüzel kişilere ait bilgiler kişisel veri kabul edilmemekte ve tüzel kişiler KVKK kapsamında hak öznesi olarak görülmemektedir.[39] Nitekim Kurul, 19.11.2018 tarihli ve 2018/131 sayılı kararında, tüzel kişiliğe ait elektronik ortamda yer alan verilerin başka bir tüzel kişilik tarafından talep edilmesi hakkındaki somut olayı incelemiş ve "Kurumumuza intikal eden söz konusu başvuruda yer alan, tüzel kişiliğe ait verilere erişilmesi yönündeki talebin Kanunun 2'nci maddesi gereğince Kanun kapsamında değerlendirilemeyeceğine," şeklinde hüküm kurarak tüzel kişilerin Kanun kapsamında korunmadığını vurgulamıştır.[40]

Tüzel kişilere ilişkin ise 2002/58/EC sayılı Elektronik Haberleşme Sektöründe Kişisel Verilerin İşlenmesi ve Özel Hayatın Gizliliğinin Korunmasına İlişkin Direktif[41] ile düzenlemeler yapılmıştır. Buna paralel olarak Elektronik Haberleşme Sektöründe Kişisel Verilerin İşlenmesi ve Gizliliğin Korunması Hakkında Yönetmelik[42] de tüzel kişilere ait kişisel verileri koruma altına almaktadır.[43]

Gerçek kişiye ilişkin kişisel veri kavramı incelendiğinde "kişi" kavramının da Kişiler Hukuku bakımından üzerinde durmak gerekir. Türk hukukunda Kişilik, tam ve sağ doğumla başlar ve ölümle sona erer; hak ehliyeti, sağ doğmak koşuluyla, ana rahmine düştüğü andan başlayarak elde edilir.[44] Kurul 18.09.2019 tarihli 2019/273

[37]Dülger, s. 9.
[38]Özkan, s. 14-15.
[39]Öztekin, s. 9-10; Onur Baskın, **Türk Hukuku Bakımından Kişilik Hakkı Kapsamında Kişisel Verilerin Korunması,** Seçkin Yayıncılık, Ankara 2021, s. 24.
[40]Kişisel Verileri Koruma Kurulu'nun 19.11.2018 tarihli ve 2018/131 sayılı kararı. (Bkz. https://www.kvkk.gov.tr/Icerik/5423/2018-131 E.T. 19.01.2024).
[41]Official Journal L 201 , 31/07/2002 P. 0037 – 0047.
[42]Yayımlanma Tarihi: RG 4.12.2020, S. 31324.
[43]Budak, s. 13.
[44]4721 sayılı Türk Medeni Kanunu (Yayımlanma Tarihi: RG 08.12.2001, S. 24607) m. 28'de "*Kişilik, çocuğun sağ olarak tamamıyla doğduğu anda başlar ve ölümle sona erer. Çocuk hak ehliyetini, sağ*

sayılı kararında vefat eden kişinin kişi sayılmayacağı, bu nedenle de KVKK kapsamında korunmayacağını ifade etmiştir.[45] Belirtmek gerekir ki cenine ait bilgiler, doğumuna dek annenin kişisel verisi olarak sayılacaktır ve annenin verisi olarak KVKK kapsamında kişisel veri olarak korunacaktır[46].

Belirli bir kişi denildiğinde akla diğer insanlardan ayırt edilebilir bir kişi gelir. Kimliği belirlenmemiş ancak makul bir çaba sonucunda belirlenebilir olan kişiler de aynı şekilde bu kapsamdadır.[47] Kişisel veri tanımında yer alan diğer şart ise kişinin kimliğinin belirli ya da belirlenebilir olmasıdır. Kurum yayınladığı 6698 Sayılı Kanun'da Yer Alan Temel Kavramlar[48] adlı belgesinde belirli ya da belirlenebilir olmayı tıpkı matufiyet şartında olduğu gibi "mevcut verilerin herhangi bir şekilde bir gerçek kişiyle ilişkilendirilmesi suretiyle, o kişinin tanımlanabilir hale getirilmesi" olarak tanımlamıştır. Matufiyet şartı da içtihatlarda adı, sanı, kimliği belli olmasa da ona yöneldiği konusunda kuşku bırakmayacak şekilde ithamlara, yönelimlere yer veren ifadeler olarak kabul edilmektedir.[49]

Bir gerçek kişinin kimliğinin belirlenebilir olup olmadığını tespit için GDPR da aynı paralelde gerçek kişiyi doğrudan veya dolaylı olarak belirlemek amacıyla, grup içinden seçme gibi, kullanılması makul bir şekilde muhtemel tüm yöntemlerin dikkate alınması gerektiğini ifade etmiştir.

Benzer bir ifade Kişisel Verilerin Korunması Hakkında Kanun Tasarısı'nın[50] da kanunun amacı bölümünde yer almıştır. Buna göre bir kişinin belirli veya belirlenebilir olması "…mevcut verilerin herhangi bir şekilde bir gerçek kişiyle

doğmak koşuluyla, ana rahmine düştüğü andan başlayarak elde eder." olarak ifade edilmiştir. Kişilikle ilgili detaylı açıklamalar için bkz.: M. Kemal Oğuzman, Saibe Oktay, **Kişiler Hukuku (Gerçek ve Tüzel Kişiler),** Filiz Kitabevi, 15. Baskı, 2015, s. 11 vd.

[45]Kişisel Verileri Koruma Kurulu'nun 18.09.2019 tarihli ve 2019/273 sayılı kararı. Bkz. https://www.kvkk.gov.tr/Icerik/6710/2019-273 (E.T. 19.01.2024).

[46]Anne bakımından korunacağını savunan görüşler için *Bkz*: Öztekin, s. 10, dn. 40.

[47]Halıcıoğlu, s. 6; Mesut Serdar Çekin, **Avrupa Birliği Hukukuyla Mukayeseli Olarak 6698 Sayılı Kanun Çerçevesinde Kişisel Verilerin Korunması Hukuku,** On İki Levha Yayıncılık, 2. Baskı, Ekim 2019, s. 42; Ersoy Kekevi, s. 105.

[48]Kişisel Verileri Koruma Kurumu, "6698 Sayılı Kanun'da Yer Alan Temel Kavramlar**"**, s. 14 (https://kvkk.gov.tr/Icerik/2030/Rehberler E.T.:19.01.2024) **[KVKK, Temel Kavramlar].**

[49]Yargıtay 4. Hukuk Dairesi 26.12.2017 tarihli, E. 2016/2955, K. 2017/8684 sayılı karar (Kazancı, E.T.: 22.06.2024).

[50]TBMM, 2016. Kanun Tasarısı, https://www5.tbmm.gov.tr/sirasayi/donem26/yil01/ss117.pdf (E.T.:10.01.2024).

ilişkilendirilmesi suretiyle, o kişinin tanımlanabilir hale getirilmesi" olarak ifade edilmiştir. İlgili ifade, "Yani verilerin; kişinin fiziksel, ekonomik, kültürel, sosyal veya psikolojik kimliğini ifade eden somut bir içerik taşıması veya kimlik, vergi, sigorta numarası gibi herhangi bir kayıtla ilişkilendirilmesi sonucunda kişinin belirlenmesini sağlayan tüm halleri kapsar. İsim, telefon numarası, motorlu taşıt plakası, sosyal güvenlik numarası, pasaport numarası, özgeçmiş, resim, görüntü ve ses kayıtları, parmak izleri, genetik bilgiler gibi veriler dolaylı da olsa kişiyi belirlenebilir kılabilme özellikleri nedeniyle kişisel verilerdir." şeklinde devam etmektedir.

KVKK'nın gerekçesinde kişinin adı, soyadı, doğum tarihi gibi bilgiler kişinin belirlenebilir olmasını sağlayan bilgilere örnek olarak verilmiştir.[51] Dikkat edilmelidir ki bu bilgiler her zaman kişinin mutlak tespitini sağlamamaktadır, sağlaması da beklenmemektedir. Aynı isme veya bilgilere sahip birden fazla kişi olabilir ya da kişi ismi yanlış yazılmış da olabilir. Bu nedenle, olayın koşulları göz önünde tutularak objektif bir teşhis yapılmalıdır. Yine de, aynı isimde kişiler olduğu için ad soyad kullanılarak kişinin kesin tespitinin yapılamayışı, ad soyad verilerini kişisel veri olmaktan çıkarmaz.[52] Başka bir deyişle, kişisel veri, tek başına kişiyi belirli kılmaya elverişli olmasa da diğer verilerle bir araya geldiğin de kişinin kimliğini belirlenebilir bir hale getirme kabiliyetine sahiptir.[53] Öte yandan, kişinin kimliğinin belirlenebilir sayılabilmesi için kişinin kimliğini belirli hale getirecek verilerin muhakkak veri işleyen kişinin hâkimiyetinde bulunmasına gerek yoktur; üçüncü bir kişi de kimlik tespiti yapabiliyorsa belirlenebilirlik söz konusudur.[54]

[51] Kişisel Verileri Koruma Kurumu, **Madde ve Gerekçesi ile Kişisel Verilerin Korunması Kanunu (Bilgi Notu) ve Kişisel Verilerin Korunmasına İlişkin Terimler Sözlüğü**, KVKK Yayınları, Ankara, 2019, s. 9 ["**KVKK, Gerekçe ve Terimler Sözlüğü"].**
[52]KVKK**, Örneklerle Kişisel Verilerin Korunması**, s. 34; Ersoy Kekevi, s. 106.
[53]Hüseyin Murat Develioğlu, **6698 sayılı Kişisel Verilerin Korunması Kanunu ile Karşılaştırmalı Olarak Avrupa Birliği Genel Veri Koruma Tüzüğü uyarınca Kişisel Verilerin Korunması Hukuku**, 1. Baskı, İstanbul, On İki Levha Yayıncılık, 2017, s. 33-35, Ayözger Öngün, s. 11-12.
[54]Çekin, s. 45-49.

1.1.2. Özel Nitelikli Kişisel Veriler

Bir verinin hassas olarak nitelendirilip nitelendirilmeyeceği, veri işlenme sürecinde tabi olunacak şartları etkileyeceğinden kişisel veri tanımı yapılırken özel nitelikli kişisel verilere değinmek gerekir.

Mevzuatta bazı tür verilerin diğer verilere oranla daha sağlam bir koruma altına alındığı görülebilir. Bu tür veriler daha özel veya GDPR gerekçesinde ifade edildiği biçimde "hassas" verilerdir.[55] Kısaca hassas veriler, özel bir korumaya tabi olan ve belirli kurallar olmadan işlenmesi kişiler arasında birtakım haksızlıklara yol açabilecek olan kişisel verilerdir.[56]

108 Sayılı Avrupa Sözleşmesi'nin "özel veri kategorileri" başlıklı 6. maddesi "iç hukukta uygun güvenlik önlemleri alınmadığı sürece kişinin ırksal kökeni, siyasal düşünceleri, dini yahut diğer inançlarına ilişkin verileri, sağlık veya cinsel hayatıyla ya da ceza mahkumiyet durumuyla ilgili kişisel veriler otomatik işleme tabii tutulamaz." ifadeleri ile işleme faaliyetleri için iç hukuktaki güvenlik önlemlerinin alınmasını şart koşmuştur. [57] Ve devamında "…tek başına veya kümülatif olarak; ilgili kişinin açık onayı; işlemle hedeflenen amaç ve araçları veya bu işlemlerin yapılmasına izin verilebilecek istisnai durumları belirten bir yasa; bir mesleki sır yükümlülüğü; risk analizini takiben alınan önlemler; belirli ve nitelikli bir organizasyonel veya teknik güvenlik önlemi (örneğin veri şifreleme) gibi özel nitelikli verilerin meşru amaçlarla işlenmesine uygun güvenlik önlemleri (örneğin, söz konusu risklere ve korunacak menfaatlere, haklara ve özgürlüklere uyarlanmış) belirlenmelidir".[58] ifadeleri ile uygun güvenlik önlemleri alınması gerektiğine yer vermiştir. İlgili maddeye göre ayrıca biyometrik verilerin işlenmesi, ilgili kişiyi benzersiz bir şekilde belirlemek amacıyla kullanılıyorsa özel nitelikli veri özelliğindedir. Bu kıstas görüntülerin işlenmesi durumu için de bu şekilde geçerli olacaktır, ek olarak görüntülerin işlenmesi kişinin ırk, etnik köken veya sağlık bilgisinin ortaya çıkarılması amacıyla yapılıyorsa

[55]*Bkz*. https://www.ab.gov.tr/siteima.g.e.,s/resimler/Nihai-ABB-HCDB-GDPR.pdf (E.T.:25.01.2024).
[56]Küzeci, s. 254 vd.**;** Budak, s. 18; Metin Bulut. **Özel Bir Hukuksal Koruma Ve Veri Kategorisi Alanı: Hassas Kişisel Veriler**, Ankara Barosu Dergisi, Cilt 78, Sayı 3, 2020, s. 109.
[57]Dülger, s. 13.
[58]Kişisel Verilerin İşlenmesi Karşısında Bireylerin Korunması için Sözleşme, 108 Konvansiyon, *Bkz*. https://itlaw.bilgi.edu.tr/media/2019/9/19/Convention108%2B_Ac%CC%A7%C4%B1klay%C4%B1c%C4%B1_Rapor.pdf (E.T.:25.01.2024).

bu durumda da özel nitelikli veri olacaktır. Burada önemli olarak belirtilmelidir ki 108 sayılı Avrupa Sözleşmesi'nde sayılan kategorilerin kapsamlı olması amaçlanmamıştır ve Sözleşme'nin Açıklayıcı Raporu'nda imzacı devletlerin ulusal hukuklarında başka hassas veri kategorileri oluşturmalarına izin verildiği ifade edilmiştir.[59]

Ancak KVKK'da özel nitelikli kişisel veriler için numerus clausus ilkesi geçerlidir; Kanun'da sayılanlar dışındaki veriler için kıyas yolu ile genişletilme yapılması söz konusu değildir.[60]

95/46/EC Sayılı Direktif'in 33. maddesinde "veri öznesi açık şekilde rıza göstermezse, temel özgürlükleri veya kişisel mahremiyeti ihlal eden yapıdaki veriler işlenmemelidir" denilmektedir. Buradan da görülebilir ki özel nitelikli kişisel veriler temel hakları ve özel hayatın gizliliğini ihlal eden veriler olarak tanımlanmaktadır.[61] Direktif m. 8'de ise "Üye Devletler, sağlık durumuna veya cinsel yaşama ilişkin verilerin işlenmesini ve sendika üyeliğini, dini veya felsefi inançları, siyasi görüşleri, ırk veya etnik kökeni açıklayan kişisel verilerin işlenmesini yasaklayacaktır." denilmiş ve bu özel nitelikli verilerin neler olacağı tanımlanmıştır.

GDPR m.9'un 1. fıkrasında "ırksal veya etnik köken, siyasi görüş, dini veya felsefi inançlar, ticaret birliklerine üyeliği gösteren kişisel veriler ile genetik, biyometrik veriler, cinsel hayata veya cinsel tercihe ilişkin bilgiler" hassas kişisel veri olarak belirtilmiştir. Bunun yanında 10. maddede mahkûmiyetler ve güvenlik tedbirlerine ilişkin verilerden de bahsedilmiştir ve bu tür verilerin de farklı bir şekilde ele alınıp işleneceği ifade edilmiştir. Nitekim GDPR Resital 51'de de bu hususta bahsedilmiş, "doğası gereği, temel hak ve özgürlüklerle ilgili olarak özellikle hassas olan kişisel veriler, işlenmeleri bağlamında temel hak ve özgürlükler açısından önemli riskler yaratabileceğinden, özel korumayı hak etmektedir" denilmiştir. Resital 51,

---

[59]Avrupa Konseyi, **Explanatory Report to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data**, Strasbourg 1981, s. 9. *Bkz*. https://rm.coe.int/16800ca434 (E.T.:28.01.2024); Paul Quinn, Gianclaudio Malgieri, "The Difficulty of Defining Sensitive Data – The Concept of Sensitive Data in the EU Data Protection Framework", German Law Journal, 2020, (Son güncelleme tarihi 2021), s. 5.

[60]Kişisel Verilerin Korunması Kurumu, **Kişisel Verilerin Korunması Kanununa İlişkin Uygulama Rehberi**, KVKK Yayınları, Ankara 2019, s. 80 **["KVKK, Uygulama Rehberi"];** Ersoy Kekevi, s. 109; Dülger, s. 14.

[61]Cemil Kaya, A**vrupa Birliği Veri Koruma Direktifi Ekseninde Hassas (Kişisel) Veriler ve İşlenmesi**, İÜHFM, Cilt 69, Sayı 1-2, 2011, s. 318; Aygözer Öngün, s. 19.

fotoğrafların işlenmesinin sistematik olarak hassas veri kategorisinde değerlendirilmemesi gerektiğini, ancak fotoğraflar gerçek bir kişinin benzersiz bir şekilde tanımlanmasına sebep olduğu zaman hassas veri kategorisine dâhil olacağını ifade etmiştir. GDPR'ın, hassas verilerin işlenmesine izin verilmediği özel durumlarda üye devletler hukukundan önce dikkate alınması gerektiğini de ayrıca belirtmiştir.[62]

GDPR m. 37 uyarınca, GDPR m. 9'da sayılmış olan özel nitelikli verilerin veya m. 10'da ifade edilmiş olan ceza mahkûmiyeti veya suça ilişkin kişisel verilerin işlenmesi durumunda; veri sorumlusu veya veri işleyen 'veri koruma görevlisi' olarak belirlenmektedir. Veri Koruma Görevlisinin veri koruma alanında yeterli uzmanlığının olması gerekir ve bu görevli veri işleme faaliyetinden sorumludur. Veri koruma görevlisi iş sözleşmesi ile istihdam edilen bir üçüncü kişi de olabilir ve bu görevli birden çok şirket veya kamu kurumu için aynı anda çalışabilir.[63]

7499 sayılı Ceza Muhakemesi Kanunu İle Bazı Kanunlarda Değişiklik Yapılmasına Dair Kanun'un[64] 35'inci maddesiyle 01.06.2024 tarihinde yürürlüğe girmek üzere KVKK'nın özel nitelikli kişisel verilerin işlenme şartlarını düzenleyen 6'ncı, kişisel verilerin yurt dışına aktarılmasını düzenleyen 9'uncu ve kabahatleri düzenleyen 18'inci maddelerinde değişiklikler yapılmıştır.

Kanun'un özel nitelikli kişisel verilerin işleme şartlarını düzenleyen 6. maddesinin yeni halinde özel nitelikli kişisel veri tanımı, özel nitelikli kişisel verilerin işlenmesinin yasak olduğu vurgusu, açık rıza hukuki işleme sebebi, sır saklama yükümlülüğü altında bulunan kişiler veya yetkili kurum ve kuruluşlar tarafından özel nitelikli kişisel verilerin açık rıza gerektirmeksizin işlenmesi hukuki işleme sebebi, özel nitelikli kişisel verilerin işlenmesinde Kurul tarafından belirlenen yeterli önlemlerin alınmasının şart olduğu hüküm aynen muhafaza edilirken; Hukuki işleme sebepleri genişletilmiş, kanunlarda öngörülme ifadesine "açıkça" ibaresi eklenmiş, fiili imkansızlık durumunda özel nitelikli kişisel verilerin işlenmesi yeni bit hukuki

[62]Resital 51, *Bkz*. https://gdpr-info.eu/recitals/no-51/ (E.T.:28.01.2024).
[63]Akıncı, s. 17.
[64]Yayımlanma Tarihi: RG 12/3/2024, S. 32487.

işleme sebebi olarak tanımlanmış, aleni özel nitelikli kişisel verilerin işlenmesi yeni bir hukuki işleme sebebi olarak tanımlanmış, bir hakkın tesisi, kullanılması veya korunması yeni bir hukuki işleme sebebi olarak tanımlanmış, istihdam, iş sağlığı ve güvenliği, iş ve sosyal güvenlik veya sosyal hizmetler ile sosyal yardım alanındaki hukuki yükümlülüklerin yerine getirilmesi yeni bir işleme sebebi olarak tanımlanmış, siyasi, felsefi, dini veya sendikal amaçlarla kurulan vakıf, dernek veya diğer kar amacı gütmeyen kuruluş ya da oluşumların üyelerine yönelik kişisel verilerin işlenmesi yeni bir hukuki işleme sebebi olarak tanımlanmıştır.[65]

Özel nitelikli kişisel verilerin işlenme şartları, güncel ihtiyaçlar ve GDPR'a uyumluluk gözetilerek yapılan bu değişiklik ile özel nitelikli kişisel veriler altında düzenlenen sağlık ve cinsel hayata ilişkin veri ve diğer özel nitelikli kişisel veri ayrımı kaldırılmıştır ve işlenme şartları için öngörülmüş hukuka uygunluk sebepleri genişletilmiştir.

1.1.3. Genel Nitelikli Kişisel Veriler

Özel nitelikli kişisel veriler, yukarıda da açıklandığı üzere sayılmış veya ifade edilmiştir. Bu tanımlamalar dışında kalan tüm kişisel veriler ise genel nitelikte kişisel nitelikteki genel verilerdir.[66] Başka bir deyişle kişisel veri niteliğinde olan ve kişinin ayırt edilmesini sağlayan fakat özel nitelikli olarak sayılmamış olan, hassas nitelik taşımayan verilere genel nitelikli kişisel veri denilir.[67]

1.1.4. Kişisel Verilerin İşlenmesi

Kişisel verilerin işlenmesi kavramı KVKK m. 3/1-e'de "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,

[65]Kaya, Mehmet Bedii, **(2024) KVKK Reformu: 2024 Değişiklikleri** (Dijital Baskı 1.0), s. 8-23. https://mbkaya.com/hukuk/kvkk-reformu.pdf
[66]Budak, s. 20.
[67]Ayözger Öngün, s. 34**;** Abdülhamit Zor, **Veri Sorumlusunun Yükümlülükleri Ve Bu Yükümlülükleri İhlalinden Doğan Özel Hukuk Sorumluluğu**, Yüksek Lisans Tezi, İstanbul Üniversitesi, İstanbul 2020, s. 51.

devralınması, elde edilebilir hâle getirilmesi, sınıflandırılması ya da kullanılmasının engellenmesi gibi veriler üzerinde gerçekleştirilen her türlü işlemi…" olarak ifade edilmiştir. Buradan da görülebilir ki işleme faaliyeti geniş bir biçimde tanımlanmıştır, bu durumda kişisel veri üzerinde gerçekleşecek tüm eylemlerin kişisel verileri işleme niteliği taşıma olasılığı yüksektir.[68]

GDPR m. 4/2'de ise işleme; "otomatik yollarla olsun veya olmasın, kişisel veriler veya kişisel veri setleri üzerinde gerçekleştirilen toplama, kaydetme, düzenleme, yapılandırma, depolama, uyarlama veya değiştirme, geri getirme, danışma, kullanma, iletim yoluyla açıklama, yayma veya bir başka şekilde kullanıma sunma, uyumlaştırma ya da birleştirme, kısıtlama, kalıcı olarak silme veya yok etme gibi herhangi bir işlem veya işlem setidir" olarak tanımlanmıştır.

KVKK'da otomatik olmayan yollarla işlemenin veri kayıt sisteminin parçası olmak kaydıyla işleme sayılması şartı, "işleme" faaliyetinin tanımında yer almakta iken; GDPR'da bu şart maddi kapsam başlıklı m. 2/1'de "Bu Tüzük, kişisel verilerin tamamen veya kısmen otomatik yollarla işlenmesine ve bir dosyalama sisteminin parçasını oluşturan veya bir dosyalama sisteminin parçasını oluşturması amaçlanan kişisel verilerin otomatik yollar haricinde işlenmesine uygulanır" şeklinde yer almıştır. KVKK'nın aksine GDPR'da işleme faaliyetinin otomatik olması veya olmaması gibi bir ayrım olmaksızın korunduğu görülebilir.[69]

Bu iki tanımın da anlaşılabilmesi için otomatik olan ve otomatik olmayan yollarla işleme faaliyetleri arasındaki farkların netleşmesi gerekmektedir. Bu iki tanımın arasındaki temel fark insan müdahalesidir.[70] Şöyle ki; KVKK'nın genel gerekçesinde "Günümüzde bu veriler, gerek özel sektör ve gerekse kamu sektörü tarafından bilişim sistemleri üzerinden otomatik yollarla sıkça kullanılmaktadır" denilmiştir. Buradaki tanımdan kişisel verilerin bilişim sistemleri üzerinden herhangi bir işleme tabii tutulmasının, kişisel verilerin 'otomatik yollarla işlenmesi' durumunu oluşturduğu görülebilir. Kişilerin bilişim sistemleri aracılığıyla olmadan

[68]Öztekin, s. 13; Çekin, s. 46; Budak, s. 27-28.
[69]Budak, s. 28; Nevzat Ali Anı, **Kişisel Verilerin İşlenmesi ve Açık Rıza**, Yüksek Lisans Tezi, İstanbul Üniversitesi, İstanbul, 2018, s. 88.
[70]Dülger**,** s. 15; Öztekin**,** s. 14; Budak, s. 28.

gerçekleştirdiği işlemler ise otomatik olmayan yollarla işleme faaliyetini oluşturacaktır.[71]

KVKK'da işleme faaliyeti kısmen veya tamamen otomatik yollarla gerçekleşirse şart olmaksızın korunmaktadır. Otomatik olmayan işleme faaliyeti ise işlemenin konusu olan kişisel veriler bir veri kayıt sisteminin parçası haline geliyorsa korunur.[72]

KVKK'da sayılan on iki adet işleme faaliyetinden sonra kullanılan "gibi" ifadesinden de anlaşılabileceği gibi, işleme faaliyetleri sınırlı bir biçimde sayılmamıştır.[73] Benzer şekilde GDPR'da da "herhangi bir işlem" ibaresi kullanılmıştır ve sınırlanmamıştır.

GDPR m. 35'teki düzenleme uyarınca veri işleme faaliyetinin ilgili kişilerin hak ve özgürlükleri bakımından yüksek risk içerdiği muhtemel durumlarda, GDPR hükümlerine uyumun artırılması için veri sorumlusunun bir veri koruma etki değerlendirilmesi yapması beklenir. GDPR m. 35/2'de ne gibi durumlarda bu değerlendirmenin yapılacağı ayrıntılı olarak ifade edilmiştir.[74] Yine, 84. Resital'de de bu veri koruma etki ve risk değerlendirilmesinden bahsedilmiş ve ilgili değerlendirmenin kişisel verilerin işlenmesinin GDPR ile uyumlu olması için alınması gereken makul tedbirler belirlenirken dikkate alınması gerektiği ifade edilmiştir. Ayrıca etki değerlendirmesi, veri sorumlusunun mevcut teknoloji ve uygulama maliyeti bakımından alınabilecek uygun tedbirlerle azaltılamayacak bir risk içerdiği durumlarda, veri koruma otoritesine danışılması gerektiği de yer almaktadır.[75] Ayrıca 95. Resital uyarınca, veri işleyenin de gerektiği hallerde veri koruma etki değerlendirmelerinin gerçekleştirilmesinden ve veri koruma otoritesine danışılmadan kaynaklanan yükümlülüklere uyması konusunda veri sorumlusuna yardımcı olması gerektiği belirtilmiştir.[76]

[71]Dülger, s. 15; Budak, s. 14.
[72]Dülger, s. 16.
[73]Çekin, s. 46.
[74]Akıncı, s. 17.
[75]Resital 84. *Bkz*. https://gdpr-info.eu/recitals/no-84/ (E.T.:17.03.2024).
[76]Resital 95. *Bkz*. https://gdpr-info.eu/recitals/no-95/ (E.T.: 17.03.2024).

Kişisel verilerin korunması için, işleme faaliyetinin kontrollü yapılması gerekir.[77] Nitekim "genel ilkeler" başlıklı KVKK m. 4'te verilerin işlenmesi sırasında riayet edilecek temel ilkeler sıralanmıştır. İlgili maddede bunlar; "(1) Kişisel veriler, ancak bu Kanunda ve diğer kanunlarda öngörülen usul ve esaslara uygun olarak işlenebilir. (2) Kişisel verilerin işlenmesinde aşağıdaki ilkelere uyulması zorunludur: a) Hukuka ve dürüstlük kurallarına uygun olma. b) Doğru ve gerektiğinde güncel olma. c) Belirli, açık ve meşru amaçlar için işlenme. ç) İşlendikleri amaçla bağlantılı, sınırlı ve ölçülü olma. d) İlgili mevzuatta öngörülen veya işlendikleri amaç için gerekli olan süre kadar muhafaza edilme." şeklinde düzenlenmiştir.

1.1.4.1. Hukuka ve Dürüstlük Kuralına Uygun Olmak

Kişisel verilerin hukuka uygun bir şekilde işlenmesi mevzuattaki düzenlemelere uygun olarak hareket etmeyi zorunlu kılar.[78] Buradaki ilke, kapsayıcı ve geniş bir ilkedir; buradaki hukuka uygunluk ifadesi yalnızca özel norm niteliğindeki hükümlerle sınırlı değildir; ayrıca genel hukuk kuralları ve evrensel hukuk ilkelerine uygun olması gerektiğini ifade eder.[79] Bu ilke ayrıca verinin elde edildiği ilk andan itibaren geçerli olur; veri sorumlusu ve veri işleyen bu ilkeyi her aşamada dikkate almakla yükümlüdür.[80]

Buradaki dürüstlük kuralı ise 4721 sayılı Türk Medeni Kanunu[81] m.2'de düzenlenen dürüstlük kuralı ve hakkın kötüye kullanılması yasağını ifade etmektedir. Bu kapsamda, veri sorumlusunun verileri işlerken ilgili kişilerin yararını gözetmesi esastır.[82] Veri sorumlusu, verileri işlerken güttüğü kişisel amaç ile ilgili kişinin yararları arasındaki makul dengeyi sağlamalıdır.[83]

GDPR'da ilgili ilke, "hukuka uygunluk, adalet ve şeffaflık" başlığı altında yer alır. Buradaki şeffaflık ilkesi, TMK m.2'ye yapılan atfı biraz daha somut hale

[77]Dülger, s. 16.
[78]KVKK, **Temel İlkeler**, s. 1.
[79]Dülger**,** s. 109; Halıcıoğlu, s. 45; Budak, s. 30.
[80]Küzeci, s. 207; Budak, s. 31; Halıcıoğlu, s. 45.
[81]Yayımlanma Tarihi: RG 8/12/2001 S. 24607.
[82]Küzeci, s. 207; Halıcıoğlu, s. 45-46.
[83]Halıcıoğlu, s. 46.

getirmektedir. Veri sorumlusu verileri, hukuka uygunluk sınırlarında, adil ve şeffaf bir şekilde işlemelidir.

1.1.4.2. Doğru ve Gerektiğinde Güncel Olmak

Bu ilke kısaca, kişisel verilerin doğru ve gerektiğinde güncel olmasını sağlama yükümlülüğünü veri sorumlusuna yükler. Veri sorumlusu, bu durumu sağlayacak kanalları açık tutmalıdır.[84] İlgili ilke, GDPR'da da aynı bağlamda düzenlenmiştir.

İlke, ilgili kişinin verilerin düzeltilmesini istemesi ile de bağlantılıdır.[85] Bu bağlamda veri sorumlusunun örnek olarak ilgili kişilere kendi verilerinin düzeltilmesi için başvuru yapabilme kanallarını sağlaması ve yapılan başvuruları dikkate alması gerekir.

Bu ilke ile korunması amaçlanan değer, ilgili kişilerin güncel olmayan ve kaydı yanlış tutulmuş olan kişisel verilerden zarar görmemesini sağlamaktır; kişisel verilerin korunması da ancak bu şekilde mümkün hale gelir.[86]

İlgili konuya ilişkin en çok tartışılan konu güncel bilgilere nasıl ulaşılacağıdır. Güncel bilgi, veri sorumlusunun kendiliğinden elde edeceği bir bilgi olarak mı değerlendirilmelidir, yoksa ilgili kişinin güncel verilerini veri sorumlusuna ulaştırması gerekmektedir? Bir görüş, bu hususa yönelik ilgili kişinin değişen bilgisini veri sorumlusuna bildirmesinin makul olduğunu savunmaktadır; veri sorumlusunun elinde tuttuğu bilgilerin sürekli değişip değişmediğini kontrol etmesi veri sorumlularına çok ciddi bir iş yükü yükleyecektir ve uygulamada sorunlu bir bakış açısı olacaktır. Ayrıca veri sorumlusunun olumsuz sonuçlarla karşılaşmaması için düzenli aralıklarla ilgili kişilere bilgilerinin doğruluğunu kontrol etmelerine olanak sağlayan bir sistem kurulmalıdır.[87] Bir başka görüş ise veri sorumlusunun sakladığı ve işlediği verileri güncel tutmak için uygun bir veri işleme ve elde etme yöntemi belirlemesi ve düzenli

[84]Halıcıoğlu, s. 46.
[85]KVKK, **Temel İlkeler**, s. 5.
[86]Dülger**,** s. 131; Halıcıoğlu, s. 47; Budak, s. 32.
[87]Dülger, s. 133.

aralıklarla bilgilendirmenin yapılabileceği bir sistem kurması gerektiğini ifade etmiştir.[88]

Kanaatimizce, veri sorumlusunun bilmesi beklenemeyen değişiklikleri ilgili kişinin bildirmesi ve bilip düzeltmesinin mümkün olduğu değişikliklerden veya yanlışlıklardan kendisinin sorumlu olması makul bir yaklaşım olacaktır. Uygulamada veri güvenliğini sağlamak adına ciddi yükümlülükleri olan veri sorumlusunun, değişen her kişisel veriden kendiliğinden haberdar olmasını beklemek gerçekçi olmayacaktır.

Son olarak belirtilmelidir ki işlenen kişisel verilerin doğru ve güncel olması veri sorumlusuna bizzat yüklenmiş bir yükümlülüktür, bu yükümlülük bir temsilcinin yetkilendirilmesi ile devredilemez. Veri sorumlusunun bu noktada aktif bir özen yükümlülüğü söz konusudur, ancak bu husus ancak ilgili kişinin verilerinin, ilgili kişi üzerinde direkt sonuç doğuran hususlarda geçerli olduğunu da belirtmek gerekir.[89]

1.1.4.3. Belirli, Açık ve Meşru Amaçlar İçin İşlenmek

Bu ilke, veri işlemenin sınırını belirleyen ve hangi amaç ile işleneceğini ifade eden ilke olduğundan, veri işleme için en önem arz eden ilkelerden biridir.

Verinin toplanma amacının belirli ve açık olması; ilgili kişilerin maddi ve manevi bütünlüğü, AY ve AİHM'de de korunan özel hayatın gizliliği gibi temel haklar açısından oldukça önem arz eder.[90] Burada veri sorumlusu işleme amacından sapan verileri veya işleme için gereken veriden fazlasını süresiz, sınırsız ve anonimleştirmeden depolamamalıdır.[91]

KVKK'nın gerekçesinde "veri sorumlusunun, veri işleme amacını açık ve kesin olarak belirlemesini ve bu amacın meşru olmasını zorunlu kıldığını; aksi durumlarda veri sorumlularının, belirttikleri bu amaçlar dışında, başka amaçlarla veri

[88]Halıcıoğlu, s. 47.
[89]Kişisel Verileri Koruma Kurumu, **"6698 Sayılı Kişisel Verilerin Korunması Kanunu Hakkında Doğru Bilinen Yanlışlar - 2**, KVKK Yayınları, Ankara, 2020, s. 23 **["KVKK, Doğru Bilinen Yanlışlar 2"];** Dülger, s. 133.
[90]Halıcıoğlu, s. 48.
[91]Küzeci, s. 209; Halıcıoğlu, s. 48; Budak, s. 33.

işlemeleri halinde, bu fiillerinden dolayı sorumlu olacakları" denilmiş ve ilgili ilkenin amacı bu şekilde açıklanmıştır.[92] Yine, KVKK'nın gerekçesinde verilerin meşru amaçlarla işlenmesi durumu "veri sorumlusunun işlediği verilerin, yapmış olduğu iş veya sunmuş olduğu hizmetle bağlantılı ve bunlar için gerekli olması" şeklinde tanımlanmıştır.[93]

Meşruluk durumu, GDPR'da yer alan birtakım durumlarla somutlaştırılmıştır. Buna göre, ilgili kişinin rızasının bulunması, ilgili kişinin taraf olduğu bir sözleşmenin ifası veya ilgili kişinin bir sözleşmenin tarafı olmadan önceki isimleri sebebiyle işlemenin gerekliliği, veri sorumlusunun hukuki yükümlülüğünü gerçekleştirebilmesi için işlemenin zorunluluğu gibi bazı durumlar sıralanmıştır.[94]

1.1.4.4. İşlendikleri Amaçla Bağlantılı, Ölçülü ve Sınırlı Olmak

KVKK gerekçesinde bu ilkeyle ilgili "işlenen verilerin, belirlenen amaçların gerçekleştirilebilmesine elverişli olmasını, amacın gerçekleştirilmesiyle ilgili olmayan veya ihtiyaç duyulmayan kişisel verilerin işlenmesinden kaçınılması" amaçlandığı ifade edilmiştir.[95]

Bu ilke farklı kaynaklarda farklı kavramlarda bulunabilmektedir. Kimi kaynaklarda bu ilke yerine "veri ekonomisi" ifadesi de kullanılmıştır; yani veri sorumlusu amacına ulaşmak için en az miktardaki veriyi kullanmalı ve kullanımını sınırlandırmalıdır.[96] Başka bir deyişle, veri sorumlusu "veri tasarrufunda" bulunacaktır.[97]

Amaca bağlılık ve amacın sınırlandırılması hususları ise verilerin işlenmeleri için öngörülmüş olan amaç ile bağlantılı olmasını gerektirir.[98] GDPR'da bu husus amacın sınırlandırılması olarak ifade edilir ve buna göre veri sorumlusu sadece

[92]KVKK, **Gerekçe ve Terimler Sözlüğü**, s. 7-8.
[93]KVKK, **Gerekçe ve Terimler Sözlüğü**, s. 7-8.
[94]*Bkz*. GDPR m. 9.
[95]KVKK, **Gerekçe ve Terimler Sözlüğü**, s. 7.
[96]Küzeci, s. 53; Halıcıoğlu, s. 52; Budak, s. 34.
[97]Halıcıoğlu, s. 52.
[98]Dülger, s. 125.

belirlediği amaç için verileri işleyebilecektir. Buradaki yaklaşım meşruluk ilkesi ile bu açıdan bağlantılıdır.[99]

1.1.4.5. İlgili Mevzuatta Öngörülen veya İşlendikleri Amaç İçin Gerekli Süre Kadar Saklanmak

KVKK'nın genel gerekçesinde bu ilke; "kişisel verileri, anca ilgili mevzuatta öngörülen veya işlendikleri amaç için gerekli olan süre kadar muhafaza edilecektir ve veri sorumluları, ilgili mevzuatta verilerin saklanması için öngörülen bir süre varsa bu süreye uygun hareket edecek; aksi durumda verileri, ancak işlendikleri amaç için gerekli olan süre kadar muhafaza edebilecektir" olarak açıklamıştır.[100]

Veri sorumlusunun verilerin ne zaman silineceğini, anonimleştirileceğini ya da yok edileceğini belirlemesi gerekir. Buradaki süre, ilkenin lafzında da yer aldığı üzere ilgili mevzuatlarda belirlenmiş olabileceği gibi, veri sorumlusu tarafından da makul bir ölçüt göze alınarak belirlenebilir.[101] Uygulamada veri sorumluları bu ilke uyarınca uygun saklama ve imha politikaları belirlemektedir.

Fransız Veri Koruma Otoritesi, veri sorumlusunun web sitesine üye olurken gereğinden fazla bilgi topladığını ve bu bilgileri belirttiği üzere 10 yıl süreyle değil, daha uzun süre boyunca sakladığı bir somut olayda; veri sorumlusunun ayrıca şifreleme için kurduğu yöntemi zayıf bulmuştur. Veri sorumlusunun GDPR m. 32'den kaynaklanan yükümlülüklerini ihlal ettiğine hükmedilmiş, kişisel verilerin gerekenden daha uzun süre tutulması, gizlilik politikalarının eksik olması, kişisel verilerin yeterince güvence altına alınmaması nedeniyle 105.000 Euro para cezasına hükmetmiştir.[102]

[99]Halıcıoğlu, s. 52.
[100]KVKK, **Gerekçe ve Terimler Sözlüğü**, s. 8.
[101]Dülger, s. 136; Halıcıoğlu, s. 54; Budak**,** s. 36.
[102]CNIL (France) - SAN-2023-023, "*GDPRhub, ,* https://gdprhub.eu/index.php?title=CNIL_(France)_-_SAN-2023-023&oldid=39536" (E.T.: 19.03.2024).

1.1.4.6. GDPR Uyarınca Hesap Verilebilirlik İlkesi

Hesap Verilebilirlik İlkesi GDPR'da yer alan ilkelerden bir diğeridir; veri sorumlusunun yükümlülüklerini yerine getirmesini amaçlar.[103] Buna göre, veri sorumlusunun ispatlanabilir bir uyum süreci yürütmesi esastır. Veri sorumlusu ayrıca etki analizi yapmalıdır. Ayrıca GDPR m. 37'de düzenlenen veri koruma görevlisi atanması ile veri sorumlusunun hesap verilebilirlik ilkesi kapsamında yükümlülüklerini yerine getirmesi ve yasal süreçleri sürdürebilmesinin garantilenmesi amaçlanmıştır.[104] KVKK kapsamında veri analizi ve veri koruma görevlisi düzenlenmemiştir.

1.1.5. Veri Sorumlusu ve Veri İşleyen

Veri sorumlusu ve veri işleyen kavramları kişisel verilerin korunması hukuku için oldukça önemli kavramlardır. Özellikle veri sorumlusunun doğru tespit edilebilmesi oldukça önemlidir, çünkü birçok mevzuatta sorumlulukların birçoğu veri sorumlusuna yüklenmiştir ve merkezi bir konuma sahiptir.[105]

1.1.5.1. Veri Sorumlusu

KVKK'nın 3. maddesi 1. fıkrasında veri sorumlusu, "kişisel verilerin işleme amaçlarını ve vasıtalarını belirleyen, veri kayıt sisteminin kurulmasından ve yönetilmesinden sorumlu olan gerçek veya tüzel kişi" olarak tanımlanmıştır. GDPR'da ise veri sorumlusu için "controller" terimi kullanılmıştır.

Avrupa Birliği Türkçe çevirisi uyarınca veri sorumlusu terimi "yalnız başına veya başkalarıyla birlikte kişisel verilerin işlenmesinin amaçlarını ve yollarını belirleyen gerçek veya tüzel kişi, kamu makamı, kamu kurumu veya diğer organlar" olarak tanımlanmıştır. İlgili maddenin devamında ayrıca veri işleme amaç ve yöntemleri AB veya üye devletlerin hukukuna göre belirlenmesi halinde veri

[103]Kaya, Mehmet Bedii, **Kişisel Verilerin Korunmasında Yeni Paradigma: Hesap Verebilirlik İlkesi**, İÜHFM, Cilt 78, Sayı 4, 2021, s 1884; Budak, s. 38.
[104]Kaya, s. 1887; Budak, s. 38.
[105]Halıcıoğlu, s. 36**;** Çekin**,** s. 48**;** Develioğlu, s. 41; Zor, s. 59.

sorumlusunun AB hukuku veya üye devletlerin hukuku uyarınca tespit edileceği ifade edilmiştir. [106]

GDPR ile veri sorumlusu açısından daha bütüncül bir yaklaşım söz konusu olmuştur. Şöyle ki, veri sorumlusunun veri işleme faaliyeti için bir sebep göstermesi tek başına yeterli gelmemektedir, ayrıca "gerekli teknik ve idari tedbirleri" almakla yükümlüdür.[107] Yani kişisel verilerin işlenmesi faaliyeti kanuna uygun olsa veya ilgili kişinin rızası alınmış olsa dahi, belirli ilkeler dikkate alınmadan gerçekleştirilen veri işleme faaliyeti hukuka aykırı olacaktır.[108]

Veri sorumlusu açısından, ilgili kişideki gibi bir gerçek kişi olma şartı aranmamaktadır. Gerçek kişiler ya da şirketler, vakıflar, dernekler ve kamu kurumları gibi tüzel kişiler veri sorumlusu olabilir.[109] Tüzel kişilik içerisinde veri işleme faaliyetinde bulunan gerçek kişiler veya tüzel kişiliği bulunmayan birimler[110], KVKK'ya göre veri sorumlusu sıfatını haiz değildir.[111] Tüzel kişiliklerde veri sorumlusu sıfatı tüzel kişiliğin kendisine aittir. Veri Sorumluları Sicili Hakkındaki Yönetmelik m.11/1 uyarınca tüzel kişi, veri sorumlusu olmasından kaynaklanan yükümlülüklerini yerine getirmek adına tüzel kişiliği temsile ve ilzama yetkili organı veya ilgili mevzuatta belirtilen kişi veya kişileri görevlendirebilir. Bu birimlerin kendilerine ait bir tüzel kişiliği olmadığından, bu şekilde bir görevlendirme veri sorumlusu sıfatının da bu birimlere geçtiği anlamına gelmeyecektir.[112] Dolayısıyla kamu tüzel kişilikleriyle özel hukuk tüzel kişilikleri arasında bir fark söz konusu değildir. Gerek ceza hukukundan, gerekse özel hukuktan doğan sorumluluklar açısından tüzel kişiliklerin sorumluluğuna ilişkin özel ve kamu hukuku hükümleri uygulanır.[113]

---

[106]*Bkz*. GDPR m. 4/7.
[107]Nur Buğçe Bakırel, **Veri Sorumlusu Ve Veri İşleyen Arasındaki Sorumluluk Paylaşımının Avrupa Birliği Genel Veri Koruma Tüzüğü Ve Kişisel Verilerin Korunması Kanunu Çerçevesinde Değerlendirilmesi**, Yüksek Lisans Tezi, Hacettepe Üniversitesi, Ankara 2020, s. 36; Develioğlu, s. 44.
[108]Bakırel, s. 36; Çekin, s. 47, 49.
[109]Zor, s. 60; Dülger, s. 18.
[110]Yargıtay 6. Hukuk Dairesi 14.12.2016 tarihli, E. 2016/7517 K. 2016/7471 sayılı kararıyla "Anonim şirketler tüzel kişiliğe sahip sermaye şirketlerindendir. Yürütülen ticari faaliyetlerin yaygınlaşması sebebiyle işlerin tek bir merkezden yönetiminin zorlaşması halinde kurulan ve şirketi temsil eden şubelerin ise ayrı bir tüzel kişiliği yoktur." hükmünü kurmuştur. (Kazancı, E.T.: 18.03.2024).
[111]KVKK**, Soru Cevap,** s. 29; Özkan, s. 96.
[112]KVKK, **Soru Cevap**, s. 29; KVKK, **Örneklerle Kişisel Verilerin Korunması,** s. 59.
[113]KVKK**, Örneklerle Kişisel Verilerin Korunması**, s. 59; Çekin, s. 49.

Veri sorumlusu, kişisel verilerin ne amaçla ve nasıl işleneceğini belirler ve buna uygun veri kayıt sistemini kurup yönetir.[114] Veri sorumlusunun tespit edilmesinde kişisel verilerin elde edilmesiyle başlayan süreçte kimlerden veri toplanacağı, hangi tür verilerin hangi yöntemle toplanacağı, toplanan verilerin hangi amaçla işleneceği, işleme kategorilerin belirlenmesi, kimlerin kişisel verilerinin işleneceği, verilerin hangi amaçla yayınlanacağı veya aktarılacağı, ilgili kişinin haklarını kullanıp kullanmadığı ve bu hakların nasıl saklanacağı, kişisel verilerin ne kadar süre ile saklanacağı ve hangi yöntemle imha edileceği, kimlere erişim yetkisi verileceği konularında karar yetkisine sahip olan kişinin kim olduğuna bakılır. Sayılan konularda karar yetkisi olan kişi veri sorumlusudur.[115,116]

KVKK'da yer verilmese de GDPR'da yer alan bir önemli kavram da "ortak veri sorumlusu" kavramıdır. 95/46/EC sayılı Direktif'e veri sorumlusu tanımında amaç ve araçları münferiden veya başkasıyla beraber belirleyen kişi denilerek her ne kadar müşterek veri sorumlusuna bir atıf yapılmış olsa da, ayrıca bir düzenleme yapılmamıştır. Direktif'e göre "kimliği belirli veya belirlenebilir bir gerçek kişiyle ilişkili her tür veri" nin işlenmesinden sorumlu olan tek kişi veri sorumlusuydu. Ancak GDPR m. 26'de yer alan "İşleme amaçlarını ve yöntemlerini iki ya da daha fazla veri sorumlusunun ortak bir şekilde belirlediği hallerde, bu veri sorumluları birlikte veri sorumlularıdır.." düzenlemesi uyarınca ise kişisel veri işleme araçları ve vasıtalarının iki veya daha fazla veri sorumlusunda belirlendiği durumlarda veri sorumluları "müşterek veri sorumlusu" olacaktır.[117] Bu bakımdan GDPR hükümleri, sunucuları AB dışında yerleşik bulunan ve veri işleme eylemini üye devletlerin dışından sürdüren bulut hizmet sağlayıcılar için de geçerli olduğu görülür.[118]

[114]KVKK, **Örneklerle Kişisel Verilerin Korunması,** s. 59; Zor, s. 61; Özkan, s. 97.
[115]Kişisel Verileri Koruma Kurumu (KVKK), **"Veri Sorumlusu ve Veri İşleyen"**, (Çevrimiçi), https://www.kvkk.gov.tr/SharedFolderServer/CM (E.T.: 01.04.2024).
[116]Data controllers and data processors: what the difference is and what the governance implications are,ICO,https://ico.org.uk/media/for-organisations/documents/1546/data-controllers-and-dataprocessors- dp-guidance.pdf , s. 6-7. (E.T.: 02.5.2024); **Veri Sorumlusu ve Veri İşleyen**, Kişisel Verileri Koruma Kurumu, https://www.kvkk.gov.tr/SharedFolderServer/CMSFiles/31d9c444-27a5-4a75-95b1-1ca9bdb81ea5.pdf , s. 2. (E.T.: 02.05.2024)
[117]Bakırel, s. 37; Akıncı**,** s. 14; Çekin**,** s. 53.
[118]Akıncı, s. 14.

Ortak veri sorumluları, veri toplama ya da işleme faaliyetine başlamadan önce GDPR'dan doğan sorumluluklarının aralarında nasıl paylaşılacağını belirlemek zorundadır.[119] Bu paylaşım ilgili kişilerin de ulaşabileceği şekilde olmalıdır. Ayrıca sorumluluk oranını aralarında nasıl belirlemiş olurlarsa olsunlar, ilgili kişi sahip olduğu hakları bu veri sorumlularından her birine kullanabilir.[120]

1.1.5.2. Veri İşleyen

KVKK'nın 3. maddesi 1. fıkrasında veri işleyen, "ğ) Veri işleyen: Veri sorumlusunun verdiği yetkiye dayanarak onun adına kişisel verileri işleyen gerçek veya tüzel kişi" olarak tanımlanmıştır. GDPR m. 4/8'de ise "processor" olarak ifade edilen veri işleyen, "veri sorumlusu adına kişisel verileri işleyen bir gerçek ya da tüzel kişi, kamu kuruluşu, kurumu veya diğer herhangi bir organ" olarak tanımlanmıştır. Bu tanımdan da görülebileceği gibi, veri işleyen için bir veri sorumlusunun varlığı gereklidir. Yani veri işleyen, ancak veri sorumlusu tespit edildikten sonra tespit edilebilir.[121]

Veri işleyen, veri sorumlusu tarafından kendisine verilen talimatlar sonucunda kişisel verileri işleme faaliyetini gerçekleştiren ayrı bir gerçek veya tüzel kişidir.[122] Veri işleyen mutlaka veri sorumlusunun organizasyonu dışındaki bir 3. kişidir, veri sorumlusunun organizasyonunun parçası olan kişiler veri işleyen olarak nitelendirilemez.[123]

Veri işleyen ile veri sorumlusu arasında bir veri işleme sözleşmesi gerçekleştirilir. Bu sözleşme, veri işleyenin belirli talimatlar doğrultusunda veri işleme eylemini taahhüt ettiği, veri sorumlusunun ise bu işleme faaliyeti karşısında bir bedel ödemeyi taahhüt ettiği, iki tarafa da borç yükleyen bir sözleşmedir.[124]

---

[119]IT Governance Prıvacy Team, **EU General Data Protection Regulation (GDPR): An Implementation and Compliance Guide - Second Edition**, IT Governance Yayımları, 2. Baskı, 2017, s. 163; Bakırel, s. 37; Çekin**,** s. 53-54.
[120]Bakırel, s. 37-38; Çekin, s. 53-54.
[121]Öztekin, s. 21.
[122]KVKK**, Uygulama Rehberi,** s. 56**;** Özkan, s. 97.
[123]Özkan, s. 97-98; Kişisel Verileri Koruma Kurumu, **"6698 Sayılı Kişisel Verilerin Korunması Kanunu Hakkında Doğru Bilinen Yanlışlar**, KVKK Yayınları, Ankara, 2019, s. 21 **["KVKK, Doğru Bilinen Yanlışlar "].**
[124]Taştan, s. 119-124. Taştan, s. 119-150; Zor, s. 63.

Gerek KVKK gerek de GDPR'daki tanımlardan anlaşılan bir diğer durum ise veri işleyenin veri işleme faaliyeti sırasında veri sorumlusunun emir ve talimatlarına bağlı olduğu ve bu emir ve talimatlarla sınırlı olarak hareket edebileceğidir.[125] Yine de veri işleyenin her unsura dair veri sorumlusundan emir veya talimat alması durumu pratik hayata uygun değildir. Bu nedenle bazı hallerde veri sözleşmesi ile veri sorumlusu,[126] "Kişisel verilerin toplanması için hangi bilgi teknolojileri sistemlerinin veya diğer metotların kullanılacağı, kişisel verilerin hangi yöntemle saklanacağı, kişisel verilerin korunması için alınacak güvenlik önlemlerinin detayları, kişisel verilerin aktarımının hangi yöntemle yapılacağı, kişisel verilerin saklanmasına ilişkin sürelerin doğru uygulanabilmesi için kullanılacak metot, kişisel verilerin silinmesi, yok edilmesi ve anonim hale getirilmesi yöntemleri" hususlarında karar verme yetkisini veri işleyene bırakabilir.

Veri işleyenin sorumluluklarına dair KVKK'da detaylı bir düzenleme yer almamaktadır. Ancak GDPR kapsamında veri sorumlusuna yüklenen sorumlulukların yanı sıra veri işleyene de bazı sorumluluklar yüklenmiştir.

Veri sorumlusu aynı şekilde veri işleyen de olabilir ve bu durum gerçek kişiler için de geçerlidir.[127] Örneğin bir hukuk bürosu müvekkillerine ve çalışanlarına karşı hem veri sorumlusu hem de veri işleyen konumunda bulunabilir.

Bir görüşe göre, KVKK'daki veri işleyene yönelik olan düzenlemeler eksiktir ve veri işleyen kavramının önemini yansıtmamaktadır. 95/46/EC sayılı Direktif'te veri işleyenin veri sorumlusu ile olan ilişkisine dair daha detaylı düzenlemeler bulunur. GDPR m. 28 uyarınca ise veri işleyenin seçimi hakkında özel hüküm düzenlenmiş ve veri sorumlusu ile aralarında sözleşme zorunluluğu öngörülmüştür. KVKK'da ise bu hususlarda bir düzenleme yer almadığından veri sorumlusu ile veri işleyenin arasındaki ilişki açısından sessiz kalınmıştır. Bu görüş, Direktif'in veya GDPR'ın hükümlerinin dikkate alınmasını isabetli bulmaktadır.[128]

[125]Bakırel, s. 41.
[126]KVKK, **Örneklerle Kişisel Verilerin Korunması,** s. 62-63.
[127]KVKK, **Örneklerle Kişisel Verilerin Korunması**, s. 63; Özkan**,** s. 100-101.
[128]Çekin, s. 58-60.

1.2 Veri Sorumlusunun Yükümlülükleri

KVKK, veri sorumlusuna birtakım yükümlülükler yüklemiştir. Bunlar; aydınlatma yükümlülüğü, veri güvenliğine ilişkin yükümlülükler, veri sorumluları siciline kayıt yükümlülüğü, ilgili kişinin yaptığı başvuruların cevaplanması ve Kurul kararlarının yerine getirilmesi yükümlülüğü ve son olarak Kurul'a bildirim yükümlülüğü şeklinde sayılabilir.

2. KVKK VE GDPR KARŞILAŞTIRMASIYLA VERİ SORUMLUSUNUN VERİ GÜVENLİĞİNE İLİŞKİN YÜKÜMLÜLÜKLERİ

2.1. Genel Olarak

Veri güvenliği ilkesi, kişisel verilerin korunması hukukunun ayrılamaz bir alanıdır. Bu ilke kişisel verilerin korunması hukukunun en temel amaçlarına hizmet eder.[129] Veri güvenliği, belirli bir süreyle sınırlı olmayan, sürekli bir sorumluluktur. Bu nedenle veri güvenliğine ilişkin ilgili tedbirlerin bir defa alınması veri sorumlusunun bu sorumluluğunu yerine getirdiği anlamına gelmeyecektir.[130]

Kişisel verilerin korunması kavramı ile veri güvenliği birbirlerinden farklı kavramlardır.[131] Şöyle ki; kişisel verilerin korunması kavramı ilgili kişinin verilerinin hukuka uygun bir şekilde ve belirli sınırlara uyularak işlenebileceğini ve bu yolla ilgili kişinin hak ve özgürlüklerini korumayı amaçlar. Oysaki veri güvenliği kavramı sadece verinin korunmasını amaçlar ve bu açıdan kişisel verilerin korunması kavramından daha sınırlı bir alanı ifade eder. Bir başka deyişle, kişisel verilerin korunması kavramı veri korunmasını da gerektirir ve kapsar.[132] Kişisel verilerin korunmasında amaç bireylerin korunmasıdır, veri güvenliği bu amaca hizmet eden araç olarak yer alır.[133] Nitekim KVKK'da ve GDPR'da da belirtildiği üzere, veri sorumlusunun kişisel verilerin güvenliğini sağlamak için her türlü idari ve teknik tedbirleri alması gerekir.[134] Veri korunması kavramının hizmet ettiği amaç da budur. Bu bağlamda veri güvenliği ve kişisel verilerin korunması, birbirinden ayrılamaz iki unsurdur.[135]

Veri güvenliğine ilişkin yükümlülükler, KVKK'nın aynı başlıklı 12. maddesinde düzenlenmektedir. Kurum, veri güvenliğini "kişisel verilerin hukuka aykırı olarak işlenmesini ve bu verilere hukuka aykırı olarak erişilmesini önlemeye ve bunların hukuka uygun olarak muhafazasını sağlamaya yönelik gerekli her türlü teknik

[129]Küzeci, s. 262; Dülger, s. 176; Çekin, s. 145.
[130]Dülger**,** s. 176.
[131]Zor, s. 91; Küzeci, s. 253**;** Çekin, s. 145; Halıcıoğlu, s. 84.
[132]Zor, s. 91; Küzeci, s. 253; Halıcıoğlu, s. 84.
[133]Küzeci, s. 262; Çekin, s. 145.
[134]*Bkz*. KVKK m. 12/c; GDPR m. 32.
[135]Çekin, s. 145.

ve idari tedbirlerin alınması" olarak tanımlamıştır.[136] Bu tanım KVKK bakımından eksik bir tanımdır, nitekim ilgili tanım teknik ve idari tedbirlerin alınması yükümlülüğü paralelinde yapılmış bir tanımdır. Oysaki teknik ve idari tedbirlerin alınması veri güvenliğine ilişkin yükümlülüklerin sadece bir kısmıdır.[137]

Veri güvenliğinin sağlanması yükümlülüğü, mutlak bir sonucu gerekli kılmaz. Sonuca bağlı bir sorumluluk hali düzenlememiştir. Kanun'da düzenlenen yükümlülük; güvenliğin sağlanmasındaki süreçte aranan özen düzeyinin gösterilmesini ve gerekli önlemlerin alınmasını hedeflediğinden, veri sorumlusunun söz konusu olabilecek her türlü saldırıyı bertaraf etme yükü altında olmadığı görülür.[138] Bu açıdan veri sorumlu, üzerine düşen görevleri yaptıktan sonra sorumlu olmayacaktır.

Veri işleme güvenliği, GDPR m. 32'de düzenlenmiştir. İlgili maddede ne gibi teknik ve idari önlemlerin alınacağı sayılmış ve Resital 83'te yer alan "Güvenliğin sağlanması ve bu Tüzük'ü ihlal edecek şekilde işleme faaliyetinin gerçekleştirilmesinin önlenmesi amacıyla, veri sorumlusu veya veri işleyen, işleme faaliyetinin doğasında bulunan riskleri değerlendirmeli ve şifreleme gibi bu riskleri azaltmaya yönelik tedbirler uygulamalıdır. Bu tedbirler, riskler ve korunacak kişisel verilerin niteliği ile ilgili olarak teknolojinin durumu ve uygulama maliyetleri dikkate alınarak, gizlilik de dâhil olmak üzere uygun bir güvenlik düzeyi sağlamalıdır. Veri güvenliği riskini değerlendirirken, özellikle fiziksel, maddi veya maddi olmayan hasara yol açabilecek, iletilen, saklanan veya başka bir şekilde işlenen kişisel verilerin kazara veya yasadışı imhası, kaybı, değiştirilmesi, yetkisiz ifşası veya bunlara erişim gibi kişisel veri işlemenin sunduğu riskler göz önünde bulundurulmalıdır" ifadeleri ile detaylandırılmış ve açıklanmıştır.[139]

KVKK'da ise GDPR'ın aksine oldukça genel bir düzenleme söz konusudur ve teknik ve idari önlemlerin ne olduğu belirtilmemiştir. Bir görüşe göre bu durumu bir eksiklik olarak değil, KVKK'nın genel bir kanun olması durumunun sonucu olarak

[136]KVKK**, Temel Kavramlar**, s. 12.
[137]Öztekin, s. 32.
[138]Kapancı, Kadir Berk, **Gelişen Teknolojiler Ve Hukuk Iv : Siber Güvenlik,** *Siber Güvenlik Ve Özel Hukuk Sorumluluğu Üzerine Değerlendirmeler,* On İki Levha Yayıncılık, 2023, s. 69.
[139]*Bkz*. https://gdpr-info.eu/recitals/no-83/#:~:text=In%20order%20to%20maintain%20security,those%20risks%2C%20such%20as%20encryption. (E.T.:20.03.2024).

yorumlamıştır.[140] Nitekim Kurum, GDPR'ın aksine oldukça geniş olan bu düzenlemeye yönelik Kişisel Veri Güvenliği Rehber'ini[141] yayınlamıştır ve bu yayım ile veri güvenliğinin sağlanması için alınabilecek teknik ve idari tedbirlerden bahsetmiştir. Rehber, "kişisel verilerin hukuka aykırı olarak işlenmesi ile kişisel verilere hukuka aykırı olarak erişilmesinin önüne geçilerek kişisel verilerin muhafazasının sağlanması ve bireylerin temel hak ve özgürlüklerinin korunmasının temini için veri sorumlularına yol göstermesi amacıyla" ifadeleriyle hazırlanmıştır.[142]

Özel nitelikli kişisel verilerin işlendiği durumlarda veri sorumlusunun alması gereken tedbirler ise Kurul'un 31/01/2018 tarihli ve 2018/10 sayılı kararında ifade edilmiştir.[143] KVKK m. 6/4'te yer alan "Özel nitelikli kişisel verilerin işlenmesinde, ayrıca Kurul tarafından belirlenen yeterli önlemlerin alınması şarttır," hükmü uyarınca Kurul, ilgili önlemleri bu karar çerçevesinde belirlemiştir.

Veri güvenliğine ilişkin ilkeler uygulanırken somut durum kendi içinde değerlendirilmelidir.[144] Bir veri sorumlusunun alması beklenen önlemler ile bir başka veri sorumlusunun alması gereken önlemler aynı olmayabilir. İşlenilen verinin türü, veri sorumlusunun idari ve teknik yapısı gibi faktörler, alınması beklenen önlemleri elbette ki etkileyecektir.

2.1.1. Veri Güvenliği

Yukarıda da ifade edildiği üzere, veri, belirli şartları taşıyan bir tür bilgidir.[145] Bu nedenle bilgi güvenliği kapsamında incelenen hususlar esasınsa kişisel verilerin güvenliği başlığında da incelenmelidir. Kişisel verilerin güvenliği de bilgi güvenliğine

[140]Serdar Çelikel, **Kişisel Verilerin Korunması Hukuku Kapsamında Veri Sorumlusu Ve Veri Sorumlusunun Yükümlülükleri**, Doktora Tezi, Ankara Üniversitesi, Ankara, 2021, s. 124.
[141]Kişisel Verileri Koruma Kurumu (KVKK), **"Kişisel Veri Güvenliği Rehberi (Teknik ve İdari Tedbirler)"**, (Çevrimiçi), https://www.kvkk.gov.tr/SharedFolderServer/CMSFiles/7512d0d4-f345-41cb-bc5b-8d5cf125e3a1.pdf (E.T.:01.03.2024) ["**KVKK, Rehber"].**
[142]KVKK, **Rehber**, s. 3.
[143]Kişisel Verileri Koruma Kurulu, 31/01/2018 Tarih, 2018/10 Sayılı Kararı. *Bkz*. https://www.kvkk.gov.tr/Icerik/4110/2018-10 (E.T.: 01.03.2024).
[144]Küzeci, s. 264.
[145]*Bkz*. KVKK m. 3/1-d.

ilişkin temellerle ilişkilidir.[146] Bir başka ifadeyle kişisel verilerin güvenliğinin tam olarak sağlanması için bilgi güvenliğine ilişkin tedbirler de dikkate alınmalıdır.[147]

2.1.2. Bilgi Güvenliği

Bilgi güvenliği, geniş bir tanımla bilgiyi her türlü tehditten korumak olarak ifade edilebilir[148] ve üç temelden oluşmaktadır. Bunlar; gizlilik, bütünlük ve erişilebilirliktir.[149,150] Bilgi güvenliği ile korunması amaçlanan değerler bunlardır.[151] Bunun dışında sorumluluk, erişim denetimi, güvenilirlik ve emniyet etkenleri de bilgi güvenliğini destekleyen unsurlar olarak ifade edilmiştir.[152]

Gizlilik, kısaca bilginin yetkisi ve erişim izni olmayan kişilerden saklanması olarak tanımlanabilir.[153] Özellikle günümüzün ilerlemekte olan teknolojisiyle beraber saldırganların yetkileri olmayan bilgilere erişebilecekleri birçok yol mevcuttur. Bu nedenle gizlilik ilkesinin sağlanması oldukça mühimdir. Bu ilke, erişimin ve kullanımın sınırlandırılması ve bilginin üçüncü kişiler bakımından kullanışsız hale getirilmesi gibi yollarla korunur, ayrıca gizlilik ilkesinin sağlanması için şifreleme algoritmaları da kullanılır.[154]

Bütünlük ise bilginin değiştirilmemesi ya da bozulmaması anlamına gelir. Buna göre bilgi göndericiden çıktıktan sonra tamam bir şekilde alıcısına ulaşmalıdır.[155]

---

[146]Öztekin, s. 33.
[147]Melisa Geko ve Simon Tjoa, **An Ontology Capturing the Interdependence of the General Data Protection Regulation (GDPR) and Information Security**, The Central European Cybersecurity Conference, No: 19, 2018, s. 2.
[148]Öztekin, s. 33.
[149]Öztekin, s. 34; Türkay Henkoğlu, **Kişisel Verileriniz Ne Kadar Güvende? Bilgi Güvenliği Kapsamında Bir Değerlendirme**, Arşiv Dünyası Dergisi, Sayı 18-19, 2017, s. 49; Mehmet Tekerek, **Bilgi Güvenliği Yönetimi**, KSÜ Fen ve Mühendislik Dergisi, Cilt 1 Sayı 11, 2008, s. 132; Canberk, Sağıroğlu, s. 170
[150]Jeff Koseff, **Defining Cybersecurity Law**, Iowa Law Review, Cilt 103, Sayı 985, 2018, s. 985; Thomas J. Smedinghoff, **The State of Information Security Law: A Focus on the Key Legal Trends**, Locke Lord LLP; Locke Lord LLP, 2008, s. 2.
[151]Henkoğlu, s. 49.
[152]Canberk, Sağıroğlu, s. 170; Tekerek, s. 133-134.
[153]Tekerek, s. 134; Canberk, Sağıroğlu, s. 170.
[154]Tekerek, s. 133**;** Öztekin, s. 33.
[155]Tekerek, s. 133; Öztekin, s. 33; Canberk, Sağıroğlu, s. 170.

Erişilebilirlik ise bilişim sistemlerini, kurum içinden veya dışından gelebilecek ve erişilebilirliği sınırlayabilecek veya tamamen engelleyebilecek tehditlere karşı koruma sağlamayı hedefleyen bir ilkedir. Bu ilke uyarınca erişim yetkisi olan kişiler bilgiye zamanında ulaşabilir.[156]

Bilgi güvenliğinin sağlanması çeşitli yollarla gerçekleşir. Öncelikle korunacak kritik bilgilerin tanımlanması ve tespiti gerekir. Sonrasında olası tehditler belirlenmeli, bu tehditlerin defedilmesi için uygun metotlar uygulanmalıdır. Bilgi güvenliğinin sağlanması için makul teknik ve idari tedbirler alınmalı, bu tedbirlerin güncel ve yeterli kaldığından emin olunmalıdır.[157] Bilgi güvenliğinin temelini oluşturan bu üç ilke ve sağlamayı hedefledikleri amaçları veri güvenliği ilkeleriyle ve korumak istenen değerlerle örtüşmektedir. Ayrıca bilgi güvenliğinin sağlanmasına yönelik uygulanacak eylemler, veri güvenliğinin sağlanması için uygulanacak eylemlerle paralel bir görünümdedir.[158]

2.2. Veri Sorumlusunun Veri Güvenliğine İlişkin Sorumluluğunun Hukuki Kaynakları

Uluslararası düzeyde kişisel verilerin korunması ilk olarak 1948 tarihli İnsan Hakları Evrensel Beyannamesi ve 1950 yılında imzalanan Avrupa İnsan Hakları Sözleşmesi (AİHS) ile başlamıştır.[159] Avrupa Konseyi, 1970'lı yıllar itibariyle kişisel verilerin korunması için birçok çalışma yapmıştır.[160]

Daha sonra Avrupa Konseyi tarafından 1981 tarihinde kişisel verilerin korunması konusundaki ilk geniş kapsamlı sözleşme olan 108 sayılı "Kişisel Verilerin Otomatik İşleme Tabi Tutulması Karşısında Bireylerin Korunması Sözleşmesi" imzalanmış ve söz konusu sözleşmeyi imzalayan ülkeler tarafından iç hukuka aktarılması yükümlülüğü getirilmiştir. Türkiye, 28 Ocak 1981 tarihinde bu sözleşmeyi

[156]Tekerek**,** s. 133.
[157]Henkoğlu**,** s. 48-50; Tekerek, s. 135-136; Canberk, Sağıroğlu, s. 170-172; Öztekin, s. 34-35.
[158]Öztekin, s. 133-134.
[159]Gültekin, N. M., (2012) **Kişisel Verilerin Ceza Hukuku Yönünden Korunması,** Galatasaray Üniversitesi Kamu Hukuku A.B.D., Yüksek Lisans Tezi, s. 22.
[160]Kişisel Verilerin Korunması Kurumu, Kişisel Verilerin Korunması Alanında Uluslararası ve Ulusal Düzenlemeler, KVKK Yayınları, Ankara 2018, s. 4. **["KVKK, Düzenlemeler"].**

imzalayan ilk ülkelerdendir, ancak iç hukuka dâhil edilmesi 17 Mart 2016 tarihli ve 29656 sayılı Resmi Gazete'de yayımlanması ile gerçekleşmiştir.

108 Sayılı Sözleşme, üye ülkelerdeki uyruğu veya ikametgâhı fark etmeksizin gerçek kişilerin temel hak ve özgürlüklerini ve kişisel verilerini korumayı amaçlar ve özel yaşam haklarını koruma altına alır.[161] Veri güvenliği ise 108 Sayılı Sözleşme'nin 7. maddesinde yer bulmuştur. İlgili maddede veri güvenliği hususu "otomatik dosyalara kaydedilen kişisel verileri korumak için, bunların sonucu veya izinsiz olarak imhasına veya kaza sonucu kaybolmasına veya bunların izinsiz olarak elde edilmesine, değiştirilmesine veya dağıtılmasına uygun güvenlik önlemleri alınır" şeklinde ifade edilmiştir.[162]

1990'lı yıllarda başlayan AB'nin kişisel verilerin korunması hukukuna yönelik çabaları sonucu "Avrupa Parlamentosu ve Avrupa Konseyi Kişisel Verilerin İşlenmesi ve Serbest Dolaşımı Bakımından Bireylerin Korunmasına İlişkin Direktif" 1998 yılında yürürlüğe girmiştir. Söz konusu direktifi kişisel verilerin korunması konusundaki en büyük gelişme olarak nitelemek mümkündür çünkü ilk defa kişisel verilerin korunması konusunda Avrupa Birliği'ne üye tüm ülkelerde geçerli olacak temel esaslar belirlenmiş ve AB veri koruma standartlarına sahip olmayan ülkelere veri aktarımı yasaklanmıştır.[163,164]

Direktif ile gerçek kişilerin verilerinin korunması temel bir insan hakkı olarak kabul edilmiş ve veri işleme şartları, yanlış verilerin düzeltilmesi hakkı, hukuka aykırı veri işlemelerine karşı başvuru hakkı, hassas verilerin istisnai durumlarda işlenmesi gibi temel hak ve ilkelere yer verilmiştir.[165]

Üye devletlerin, Direktif'in "17. maddesinde işlem güvenliğini "kazayla ya da hukuka aykırı bir şekilde verilerin imhasına, kaza sonucu kaybolmasına, değiştirilmesine, yetkisiz bir biçimde açıklanmasına veya erişimine ve diğer tüm

[161]KVKK, **Düzenlemeler**, s. 4.
[162]Bkz. https://inhak.adalet.gov.tr/Resimler/Dokuman/2712020140848108_tur.pdf (E.T.:17.03.2024).
[163]Korkmaz, İ., (2016), **Kişisel Verilerin Korunması Kanunu Hakkında Bir Değerlendirme,** TBB Dergisi, vol. 124, s. 83-84, s. 94-95.
[164]Korkmaz, İ., (2017), **Kişisel Verilerin Ceza Hukuku Kapsamında Korunması,** s. 74, Seçkin Yayınları.
[165]Küzeci, s. 186.

hukuka aykırı işleme biçimlerine karşı uygun teknik ve idari tedbirleri temin etmesini düzenlemektedir. Şeklinde ifade etmektedir."[166] Madde uyarınca; veri sorumlusunun uygun teknik ve idari tedbirleri alması ve bunu yaparken Direktif'e göre uygulama maliyetleri günün teknolojisi ve olası riskleri değerlendirmesi gerekmektedir. Ayrıca veri sorumlusunun veri işleyenin de sayılan tedbirlere uymasını sağlama ve veri işleyen ile aralarında bir sözleşme akdetme yükümlülüğü bulunur.

Direktif'in bazı üye devletlerine kendi ulusal düzenlemelerini bu doğrultuda düzenlemelerinde aracılık ettiği söylenebilir.[167] Ancak bu sefer Avrupa Birliği'ne üye ülkeler arasındaki yeknesaklığın sağlanması ihtiyacı doğmuştur. Bu nedenle, hukuki hedefleri ortaya koyarak bu hedefe ulaşmada kullanılacak araçların seçimini üye ülkelere bırakan "direktif" yerine, herhangi bir iç hukuk düzenlemesi gerektirmeden üye ülkelere doğrudan uygulanabilen "Tüzük" tercih edilmiş[168] ve Direktif, çağın ihtiyaçlarının değişmesi sebebi ile uygulamadaki farklılaşmaya çare olmakta yetersiz kalmaya başlayınca Avrupa Parlemantosu'nda 2016 yılında belki de son yirmi beş yılın en kapsamlı kişisel verilerin korunması düzenlemesi olan GDPR'ı kabul edilmiştir. GDPR, Direktif'in aksine üye devletlerde doğrudan uygulanabilmektedir.[169,170] Ayrıca GDPR'da veri güvenliğine dair daha detaylı, somutlaştırılmış düzenlemeler bulunmaktadır ve GDPR Avrupa Birliği'ndeki tüm bireylerin kişisel verilerini korumaktadır.

GDPR'ın dördüncü bölümünün ikinci kısmında kişisel veri güvenliği ile ilgili maddeler yer almaktadır. Madde 32, 33 ve 34 kapsamında işleme güvenliği ve veri ihlal bildirimi ele alınmıştır. İşleme güvenliği güvenliğini sağlamak adına veri sorumlusunun ve veri işleyenin uygun teknik ve idari güvenlik tedbirlerini alması zorunludur. Buradaki yaklaşımda görülebilir ki veri güvenliğinden veri sorumlusunu sorumlu kılan Direktif'in aksine, veri işleyenin de sorumluluğu söz konusudur.[171]

---

[166]Öztekin, s. 34.
[167]Öztekin, s. 39.
[168]Akıncı, s. 14.
[169]Öztekin, s. 40.
[170]British Legal Technology Forum, **The Main Differences Between The DPD And The GDPR And How To Address Those Moving Forward,** London UK, 2017, s. 1. *Bkz.* https://britishlegalitforum.com/wp-content/uploads/2017/02/GDPR-Whitepaper-British-Legal-Technology-Forum-2017-Sponsor.pdf (E.T.:17.03.2024).
[171]British Legal Forum, s. 1 vd.; Öztekin, s. 41.

GDPR m. 32/2'de "Uygun güvenlik seviyesi değerlendirilirken, iletilen, depolanan veya işlenen kişisel verilerin kazara veya hukuka aykırı olarak yok edilmesi, kaybı, değiştirilmesi, izinsiz şekilde açıklanması veya bunlara erişim başta olmak üzere, özellikle işlemenin yol açtığı riskler göz önünde bulundurulur." ifadesi yer almaktadır. Buradaki yaklaşım, veri sorumlusunun olası riskleri tespit edip önlemeye çalışması yönündedir, yani risk temellidir. Burada veri sorumlusu, veri işleyen, üçüncü kişi veya bu kişilerin çalışanları bakımından ortaya çıkabilecek riskler gözetilmelidir.[172]

GDPR, KVKK'dan farklı olarak alınabilecek teknik ve idari tedbirlerden bazılarını düzenleyerek somutlaştırmıştır. Bu tedbirler; kimliksizleştirme, şifreleme, işleme, hizmet ve sistemlerinin gizliliği, bütünlüğü, erişilebilirliği, dirençliliği, fiziki ya da teknik bir olay halinde erişilebilirlik, uygulanan tedbirlerin düzenli şekilde değerlendirilmesi olarak ifade edilir. [173]

KVKK m. 12, veri güvenliğine ilişkin yükümlülükleri düzenlemektedir. Bu maddede veri sorumlularına 4 ayrı yükümlülük yüklenmiştir. Bunlar; veri sorumlusunun gerekli teknik ve idari tedbirleri alması, veri sorumlularının denetim yükümlülüğü, kişisel verilerin amaç dışında kullanma veya kişisel verileri başkalarına açıklama yasağı ve veri ihlal bildiriminin yapılmasıdır.

Direktif'in aksine KVKK'da daha geniş bir düzenleme bulunur. Kanunda somutlaştırılmamış hususlar ise sonradan Kurum'un yayımladığı rehberler ile somutlaştırılmaya çalışılmıştır.

2.3. Veri Sorumlusunun Veri Güvenliğine İlişkin Yükümlülükleri

KVKK m. 12'de veri sorumlusunun veri güvenliğine ilişkin dört adet farklı yükümlülüğüne yer verilmiştir. Bunlar; veri sorumlusunun gerekli teknik ve idari tedbirleri alması, veri sorumlusunun kanun hükümlerinin uygulanmasına ilişkin kendi kurum ve kuruluşlarında gerekli denetimleri yapması veya yaptırması, kişisel verilerin

[172]Öztekin, s. 41.
[173]Öztekin, s. 41.

amacı dışında kullanılmaması veya hukuka aykırı başkalarına açıklanmaması ve son olarak veri ihlal bildiriminin yapılması olarak ifade edilir. Kurum, KVKK m. 12'yi yayınladığı Rehber ile ve birtakım kararları ile somutlaştırma yönünde eylemlerde bulunmuştur.

GDPR m. 32'de veri sorumlusu ve veri işleyenin, son teknolojiyi, uygulama maliyetleri ve işleme faaliyetinin mahiyetini, kapsamını, bağlamını ve amaçlarını gerçek kişilerin hakları ve özgürlüklerine yönelik riskleri birlikte değerlendirmek suretiyle, belirlenen riske uygun bir güvenlik seviyesi sağlanmak üzere teknik ve idari tedbirler alması gerektiği belirtilmek suretiyle düzenlenmiştir.[174] İlgili maddenin 1. fıkrasının devamında ne gibi teknik ve idari önlemler alınabileceği"(a) kişisel verilerde takma ad kullanımı ve şifreleme; (b) işleme sistemlerinin ve hizmetlerinin gizliliğini, bütünlüğünü, kullanılabilirliğini ve mukavemetini sürekli olarak sağlama kabiliyeti; (c) fiziksel veya teknik bir olay durumunda, kişisel verilerin kullanılabilirliğinin ve kişisel verilere erişimin vakitlice yeniden sağlanma kabiliyeti; (d) işlemenin güvenliliğinin sağlanmasına yönelik olarak teknik ve kurumsal tedbirlerin etkililiğinin düzenli olarak sınanmasına, ölçülmesine ve değerlendirilmesine ilişkin süreç."[175] ifadeleriyle detaylandırılmıştır:

GDPR m. 32 ile ilgili bulunan resitallerden bazıları şunlardır: "Gerçek Kişilerin Hak ve Özgürlüklerine Yönelik Riskler" başlıklı Resital 75, "Gerçek Kişilere Yönelik Risklerin Değerlendirilmesi" başlıklı Resital 76, "Risklerin Değerlendirilmesine İlişkin Kılavuz" başlıklı Resital 77, "Uygun Teknik ve Organizasyonel Önlemler" başlıklı Resital 78, "Sorumlulukların Açıkça Paylaştırılması" başlıklı Resital 79 ve "İşleme Risklerinin Değerlendirilmesi ve Azaltılması" başlıklı Resital 83.[176]

Veri güvenliğine ilişkin sorumluluk maddesi, AB'de kişisel verilerin korunması mevzuatına ilişkin en önemli düzenlemelerden olan ve KVKK'nın da temel alındığı Direktif'te m. 23'te düzenlenmiştir. İlgili madde uyarınca veri sorumlusu, kişisel verilerin korunması hukukuna aykırı olan her türlü veri işleme faaliyeti

[174]Develioğlu, s. 107.
[175]https://gdprhub.eu/Article_32_GDPR (E.T.:19.03.2024).
[176]https://gdprhub.eu/Article_32_GDPR (E.T.:19.03.2024).

sonucunda uğranılan tüm zararlardan sorumludur.[177] Direktif'e göre hukuka aykırı veri işleme faaliyetlerinden yalnızca veri sorumlusu sorumluyken, bu durum KVKK'ya ve GDPR'a bu şekilde yansımamıştır; veri güvenliğine ilişkin sorumluluk maddesi ise özel hukuka ilişkindir[178] ve göre veri işleyenin veri sorumlusu ile birlikte veri işleme faaliyetinde bulunması halinde gerekli teknik ve idari tedbirleri alma konusunda müşterek olarak sorumludur.

Tezimizin konusu ile sınırlamak amacıyla, veri güvenliği konusu KVKK'da yer alan haliyle detaylandırılacak, GDPR ile ilgili bölümlerde karşılaştırılarak değerlendirilmesi yapılacaktır.

2.3.1. Hukuka Aykırı İşlemenin Önlenmesi

KVKK m. 12/1-a'da ifade edildiği gibi, teknik ve idari tedbirler vasıtasıyla sağlanacak ilk amaç hukuka aykırı işlenmenin önlenmesidir. Veri işleme faaliyeti yukarıda da anlatıldığı üzere hukuka uygun şekilde gerçekleşebileceği gibi, ilgili şartların sağlanmaması ile hukuka aykırı şekilde de gerçekleşebilir.

Buradaki hukuka uygunluk kavramı oldukça geniştir, ancak veri koruma hukukuna ilişkin mevzuatlarda ve somut olayın tabi olduğu ilgili mevzuatlarda hukuka uygun olarak kabul edilen veri işleme stilleri öngörülmüştür.[179] Diğer taraftan, veri işlemenin sadece kanundaki şartlarla öngörülmüş olması kendi başına hukuka uygun bir işlemeden söz edildiği anlamına gelmeyecektir. Burada veri işlemenin Anayasa'nın temel hak ve özgürlüklere ilişkin koruduğu değerlerle uyuşması da önem arz eder.[180] Kişisel veri işlemenin Anayasa'ya aykırı bir şekilde gerçekleşmesi durumu, işleme ilgili mevzuatlarda öngörülen temel şartlar ve usul çerçevesinde gerçekleşmiş olsa dahi, gerçekten bir kişisel verilerin korunması hakkı sağlamaz ve hukuka uygun olduğu ifade edilemez.[181]

---

[177]Uçak, s. 58.
[178]Öztekin, s. 43.
[179]Dülger, s. 110.
[180]*Bkz*. Doğan Kılınç, "**Anayasal Bir Hak Olarak Kişisel Verilerin Korunması**", Ankara Üniversitesi Hukuk Fakültesi Dergisi, Cilt 61, Sayı 3, 2012, ss. 1089-1172.
[181]Kişisel Verileri Koruma Kurumu, **Kişisel Verilerin İşlenmesine İlişkin Temel İlkeler**, Ankara, 2019, s. 4-5. **["KVKK, Temel İlkeler"].**

Kurul, alınacak tedbirlerle önlenmesi gerekli olan hukuka aykırı işleme faaliyetlerini, veri sorumlusunca gerçekleştirilen işleme faaliyeti olarak yorumlamaktadır.[182] Buna örnek olarak Kurul'un 2021/889 sayılı Karar'ı gösterilebilir. Halı saha işletmeciliği yapan veri sorumlusunun, spor tesislerinde spor yapanların rızası alınmadan görüntü kaydı yapmakta olduğu ilgili olayda, Kurul, "ilgili kişinin kişisel verisi olan görüntüsünün Kanunda yer alan herhangi bir kişisel veri işleme şartına dayanmaksızın veri sorumlusu tarafından işlendiği dikkate alındığından veri sorumlusunun Kanunun 12 nci maddesinin (1) numaralı fıkrasının (a) bendi kapsamında kişisel verilerin hukuka aykırı işlenmesini önlemek amacıyla uygun güvenlik düzeyini temin etmeye yönelik gerekli teknik ve idari tedbirleri almadığı" sonucuna varmıştır ve veri sorumlusu KVKK m. 18/1 uyarınca idari para cezasına çarptırılmıştır.[183] Veri sorumlusu tarafından açık rıza formlarının hazırlandığı iddia edilse de, Kurul bu uygulamanın ilgili kişinin yayımlanan görüntülerinde gerçekleştirilmediğinden bahisle yeni tarihli bir uygulama olduğunun altı çizilmiş ancak her halükarda Kanun'un 5. maddesinin birinci fıkrası kapsamında düzenlenen açık rızanın, rıza veren kişinin "olumlu irade beyanı" nı içermesi gerektiğini vurgulamış; ilgili kişiden rıza alınmaksızın görüntü kaydı alınmasının veri sorumlusu tarafından uygulanacak tedbirlerle önlenmesi gerektiğine işaret etmiştir.

Yine, yerel haber sitesi görevi yapan veri sorumlusunun, ilgili kişinin kişisel verilerinin yer aldığı sınav sonuç belgesini açık rıza almadan paylaştığı bir başka somut olayda Kurul, veri sorumlusunun hukuka aykırı olarak işleme faaliyeti gerçekleştirmesini KVKK m. 12/1'in ihlali olarak yorumlamıştır.[184]

Bir başka kararda ise veri sorumlusu, aralarında araç kiralama sözleşmesi imzaladığı ilgili kişinin sözleşmede belirtilen kredi kartı yerine hiçbir şekilde onayının ve bilgisinin bulunmadığı başka bir kredi kartının bilgilerini kullanmıştır. Bilgisinin bulunmadığı kredi kartı bilgileri, veri sorumlusu ile ilgili kişi arasında daha önce addedilen bir sözleşmede geçtiği ve veri sorumlusunun bu bilgileri hukuka aykırı bir

[182]Öztekin, s. 47.
[183]Kişisel Verileri Koruma Kurulu'nun 03.09.2021 tarihli 2021/889 sayılı kararı. *Bkz*. https://www.kvkk.gov.tr/Icerik/7139/2021-889 (E.T.: 04.03.2024).
[184]Kişisel Verileri Koruma Kurulu'nun 06.01.2022 tarihli ve 2022/13 sayılı kararı. *Bkz*. https://www.kvkk.gov.tr/Icerik/7179/2022-13 (E.T.: 04.03.2024).

şekilde işlediği gözetilmiş ve Kurum burada da KVKK m. 12/1'in ihlaline karar vermiştir.[185]

Alınması gerekli tedbirler ve bu tedbirlerin düzeyi, somut olayın koşullarına, barındırdıkları risk düzeylerine ve elbette işlenen verilerin niteliğine göre değişkenlik gösterecektir; bu noktada tedbirlerin tespiti, düzeyi, güncel gerekliliklere uygun olması, devamlılığı ve bunların denetimi elzemdir.[186]

Bir başka Kurul kararı da veri sorumlusunun, iş başvurusu yapan ve işe alınmayan ilgili kişinin, başvuru sonrası kişisel verilerinin silinmemesini konu almıştır. Buna göre hiçbir işleme şartına dayanmaksızın kişisel verilerin işlenmeye devam etmesini ve imha edilmemesini; KVKK m. 7'ye uygun bulmamış, bu durumu da yine KVKK m. 12/1'in ihlali olarak yorumlamıştır.[187] Belirtilmelidir ki kişisel verilerin silinmemesi, imha edilmemesi veya anonim hale getirilmemesi de kişisel verilerin hukuka aykırı işleniş hallerinden biridir.[188]

Yine benzer bir şekilde, bir insan kaynakları firması olarak görev yapan veri sorumlusunun firmasının ilgili kişinin kişisel verisi niteliğindeki e-posta adresinin ilgili kişiye ticari amaçlı bir e-posta gönderilmesi suretiyle işlendiği ancak KVKK'nın 5'inci maddesinde yer alan işleme şartlarından herhangi birinin söz konusu olmadığı bir somut olayda; Kurul, veri sorumlusunun KVKK m. 12/1 uyarınca yükümlülüklerine aykırı davrandığına hükmetmiştir.[189]

Buradaki değerlendirmenin veri sorumlusunun işlediği verilere karşı üçüncü kişiler tarafından gerçekleştirilebilecek hukuka aykırı işleme faaliyetlerine yönelik yapılması gerektiğinin savunulduğu bir görüşe göre; veri sorumlularının madde 12 kapsamında alacağı tedbirler olası risklere karşı alınacak olan tedbirlerdir ve veri sorumlularının tedbir almış olması durumunda dahi riskler bulunmaktadır ve "teknik

[185]Kişisel Verileri Koruma Kurulu'nun 27/02/2020 tarihli ve 2020/166 sayılı kararı. *Bkz*. https://kvkk.gov.tr/Icerik/6889/2020-166 (E.T.:04.03.2024).
[186] Kapancı, s. 69.
[187]Kişisel Verileri Koruma Kurulu'nun 06.07.2021 tarihli 2021/670 sayılı kararı. *Bkz*. https://www.kvkk.gov.tr/Icerik/7136/2021-670 (E.T.: 05.03.2024).
[188] Öztekin, s. 50.
[189]Kişisel Verileri Koruma Kurulu'nun 09.12.2021 tarihli 2021/1243 sayılı kararı. Bkz. https://www.kvkk.gov.tr/Icerik/7274/2021-1243 (E.T.:06.03.2024).

ve idari tedbirler, veri sorumlusunun tamamen kontrol edemediği risk ve tehditleri bertaraf etme amacıyla alınmaktadır. Bu nedenle de teknik ve idari tedbirlerin alınacağı hususlarda veri sorumlusunun bir sonuç garanti edebilmesi mümkün değildir. Ancak veri sorumlusunun kendi faaliyetleri kapsamında hukuka uygun bir şekilde kişisel veri işlemesi, aydınlatma yükümlülüğünün yerine getirilmesi gibi kontrolü altında olan ve belirli bir sonucu gerçekleştirebileceği bir yükümlülüktür."[190]

Bir başka görüşe göre ise ilgili madde veri sorumlularına KVKK m. 4 ve 9 hükümlerine uygun işleme olup olmadığı yönünde denetleme yükümlülüğü de getirmektedir.[191]

Kanaatimizce, Kurul'un bu değerlendirmesi geniş bir yorumlamaya sebep olmaktadır ve ilgili madde üçüncü kişilerin ihlal durumları bakımından veri sorumlusunun sorumluluğuna ilişkin yorumlanmalıdır. İlgili maddede üçüncü kişilerin risk taşıyan hukuka aykırı işleme faaliyetlerine karşı veri sorumlusunun önleme yükümlülüğünün olması durumuna ilişkin lafzi bir yorumu yapıldığında çıkarılacak olan sonuç açıktır.

Kurul'un veri sorumlusunun hukuka aykırı işleme faaliyetini gerçekleştirmesi eylemini teknik ve idari tedbir alma yükümlülüğünün ihlali kapsamında değerlendiren bir tutumu olduğu görülebilir. Nitekim kararlarda da Kurul ne gibi teknik ve idari tedbirin alınmış olması gerektiğine değinmemiştir.

Buradaki bu yaklaşımlar, Kurul'un hukuka aykırı işleme faaliyetinin gerçekleşmesinin, gerekli teknik ve idari tedbirlerin alınmamış olmasının sonucu olarak değerlendirdiğini gösterir. Buradaki bu yaklaşım geniş bir yorumlamadır ve veri sorumlusunun gerçekleştirdiği her türlü işleme faaliyetinde de KVKK m. 12/1'e göre bir değerlendirme yapmaktır. Esasen Kurul söz konusu olayları hukuka aykırı veri işleme kapsamında değerlendirmelidir. Nitekim ilgili kararlarda KVKK m. 5 uyarınca ihlalin bulunduğu durumlarda Kurul sonraki adım olarak madde 12/1 kapsamında bir sonuca varmıştır. Bu aşamalı değerlendirmenin geniş bir yorumlamaya sebep olduğu ve bunun gün geçtikçe ilgili kararlar ve mevzuatlar ışığında gittikçe netlik kazanan

[190]Öztekin, s. 48-49.
[191]Çekin. s. 149.

kişisel verilerin korunması hukukunda hali hazırda yükümlülükleri oldukça fazla olan veri sorumlusunun işini daha da zorlaştıracağı kanısındayız.

2.3.2. Kişisel Verilere Hukuka Aykırı Olarak Erişilmesinin Önlenmesi

Hukuka aykırı şekilde erişim kısa bir tanımla veri sorumlusunun işlediği verilere erişme yetkisi bulunmayan bir kişinin hukuka aykırı şekilde veya erişim yetkisi bulunan bir kimsenin amacı ya da yetkisi dışında erişimidir. [192] Veri sorumlusu bünyesinde çalışan bir kişinin ilgili kişiye ait uçuş bilgilerine şirket kayıtlarından ulaştığı ve bunu başkasıyla paylaştığı bir olay hakkında Kurul, çalışanın yetkisi dışında kişisel verilere erişimini hukuka aykırı işleme niteliğinde görmüş olup, veri sorumlusu tarafından kişisel verilere erişim ile ilgili sınırlama getirilmemesi ve çalışanlara verilen eğitimin yetersiz olması sebebiyle Kanunun 12 nci maddesinde yer alan veri güvenliğinin sağlanmasına yönelik gerekli idari ve teknik tedbirlerin alınmadığı kanaatiyle Kanunun 18 inci maddesinin birinci fıkrasının (b) bendi çerçevesinde veri sorumlusu hakkında 100.000 TL idari para cezası uygulanmasına karar vermiştir.[193,194]

Söz konusu erişim, fiziki ortamdaki verilere karşı gerçekleşebileceği gibi fiziki olmayan ortamda da bulunmayan verilere erişim de söz konusu olabilir.[195] Uygulamada hukuka aykırı erişim genelde siber saldırı şeklinde görülür. Bu bakımdan bu ilke bilgi güvenliğinin gizlilik ilkesi ile bağlantılıdır.[196]

Veri sorumlularının hukuka aykırı erişimi önleyecek yeterli teknik ve idari tedbiri almadıklarına yönelik birçok Kurul kararı bulunmaktadır. Aynı şekilde veri sorumlularının GDPR'dan kaynaklanan bu yükümlülüğüne yönelik de birçok karar mevcuttur.

[192]Öztekin, s. 51.
[193]Kişisel Verileri Koruma Kurulu'nun 13.02.2020 tarihli 2020/124 sayılı kararı. *Bkz.* (https://www.kvkk.gov.tr/Icerik/6886/2020-124 (E.T.: 05.03.2024).
[194]Amaç ve yetki dışında erişimin hukuka aykırı işleme niteliğinde olması hakkında bir başka karar için *Bkz*. Kişisel Verileri Koruma Kurulu'nun 03.03.2020 tarihli ve 2020/191,192,193,194 sayılı kararları *Bkz*. https://www.kvkk.gov.tr/Icerik/6762/2020-191-192-193-194 (E.T.:06.03.2024).
[195]Çekin, s. 50-51.
[196]Öztekin, s. 51.

Örneğin; 17/03/2022 tarihli ve 2022/243 sayılı Karar uyarınca, ilgili kişiyle aynı isme sahip bir kişinin faturasının ilgili kişinin e-posta adresine gönderildiği ve bu konuya ilişkin bir onaylama metodu kullanılmadığı somut olayda, Kurul, veri sorumlusunun KVKK m. 5 ve KVKK m. 12/1-b uyarınca gerekli yükümlülüklerini gerçekleştirmediğine hükmetmiştir.[197] Kurul, iletişim kanalı doğrulama tedbirlerinin yalnızca e-ticaret sitesi üyeleri nezdinde sınırlı olarak alınmasının yeterli olmadığı, üye olmayı tercih etmeyen kullanıcılara da iletişim kanalı doğrulama tedbirlerinin uygulanmasının gerekli olduğuna işaret ederek isabetli bir karar vermiştir. Somut olaydan anlaşıldığı üzere üye olmadan alışveriş yapmak isteyen tüketicilere "misafir girişi" veya "üye olmadan devam et" seçeneklerini e-ticaret firması sunmaktadır ve üyelik aşamasında talep edilen diğer verilerini paylaşmak istemeyen kişiler nezdinde alınan tedbirlerinin hafifletilmesinin isabetli olmadığı görüşündeyiz. Gerçekten de Kurul, ilgili kişinin iletişim bilgilerini doğrulamayan veri sorumlusu hakkında idari para cezası uygulanmasına karar vermiştir.

Bir başka olayda ise veri sorumlusunun eski çalışanı olan ilgili kişi, iki farklı tarihte veri sorumlusu hastane çalışanı hekimin sekreteri tarafından izni dışında sağlık verilerine erişildiğini fark etmiş ve bunun üzerine Kurul'a başvurmuştur. Erişim yetkisi olmamasına rağmen sekreter, e-nabız sistemine giriş yetkisi olan doktorun yerine ilgili kişinin e-nabız sistemine girerek sağlık verilerine ulaşmaktadır. Somut olayda doktorun, hastalarının kişisel veri güvenliğine ilişkin makul teknik ve idari tedbirleri almadığı görülmektedir. Kurul da, veri sorumlusu bünyesinde çalışan bir kişinin yetkisi olmadan ilgili kişinin özel nitelikli bilgilerine eriştiğini tespit etmiş ve KVKK m. 12/1-b uyarınca veri sorumlusunun yükümlülüklerini yerine getirmediğinden bahisle idari para cezasına ve veri sorumlusunun Kanunun 13 üncü maddesi kapsamındaki yükümlülüğünü yerine getirmek üzere kendisine iletilen başvuruları yanıtlaması hususunda gerekli dikkat ve özen göstermesi hususunda talimatlandırılmasına karar vermiştir.[198]

[197]Kişisel Verileri Koruma Kurulu'nun 17.03.2022 tarihli 2022/243 sayılı kararı. *Bkz*. https://www.kvkk.gov.tr/Icerik/7297/2022-243 (E.T.:06.03.2024).

[198]Kişisel Verileri Koruma Kurulu'nun 21.09.2021 tarihli 2021/962 sayılı kararı. *Bkz*. https://kvkk.gov.tr/Icerik/7074/-Ilgili-kisinin-talebi-ya-da-rizasi-olmaksizin-ozel-bir-hastane-calisani-hekim-tarafindan-e-nabiz-sistemine-erisim-saglanmasi-hakkinda-Kisisel-Verileri-Koruma-Kurulunun-21-09-2021-tarihli-ve-2021-962-sayili-Karari (E.T.: 06.03.2024).

Uygulamada oldukça yaygın olduğu şekilde Kurul kararına konu olayda da, sekreter vasıflı hastane çalışanının tıpkı yetkisi varmış gibi hastalara ait çoğu özel nitelikli olan kişisel veriye erişebildiği ancak doktorların aksine mesleki sır saklama yükümlülüğü bulunmadığı bilinmektedir. Bu halde veri sorumlusu ile veriye erişimi olan kişiler arasında bir gizlilik sözleşmesi yapılarak ilgili kişilerin kişisel verilerin korunması adına tarafların yükümlülük ve sorumluluklarını belirlenmesinde yarar vardır.

İspanyol Veri Koruma Otoritesi'nin GDPR m. 32 uyarınca aldığı bir karar uyarınca, ilgili kişi veri sorumlusu olan bankasının çevrimiçi bankacılık hesabına giriş yaptığında bir başka kişinin bankacılık bilgilerini görüntüleyebildiğini görüp şikayette bulunmuştur. İspanyol Veri Koruma Otoritesi, veri sorumlusunun veri gizliliğini korumak için gereken teknik ve idari önlemi almadığından bahisle idari para cezasına hükmetmiştir.[199]

2.3.3. Kişisel Verilerin Muhafazasını Sağlamak

Bu fıkrada geçen muhafaza kavramı muğlak bir kavramdır. Bir düşünceye göre buradaki anlamın, kasıt bulunmadan kişisel verilerin kaybolmasına yahut yok olması gibi durumlara ilişkin olarak teknik ve idari tedbirlerin alınmasını gerekli olması olarak yorumlar, bu durumda kişisel verilerin muhafazası için birtakım mücbir sebepler risk oluşturmaktadır.[200] Kanaatimizce buradaki yaklaşım makuldür. Kişisel verilerin üçüncü kişilerce veya yetkisini ya da amacını aşan kişilerce muhafazasının riske girmesi, işin içine bir kasıt dâhil olması, kişisel verilerin hukuka aykırı erişimini önlemek fıkrası kapsamına girmektedir. Bu durumda bu fıkranın içinde kasıt bulunmayan hallerde verilerin tahribini konu alması doğru bir yorumlama olacaktır.

Bu durumların dışında Kurul, hukuka aykırı işleme ya da hukuka aykırı erişim benzeri bir durum olmaksızın kişisel verilerin erişilebilir hale gelmesini de kişisel verilerin muhafazasının sağlanmayışı kapsamında değerlendirmektedir. Veri sorumlusunun müşterilerine verdiği takip numaralarının son hanelerinin karışması ile

[199]AEPD Spain) - EXP202104875, GDPRhub. https://gdprhub.eu/index.php?title=AEPD_(Spain)_-_EXP202104875&oldid=37983 (E.T.:19.04.2024).
[200]Çekin, s. 148-149.

müşterilerin birbirinin kişisel verilerine erişebildiği bir olayda Kurul, veri sorumlusunun kişisel verilerin muhafazasını sağlamak için yeterli teknik ve idari tedbir almadığına kanaat etmiş, daha önce tebliğ edilen "linklerin kullanımının derhal durdurulması" şeklindeki talimatın veri sorumlusu tarafından Kurul Kararına uygun olarak yerine getirilmediği dikkate alınarak Kanunun 18 inci maddesi çerçevesinde 50.000 TL idari para cezası uygulanmasına ve asıl güvenlik açığının giderilmediği sistemin değiştirilmesi, diğer taraftan halihazırda sorgulama yapılan sisteme erişimin ivedilikle kapatılması hususunda veri sorumlusunun talimatlandırılmasına karar vermiştir.[201]

Özetle, verilerin herhangi bir hukuka aykırı erişim veya işlemenin söz konusu olmadığı hallerde, erişime yetkili olmayan kişilerce erişime açık hale gelmesi; veri sorumlusunun kişisel verilerin muhafazasını sağlamak için yeterli teknik ve idari tedbir almadığı yönünde bir değerlendirmeye sebep olabilmektedir.[202]

2.3.4. Teknik ve İdari Tedbir Alma Yükümlülüğü

KVKK m. 12'de veri sorumlusunun teknik ve idari tedbirleri alma yükümlülüğü detaylandırılmamış, GDPR'da m. 32'de ise teknik ve idari tedbirlerin ne olacağına detaylıca yer verilmiştir.

KVKK'nın 95/46/EC Sayılı Direktif doğrultusunda hazırlanmış olan 2008 tasarısında ise "Kişisel verilerin, tedbirsizlikle veya hukuka aykırı amaçlarla yok edilmesini, kaybolmasını, değiştirilmesini, yetkisiz olarak açıklanmasını veya aktarılmasını ve başka şekillerdeki tüm hukuka aykırı işlenmelerini korunacak verinin niteliği, teknolojik imkânlar ve uygulama maliyetine göre uygun teknik ve idarî tedbirleri almak zorundadır" şeklinde bir ibareye yer verilmiştir.[203] Buradan da görüldüğü üzere veri sorumlusunun teknik ve idari tedbir alma yükümlülüğünün 2008 tasarısında yer alan hali, bilgi güvenliği ile paralel bir düzenleme şekli olup, KVKK

[201]Kişisel Verileri Koruma Kurulu'nun 14.02.2019 tarihli 2019/23 sayılı kararı. *Bkz.* https://www.kvkk.gov.tr/Icerik/5464/2019/52 (E.T.: 06.03.2024).
[202]Öztekin, s. 53.
[203]*Bkz.* https://www.bilgiedinmehakki.org/blog/2008/06/18/kisisel-verilerin-korunmasi-kanunu-tasarisi-2008/ (E.T.:18.03.2024). 2008 KVKK Tasarısı ile şimdiki Kanun'un değerlendirmesi için *Bkz.* İbrahim Korkmaz, "Kişisel Verilerin Korunması Kanunu Hakkında Bir Değerlendirme", Türkiye Barolar Birliği Dergisi, Sayı 124, Mayıs-Haziran 2016, ss. 81-152.

m. 12'den farklılıklar içermektedir. Bilgi güvenliğini oluşturan üç amaç 2008 tasarısında kendini göstermiştir. Gizlilik ilkesi kişisel verilerin yetkisiz açıklanmasının ve aktarılmasının önlenmesi şeklinde, bütünlük ilkesi kişisel verilerin değiştirilip yok edilmesinin önlenmesi şeklinde ve erişilebilirlik ilkesi kişisel verilerin kaybolmasının önlenmesi şeklinde yer bulmuştur. [204]

Veri güvenliğini sağlamak için alınan teknik ve idari tedbirler değişmez ve kesin bir sonuca yönelik değildir. Günden güne gelişen teknoloji ile böyle bir sonucu garantilemenin mümkün olmadığı görülebilir. Burada aslolan veri sorumlusunun kişinin temel hak ve özgürlükleri için gerekli değerlendirmeyi yapıp, buna uygun ve makul bir tedbiri almasıdır.[205]

Aksi halde; ilgili kişilerin gerekli önlemlerin tam ve eksiksiz alınmaması sebebiyle zarara uğraması halinde, zararın giderilmesinin KVKK m. 11 ve 14 yönlendirmesi ile Türk Medeni ve Borçlar Kanunu genel hükümlerine göre talep edilebileceği görülürken; GDPR m.82'de doğrudan doğruya özel bir kusursuz sorumluluk düzenlemesi olduğu görülür.[206]

GDPR'da "uygun teknik ve idari tedbirler" ibaresi doksandan fazla kez yer almaktadır. Bu durum bile teknik ve idari önlem almanın önemini gözler önüne seren bir olgudur. GDPR, her aşamada güvenliğe ve yeterli teknik ve idari önlemlere atıfta bulunulması, veri güvenliğinin GDPR'ın merkezi bir parçası olduğuna dair açık bir gösterge oluşturmaktadır.[207] GDPR Resital 78'de de "Yönetmeliğin gerekliliklerinin yerine getirilmesini sağlamak için uygun teknik ve organizasyonel önlemler alınmalıdır. Bu tür önlemler, diğerlerinin yanı sıra, kişisel verilerin işlenmesini en aza indirgemek, kişisel verilerin mümkün olan en kısa sürede takma adını vermek, kişisel verilerin işlevleri ve işlenmesi konusunda şeffaflık, veri işlemeye tabi verilerin izlenmesini sağlamak, denetleyicinin güvenlik özellikleri oluşturmasını ve geliştirmesini sağlamaktan oluşabilir." şeklinde ifade edilmiştir.

[204]Öztekin, s. 44.
[205]Çekin, s. 145**;** Zor, s. 92.
[206]Kapancı, s. 69 vd.
[207]Burton, **Article 33. Notification of a Personal Data Breach to the Supervisory Authority** in Kuner, Bygrave & Docksey (eds.), The EU General Data Protection Regulation (GDPR): A Commentary, Oxford University Press (2020), s. 637.

GDPR m. 32'nin öngördüğü olası teknik ve idari tedbirlerin; erişim kontrolü, bütünlük, takma ad, şifreleme, iletim kontrolü, gizlilik, kurtarılabilirlik ve değerlendirme olduğu bilinmektedir.

GDPR m. 32 uygulanan güvenlik önlemlerinin ortaya çıkan riske "uygun" olması gerektiğini öngörür. GDPR'da yer alan "uygunluk" ifadesi, AB hukukunun genel ilkelerinden biri olan orantılılık ilkesi ile ilişkilendirilebilir.[208] Orantılılık ilkesi, bir eylemin varılmak istenen amaç ile orantılı olması gerektiği yönündeki yasal ilke olarak tanımlanabilir. Bu temel ilkenin keskin tanımını yapmak zordur, ancak çeşitli kaynaklarda, "adaletin sağlanmasının temel koşulu" ve AB hukukunun "temel taşı" olarak tanımlanmıştır.[209] Orantılılık yaklaşımı, genel olarak bir amaca ulaşmak için kullanılan araçlar ile amacın dengesini değerlendirir.[210,211] Herhangi bir işleme operasyonunda hangi güvenlik önlemlerinin uygun kabul edileceğinin belirlenmesi, veri sorumlusu veya işleyici açısından kapsamlı bir analiz gerektirir; veri sorumluları ve işleyiciler duruma özgü riskleri tanımlamalı, işleme faaliyetinin özel koşullarını göz önünde bulundurarak potansiyel etkilerini değerlendirmeli ve gerçekleşme olasılığı yüksek ve etkisi şiddetli olacak riskleri azaltmak için en efektif tedbirleri uygulamalıdır.[212]

2.3.4.1. Kişisel Veri Güveliğine İlişkin İdari Tedbirler

Kişisel verilerin güvenliğinin sağlanabilmesi için veri sorumlusu ve veri işleyenler tarafından teknik ve idari birtakım tedbirler alınmalıdır. KVKK m. 12/1'de ver sorumlusunun; kişisel verilerin işlenmesinde, erişilmesinde ve muhafazasında hukuka uygunluğu sağlamak amacıyla uygun güvenlik düzeyini sağlaması gerektiğine, bunun için de her türlü teknik ve idari tedbirleri almak zorunda olduğuna işaret edilmiştir. Kanun'un bu tedbirlerden hiçbirini sıralamadığı gibi ve bu hususta herhangi

[208]Christopher Kuner, Lee A Bygrave, Christopher Docksey, Laura Drechsler, **The EU General Data Protection Regulation (GDPR): A Commentary, "GDPR Article 32" section**, Oxford University Press, 2020, s. 635 vd.
[209]Aurelien Portuese, **Principle of Proportionality as Principle of Economic Efficiency**, European Law Journal, Cilt 19, Sayı 5, 2013, s. 612.
[210]Kuner, Bygrave vd., s. 635.
[211]Konu hakkında detaylı inceleme için *Bkz*. Jan Burda, T**he Principle of Proportionality in EU Law**, Yüksek Lisans Tezi, Masaryk Üniversitesi, 2018-2019.
[212]Burton, s. 635.

bir açıklamada bulunmadığı görülmektedir[213] ancak bunun bir noksanlık olmadığı görüşündeyiz. Çağın gerekliliklerin her geçen gün hızla farklılaşmakta olduğundan ve her yeni gelişmede kanun değişikliğine gidilmesi mümkün olmayacağından[214] tedbirlerin Kanun ile değil Rehber ile açıklanması isabetlidir. Zaten Rehber de, Kanun'un çizdiği sınırların içini doldurmak ve uygulanmasını sağlamak amacıyla Kurum tarafından yayımlanmıştır.

Rehber göz önünde bulundurulduğunda veri sorumlusunun alabileceği idari tedbirlerin; risk analizi, veri işleme politikalarının oluşturulması (kişisel veri işleme envanteri, erişim, bilgi güvenliği, kullanım, saklama ve imha vb. politikalarının hazırlanması), veri işleyenlerle ve veri sorumlularıyla sözleşme yapılması, çalışanlara yönelik eğitim ve farkındalık faaliyetleri, çalışanlara yönelik tedbirler (iş sözleşmeleri, disiplin yönetmeliği, gizlilik taahhütnameleri), Kurum için periyodik ve/veya rastgele denetimler, kurumsal iletişim (Kurul ve ilgili kişiyi bilgilendirme süreçleri, kriz ve itibar yönetimi vb.) ve Veri Sorumluları Sicil Bilgi Sistemine bildirim şeklinde sayıldığı görülebilmektedir.[215]

Rehber, her ne kadar sıralamış olsa da, uygulamada bu tedbirlerin özümsenemediği gözlemlenmiştir. Veri işleme politikalarını oluştursa da politikalarını hayata geçirmediği için veri ihlallerine devam etmekte olan sayısız veri sorumlusu bulunmaktadır ve uygulamadaki bu aksaklık kontrol mekanizmasının yetersiz kalmasından kaynaklanmaktadır. GDPR'ın aksine Kanun'da işleme faaliyetlerinin getirilen düzenlemelere uygun şekilde gösterme bulunmamaktadır.[216]

GDPR m. 24 uyarınca, işleme faaliyetlerinin GDPR uyarınca gerçekleşmesini sağlamak ve bu şekilde gerçekleştiğini "gösterebilmek" için uygun tedbirleri uygular, gözden geçirir ve günceller, politikaların uygulanmasını sağlar, yükümlülüklerine uygunluğu gösterir. GDPR 37 ise bazı hallerde, veri sorumlusu ve veri işleyenlere yükümlülükleri hakkında bilgi vermek, çözüm önerileri ve tavsiyeler sunmak, politika ve prosedürlere uyumluluğu sağlamak, veri koruma kapsamında farkındalık

[213]Emine Hizarcı, **6698 Sayılı Kişisel Verilerin Korunması Kanunun Ab Veri Koruma Hukuku Işığında Değerlendirilmesi**, İstanbul, Yetkin Yayıncılık, 2019, s. 136-137
[214]Çelikel, s. 123, Develioğlu, s. 100;
[215]Zor, s. 93.
[216]Kaya, s. 1892.

faaliyetleri yürütmek, etki değerlendirmesi ve performans ölçümü yapmak üzere "veri koruma görevlileri" atanmasını zorunlu kılmıştır.[217]

GDPR m. 32'de alınabilecek teknik ve idari tedbirler düzenlenmiş ve gerekçesinin 83. maddesinde ayrıntılı olarak açıklanmış olup[218] bunlar; veri işlemeye ilişkin sürekli risk değerlendirmesinin oluşturulması, bilgi güvenliği politikalarının geliştirilmesi, veri işlemeye ilişkin sorumlulukların dâhili tahsisinin oluşturulması, raporlama, durum tespiti, eğitim ve denetim stratejileri ve süreçlerinin geliştirilmesi, politikalara uyum mekanizmalarını takip etmek olabilecektir. [219]

2.3.4.1.1. Mevcut Risk ve Tehditlerin Belirlenmesi

Veri sorumlusunun önce hangi kişisel verileri işlediğini belirlemelidir ve bu verileri korumak için risk analizi yapmalıdır. Buna göre veri sorumlusunun ortaya çıkabilecek riskleri iyi tespit edebilmesi ve buna uygun gereken tedbirleri alması gerekir.

Bu riskler belirlenirken verilerin genel nitelikli mi yoksa özel nitelikli veri mi olduğunu dikkate alınmalıdır. Sonrasında önemi dolayısıyla gereken gizlilik seviyesi tespit edilmeli ve güvenlik ihlali halinde ilgili kişi için ortaya ne tür zararlar çıkabileceği ve bu zararın niceliği belirlenmelidir, buna göre risklerin önceliğinin belirlenmesi de söz konusu olacaktır. Sonrasında bu riskleri defedebilecek alternatif yollar ve çözüm önerileri, maliyet ve yararlılık ilkeleri bakımından değerlendirilmeli ve buna göre gereken teknik ve idari tedbirler ona göre uygulanmalıdır.[220]

2.3.4.1.2. Çalışanların Eğitilmesi ve Farkındalık Çalışmaları

Veri sorumlusu bünyesinde çalışan kişilerin yetkisi dışında ya da amacını aşan şekilde kişisel verilere erişimi de ihlal oluşturur. Kişisel verilerin güvenliği, sadece

[217]Dülger, s. 126.
[218]Dülger, s. 537.
[219]*Bkz*.https://gdpr-info.eu/recitals/no-83/#:~:text=In%20order%20to%20maintain%20security,those%20risks%2C%20such%20as%20encryption. (E.T.:20.03.2024).
[220]Çekin**,** s. 147.

dışarıdan değil, içeriden de risk altında olabilmektedir. Bu nedenle çalışanların bilinçli ve bilgili olması oldukça önemlidir.[221]

Veri sorumlusunun kişisel verilere erişim yetkisi olan çalışanlarıyla, yetki sınırlarının ve sürelerinin belirlenmesi oldukça önemlidir. Ayrıca özel nitelikte kişisel verileri işleyen çalışanlarla gizlilik sözleşmesi imzalanması zorunludur.[222] Nitekim özel verilerin nasıl işleneceğine dair standartları belirleyen, Kurul'un 31/01/2018 Tarih, 2018/10 Sayılı Kararı'nda, "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" gerektiği ifade edilmiştir.[223]

Çalışanların sınırlı bilgileri olsa dahi bir saldırı anında ilk müdahaleyi yapabilmesi zararın kontrol altına alınması açısından oldukça önemlidir. Ayrıca "kişisel verilerin hukuka aykırı olarak açıklanmaması ve paylaşılmaması gibi konular hakkında eğitim almaları, çalışanlara yönelik farkındalık çalışmaları yapılması ve güvenlik risklerinin belirlenebildiği bir ortam oluşturulması kişisel veri güvenliğinin sağlanması bakımından çok önemlidir." hükmü uyarınca çalışanlar için eğitim ve farkındalık çalışmaları yapılması; "izin verilmedikçe her şey yasaktır" düşünce tarzıyla hareket etmeye teşvik edilmesi yerinde olacaktır.[224]

[221]KVKK, **Rehber**, s. 9; Zor**,** s. 96; Şahin Kara, **Veri Kurtarma Yöntemlerinin Başarımlarının Değerlendirilmesi**, Yüksek Lisans Tezi, Fırat Üniversitesi, 2013, s. 9.
[222]KVKK, **Rehber** s. 9; Zor, s. 96.
[223]Kişisel Verileri Koruma Kurulu, 31/01/2018 Tarih, 2018/10 Sayılı Kararı.
[224]KVKK, **Rehber**, s. 9.

2.3.4.1.3. Kişisel Veri Güvenliği Politikalarının Oluşturulması

Kanun kişisel veri güvenliği politikası oluşturulması yönünde bir yükümlülüğü doğrudan öngörülmemiştir, ancak kişisel verilerin güvenliği için istikrarlı ve güncel bir veri güvenliği politikasının oluşturulması oldukça önemlidir.[225]

Bu nedenle alınacak tedbirlerin önceden belirlendiği bir olay yönetimi planı hazırlanmalıdır. Veri sorumluları veri kayıt sistemlerine kaydettikleri verilerin tespitini iyi yapmalı, bu tür verilerin gerektirdiği tüm makul önlemleri incelemeli ve yasal yükümlülüklerine göre hareket etmelidir. Belirlenen bu politikalar ve prosedürler bağlamında düzenli olarak kontroller yapılmalı ve belgelenmeli, eksiklikler giderilmeli ve güncellemeler yerine getirilmelidir. Her kişisel veri kategorisi için ortaya çıkabilecek riskler ve güvenlik ihlallerini yönetim planı açıkça belirli olmalıdır.[226]

2.3.4.1.4. Kişisel Verilerin Mümkün Olduğunca Azaltılması

KVKK m. 4/2 uyarınca kişisel verilerin gerektiğinde doğru ve güncel olması gerekir ve bu veriler ilgili mevzuatta öngörülen veya işlendikleri amaca uygun süre kadar muhafaza edilebilir. Faaliyeti gereği çok fazla veri toplaması gereken veri sorumluların bazıları çok fazla kişisel veri toplamanın getirdiği bir sonuç olarak bir kısmı zamanla doğru olmayan, güncelliğini yitirmiş ve herhangi bir amaca hizmet etmeyen verileri muhafaza ediyor olabilir. Bu sebeple veri sorumlusunun işlediği amaç için anılan ilgili kişisel verilerin gerekliliğini değerlendirmeli, doğru şekilde muhafaza ettiğinden emin olmalıdır. Aynı şekilde, kişisel veri işleme amaçlarına uygun olsa da sıklıkla erişmesinin gerekmediği ve arşivlenmiş verilerin daha güvenli ortamlarda muhafazası Kurum'un tavsiye ettiği bir uygulamadır. İhtiyaç duyulmayan verilerin veri saklama ve imha politikalarına uygun olarak imha edilmesi makul olandır.[227]

[225]Çekin, s. 147; Zor, s. 95.
[226]KVKK, **Rehber**, s. 11.
[227]KVKK, **Rehber,** s. 11.

2.3.4.1.5. Veri İşleyenler ve Müşterek Veri Sorumluları ile İlişkilerin Yönetimi

Veri sorumluları, bilgi teknolojileri ihtiyaçları doğrultusunda veri işleyenler ile çalışabilir.[228] Veri sorumlularının, hizmet aldıkları veri işleyenlerin sağladığı veri güvenliği seviyesinin en az kendi sağladığı güvenlik seviyesi kadar olduğundan emin olması gerekir.[229] Nitekim GDPR m. 28 uyarınca veri sorumlularının GDPR'ın gerekliliklerini yerine getirebilecek ve ilgili kişilerin haklarının korunmasını sağlayacak şekilde gereken teknik ve idari tedbirleri uygulayabilecek veri işleyenleri seçmesi gerekir.[230] Veri işleyenin seçiminde uygulanacak kriterlere yer veren m.28, aynı zamanda veri sorumlusu ile veri işleyen arasında sözleşme yapma zorunluluğuna da yer vermiştir; buna göre sözleşme, veri işleme faaliyetlerinin amacı, işlenecek veri kategorileri, tarafların hakları ve yükümlülükleri, veri işleyeninin veri sorumlusunun kayıtlı talimatlarına uyma zorunluluğu hususlarını içermelidir.[231]

Veri sorumlusu ile veri işleyen arasında akdedilecek sözleşmenin yazılı olması Kurum tarafından önerilir. Ayrıca sözleşmede; veri işleyenin yalnızca sözleşmede belirtilen veri işleme amaç ve kapsamda ve mevzuat ışığında hareket edeceğine dair bir hüküm eklenmesi, ayrıca veri işleyenin işlediği kişisel verilere yönelik süresiz sır saklama yükümlülüğü altında olacağının da yer alması faydalı olacaktır.[232] Ancak veri işleyen her ne kadar veri sorumlusu adına ve hesabına hareket etse de veri sorumlusunun sorumluluğu KVKK m. 12'de düzenlenen müşterek sorumluluk uyarınca ortadan kalkmayacaktır.

GDPR m. 26/1 uyarınca veri işleme amaçlarını ve yöntemlerini birlikte belirleyen, birlikte karar alan ya da somut bir etki yaratan kişiler ortak veri sorumlusudur. Bu halde iki ya da daha fazla veri sorumlusu, ortak veri sorumluları olacak olup, ilgili kişilere karşı birlikte sorumlu olacaklardır. Kişilerin ortak veri sorumlusu olarak belirlenebilmesi için veri işlemenin her iki tarafın da katılımı

[228]KVKK, **Rehber,** s. 11.
[229]KVKK, **Rehber** s. 12-13; Zor, s. 97.
[230]Zor, s. 97.
[231]Kaya, İrem, **Kişisel Verilerin Korunması Kanunu ve Avrupa Birliği Genel Veri Koruma Tüzüğü (GDPR) Kapsamında Ortak Veri Sorumluluğu**, Yüksek Lisans Tezi, Hacettepe Üniversitesi, Ankara, 2023, s. 34.
[232] KVKK, **Rehber,** s. 13.

olmadan mümkün olmaması gerekir; bir başka deyişle tarafların katılımı birbirlerine ayrılmaz şekilde bağlı olmalıdır.[233]

Ortak veri sorumlusu kavramı KVKK'da tanımlanmamıştır, veri sorumlularının ortak sorumluluk hali de düzenlenmemiştir. Veri işleme amaçlarını ve yöntemlerini belirleyen her bir veri sorumlusunun KVKK'nın yükümlülüklerine tabi olacağı doğal olarak görülebilir. Bu durumda ortak veri sorumlularının TBK m. 61 uyarınca müteselsil sorumlulukları gündeme gelecektir.[234]

KVKK'nın veri sorumlusu tanımına bakıldığında, birden fazla kişinin birlikte veri sorumlusu olup olamayacağı açıkça engellenmese de bu konuya bir açıklık da getirmemektedir.[235] Bu konuda KVKK'nın açık bir düzenleme içermemesi aynı zamanda ortak veri sorumluluğunu reddetmediği sonucuna da bağlanabileceği görüşündeyiz.

Mevzuatta ortak veri sorumlusu kavramına yer verilmemesine rağmen, Kişisel Verileri Koruma Kurulu 23.12.2021 Tarih ve 2021/1304 Sayılı Kararı ile bu kavrama değinmiş ve bu kavramın Türk hukuku bakımından uygulanabilir olduğuna işaret etmiştir.[236] Kurul, gelen ihbarlar neticesinde yaptığı incelemelerde, araç kiralama firmalarının müşterilerine ait kişisel verileri ile olumsuz araç kullanımı deneyimlerini derleyen ve kara liste olarak anılan bir yazılımın birçok araç kiralama firması tarafından kullanıldığı tespit edilmiştir. Bu uygulama vasıtasıyla bir araç kiralama firmasının işlediği verilere başka bir araç kiralama firması erişebilmektedir. Kurul tarafından kara liste uygulamaları kanalıyla kişisel veri işleyen araç kiralama firmaları ile yazılım şirketlerinin ortak veri sorumlusu olduğunu değerlendirilmiştir. Kararda gerekli idari ve teknik tedbirlerin tıpkı GDPR'da öngörüldüğü gibi veri sorumlularınca müteselsilen alınması gerektiği belirtilmiştir.

[233]Avrupa Veri Koruma Otoritesi, "Avrupa Birliği Genel Veri Koruma Tüzüğü kapsamında veri sorumlusu ve veri işleyen kavramlarına ilişkin 07/2020 Kılavuzu", 02.09.2020, s. 3.
[234]Develioğlu, s. 102; Zor, s. 98.
[235]Dülger, 196-197.
[236]Kaya, İrem, **Kişisel Verilerin Korunması Kanunu ve Avrupa Birliği Genel Veri Koruma Tüzüğü (GDPR) Kapsamında Ortak Veri Sorumluluğu**, Yüksek Lisans Tezi, Hacettepe Üniversitesi, Ankara 2023, s. 84.

İlk defa ortak veri sorumlusu kavramına değinilen bu kararda ortak veri sorumlularının nasıl tespit edileceği üzerinde durulmamış ancak ortak veri sorumlularının kusurları oranında sorumlu olacağı belirtilmiştir. Ancak karara konu olayda görüleceği üzere kişisel verilerin işlenmek üzere veri sorumlusu tarafından üçüncü bir kişiye aktarılıyor olması, o üçüncü kişinin mutlaka veri işleyen sıfatı kazanacağı anlamına gelmemektedir; ortak veri sorumluları kavramı ya da iki farklı veri sorumlusunun mevcudiyeti üzerinde de düşünülmelidir.[237]

2.3.4.2. Kişisel Veri Güveliğine İlişkin Teknik Tedbirler

Veri güvenliği, kişisel verilerin tüm işleme aşamalarında korunmasına hizmet eder.[238] Teknolojinin de gelişmesiyle alınması gereken teknik tedbirler değişebilmektedir. Buna nazaran veri sorumlusunun teknik tedbirlerini olabildiğince güncel ve yeni tutması gerekir. [239]

KVKK'da alınabilecek teknik tedbirler tek tek sayılmasa da Rehber uyarınca veri sorumlusunun alabileceği teknik tedbirler siber güvenliğin sağlanması (ağ güvenliği, uygulama güvenliği, şifreleme, kriptografi, veri maskeleme, veri kaybı önleme yazılımları, yedekleme güvenlik duvarları, güncel anti-virüs sistemleri vb.), kişisel veri güvenliğinin takibi (sızma testi, saldırı tespit ve önleme sistemleri, erişim logları, kullanıcı hesap yönetimi, log kayıtları), kişisel verilerin bulunduğu ortamların güvenliğinin sağlanması ve kişisel verilerin yedeklenmesidir.[240]

KVKK, m. 12 ile idari ve teknik tedbirlerin alınması noktasında veri sorumlusu ve veri işleyenlerin müştereken sorumlu olduğunu düzenlemekteyken; m.18 ile idari yaptırımların veri sorumlusuna uygulanacağını düzenlemiştir. Kanun, GDPR'ın aksine veri işleyenlerin sorumluluğunu geniş tutmamış, sorumluluğu idari ve teknik tedbirleri almak ile sınırlamıştır. Uygulamada veri sorumlusu ve veri işleyen kişileri birbirinden ayırmak her zaman kolay olmadığından, sorumluluğun dar tutulması bu kavramların

[237]Rodway, Suzanne/Carey, Peter, **Oursourcing Personal Data Processing**, Data Protection A Practical Guide to UK and EU Law, 5.Baskı, United Kingdom, 2018.s. 180-183.
[238]Çekin, s. 186.
[239]Çekin, s. 188.
[240]KVKK, Rehber**,** s. 28.

iç içe geçtiği zamanlarda zorluk yaratabilecektir.[241] Çünkü, veri sorumlusu ile veri işleyenin farklı yükümlülüklere tabi olması iki sıfatın ait olduğu gerçek ya da tüzel kişilerin ayırt edilmesini gerektirmektedir.[242] Oysa ki, gerçek ya da tüzel bir kişi aynı anda veri sorumlusu ve veri işleyen sıfatıyla faaliyet gösteriyor olabilir.

GDPR'a göre alınabilecek idari tedbirlere, kişisel verilerin takma adlandırılmasının ve şifrelenmesinin uygulanması; siber güvenlik süreçlerinin geliştirilmesi ve uygulanması; etkili yedekleme ve felaket kurtarma süreçlerine sahip olmak; Sistemler ve fiziksel araçlar için kişisel verilerin otomatik olarak silinmesine yönelik süreçlerin uygulanması; özel kategorilerdeki kişisel verileri içeren belgeler için ayrı şifreler dâhil olmak üzere, sistemlerinizi korumak için güçlü şifreler belirlemek; geçerli erişim haklarının verilmesi; Fiziksel güvenlik önlemlerinin geliştirilmesi: tesislere erişimin, ziyaretçi kayıtlarının, güvenlik aydınlatmasının ve alarmların güvenliğini sağlamaya yönelik sağlam önlemler örnek olarak gösterilebilir.

2.3.4.2.1. Siber Güvenliğin Sağlanması

Bilhassa dijital dünya ve teknolojik gelişmeler konusunda siber güvenlik, hukuk ekseninde önemli bir yere sahiptir.[243] Daha yeni teknolojilerin benimsenmesi ile ortaya siber tehdit unsuru çıkmıştır ve siber tehdit unsurlarının oluşması ile ortaya siber güvenlik kavramı çıkmıştır.[244],[245] Riskin boyutu arttıkça da alınması gereken önlemlerin de arttırılması ve farklılaştırılması zorunlu hale gelmiştir.[246] Sözlük anlamı ile siber güvenlik (cybersecurity) kavramı "bilişim sistemlerinde kişiler ve kurumlar arasında oluşturulan iletişim ortamının ve elektronik ortamda paylaşılan bilgilerin bütünlüğünün ve gizliliğinin korunması" olarak tanımlanmıştır.[247] Bir başka sözlük uyarınca ise aynı tanımlama "suç oluşturan veya yetkisiz kullanılan bir elektronik veriye karşın korunma hali veya bu amaçların gerçekleşmesine karşı alınan tedbirler"

[241]Akıncı, s. 29.
[242]Rodway/Carey, s. 182.
[243]Kapancı, s. 78.
[244]John M Blythe, **Cyber Security In The Workplace: Understanding and Promoting Behaviour Change**, Conference: Proceedings of CHItaly 2013 Doctoral Consortium, 2013, s. 92.
[245]Tunca**,** Sibel, **Modern Çağda Siber Güvenlik Kavramı**, Dumlupınar Üniversitesi İktisadi ve İdari Bilimler Fakültesi Dergisi, Sayı: 3-4, 2019, s. 1-2.
[246]Küzeci, s. 256
[247]*Bkz*. https://sozluk.gov.tr/ (E.T.:10.03.2024).

olarak ifade edilmiştir.[248] Kişisel verilerin muhafazasının ve işleme faaliyetlerinin önemli bir kısmının elektronik ortamda gerçekleşmesi sebebi ile alınması gereken tedbirlerin başında siber güvenliğin sağlanması olacaktır.[249]

GDPR m.32 ile benzer şekilde KVKK m. 12'nin de veri sorumlusu için öngördüğü gerekli güvenlik düzeyinin sağlanması yükümlülüğünün en önemli gereklerinden birinin siber güvenliğin sağlanması olduğu söylenebilir.

Siber güvenlik ürünlerinin kullanılması, siber güvenliğin sağlanması için başvurulan en yaygın tedbirlerdendir. Ancak tek bir siber güvenlik ürününün kullanılması tek başına güvenliği sağlamayabilir. Kurum tamamlayıcı sistemler ile desteklemeyi önermektedir.[250]"İnternet üzerinden gelebilecek izinsiz erişim tehditlerine karşı güvenlik duvarı, kişisel verilerin güvenliğini tehdit edebilecek internet sitelerine veya online servislere erişimi engelleyecek ağ geçidi, siber güvenliğin sağlanmasında alınabilecek tedbirlere örnektir."[251] Bahsedilen internet ağ geçidi, saldırıları durduran ilk savunma mekanizmasıdır.[252] Sistemlerin doğru çalışabilmesi adına, kullanılan yazılım ve donanımların düzenli olarak test edilmesi ve gerekiyorsa güncellenmesi gerekir.[253] Veri güvenliğinin sağlanması süreklilik arz etmelidir, bu sebeple sadece sistemin kuruluşunda değil, sistemin işleyişinin devam ettiği süreçte de önem taşır.[254]

Kişisel verileri şifreleyerek muhafaza etmek bu açıdan faydalıdır. Bu tedbir her tür kişisel veri için gerekmemektedir. Ancak, Kurul'un özel nitelikli kararların işlenmesine ilişkin verdiği karar uyarınca özel nitelikli kişisel verilerin muhafaza edilmesi için kriptografik yöntemler kullanmak ve kriptografik anahtarlarının güvenli bir şekilde kaydının yapılması zorunludur.[255]

---

[248]*Bkz*. https://en.oxforddictionaries.com/definition/cybersecurity (E.T.: 10.03.2024).
[249]Altındere, Murat, **Kişisel Verilerin Korunması Hukuku ve Uygulanması**, Ankara, Adalet Yayınevi., 2020, s. 81.
[250]Altındere, s. 176.; KVKK, **Rehber**, s. 17.
[251]Zor, s. 99.
[252]Altındere, s. 82, 175-176.; Küzeci, s. 255.
[253]KVKK, **Rehber**, s. 18., Altındere, s. 82-83.; Küzeci, s. 255-256.
[254]Kapancı, s. 68.
[255]*Bkz*. Kişisel Verileri Koruma Kurulu, 31/01/2018 Tarih, 2018/10 Sayılı Karar.

Kurum ayrıca veri sorumlularının, erişim yetki ve kontrol matrisi oluşturmalarını önermektedir.[256]

2.3.4.2.2. Kişisel Veri Güvenliğinin Takibi

Veri güvenliğine yönelik bir siber saldırıya veya zararlı yazılımlara maruz kalan veri sorumlusunun bu tehditleri olabilecek en hızlı şekilde fark edip önlemelidir.

Bu durumun önüne geçebilmek ve etkin bir veri güvenliği sağlayabilmek için veri sorumlusunun; sistem uyarıların takip edilmesi, bilişim ağlarında hangi yazılım ve servislerin çalıştığını kontrol etmesi, bilişim ağlarında sızma veya olmaması gereken bir hareket olup olmadığını tespit etmesi, tüm kullanıcıların işlem hareketleri kaydının düzenli olarak tutması (örn: log kayıtları), güvenlik sorunlarını mümkün olduğunca hızlı bir şekilde raporlaması, raporlama sisteminin düzenli test edilmesi, sonuçlara göre değerlendirmelerde bulunarak güvenlik açıklarının giderilmesi, çalışanların sistem ve servislerdeki güvenlik zaafiyetlerini ya da bunları kullanan tehditleri bildirmesi için resmi bir raporlama prosedürü oluşturması gerekir.[257][258]

2.3.4.2.3. Kişisel Verilerin Bulunduğu Ortamların Güvenliğinin Sağlanması

Veri sorumlusunun kişisel verilerin muhafaza edilmesinde; kişisel verilerin çalınma, kaybolma, bozulma ya da dış riskler vb. tüm risklere karşı önlem alması gerekir. Kişisel verilerin muhafaza edildiği ortamın güvenliğinin ve denetiminin yapılması oldukça önemlidir. Kişisel veri içeren fiziki dosyalar, sunucular, taşınabilir bellek yedekleme cihazları, CD ya da DVD gibi cihazların sadece belirli yetkili kişilerin girebileceği bir ortamda kilit altında korunması ve bu ortamın da giriş çıkış kaydının tutularak denetilmesi gereklidir.[259]

[256]KVKK, **Rehber**, s. 18.
[257]Zor, s. 100.; Altındere, s. 178-179.; KVKK, **Rehber**, s. 18.; GDPR m. 32/1d
[258]Ayrıca bkz. Küzeci, s. 262.
[259]KVKK, **Rehber** s. 20-21; Zor, s. 100.; Küzeci, s. 255-256.

2.3.4.2.4. Kişisel Verilerin Yedeklenmesi

Siber saldırılar ile üçüncü kişiler kişisel verilere erişebilir, değiştirebilir veya yok edebilir. Ayrıca kötü amaçlı yazılımlar da muhafaza edilen verilere erişimi kısıtlayabilir veya tamamen engelleyebilir. Bu gibi durumlarda veri sorumlusunun yedeklenen verileri kullanarak en kısa sürede harekete geçmesi esas olandır. Bu sebeple veri sorumlusunun veri yedekleme stratejileri geliştirip uygulaması gerekir. Buradaki önemli faktör bu yedeklenen verilere sadece sistem yöneticisinin erişebilir olmasıdır. Yedeklenen veriler mutlaka ağ dışında tutulmalıdır. Yoksa hali hazırda gerçekleşen siber saldırılar yedeklenen verilere erişimi de engelleyebilir ve bu da yedeklemenin amacına uymayan bir sonuca yol açacaktır.[260] Kurum, bu halde veri sorumlusunun, yedeklenen verilere ulaşması ve en kısa sürede faaliyetlerine devam etmesini beklemektedir.[261]

2.3.4.3. Veri Sorumlusunun Denetim Yükümlülüğü

KVKK m. 12/3'te veri sorumlusunun gerekli denetimleri yapmak veya yaptırmak zorunda olduğu ifade edilmiş veri sorumlusuna denetim sorumluluğu yüklenmiştir. Bu yükümlülük Rehber uyarınca ayrıca veri sorumlusunun alacağı idari tedbirlerden biri olarak sayılmıştır. [262]

Denetim yükümlülüğü uyarınca veri sorumlusunun kendi kurum ya da kuruluşunda KVKK hükümlerinin uygulandığından emin olmalıdır, bu nedenle de gereken denetimde bulunmayı veya bu denetimin yapılmasını sağlamalıdır. Yani bu denetim veri sorumlusunca veya bir üçüncü kişi aracılığıyla gerçekleştirilebilir.

Burada bu denetimin kapsamının ne olduğu da incelenmelidir. Kanun lafzından anlaşılan denetimin yalnızca veri güvenliğine ilişkin değil, aynı zamanda KVKK hükümlerinin uygulanmasına dair ilgili tüm hususlar bu denetimin

[260]KVKK, **Rehber,** s. 24.; Göksu, Mustafa, **Hukuk Yargılamasında Elektronik Delil**, Ankara, Adalet Yayınevi, 2010, s. 23
[261]Çekin, s. 151
[262]KVKK, **Rehber**, s. 29.; Kaya, s. 1892

kapsamındadır. [263] Nitekim Kurul'un "aydınlatma metinleri mevzuata uygun olmayan ve ilgili kişiye 30 gün içinde cevap vermeyen veri sorumlusunun gerekli denetimleri yapmak bakımından da ihlale sebep olduğuna ve disiplin hükümleri doğrultusunda yükümlü kişiler hakkında işlem yapılmasına"[264] karar verdiği düşünüldüğünde, denetim yükümlülüğünün sadece veri güvenliği bakımından sınırlanmamış olduğu görülür.[265] Bu durum da Kanun lafzını destekler.

Son olarak belirtmek gerekir ki KVKK'da ya da Rehber'de denetim bakımından bir zaman dilimi öngörülmemiştir. İlgili maddede geçen "gerekli" ibaresinden de anlaşılabileceği gibi, denetim için gereken süre veri sorumlusunca takdir edilmelidir.

2.3.4.4.Kanuna Aykırı Başkasına Açıklama ve İşleme Amacı Dışında Kullanım Yasağı

Veri güvenliğine ilişkin diğer bir yükümlülük ise KVKK m. 12/4'te "Veri sorumluları ile veri işleyen kişiler, öğrendikleri kişisel verileri bu Kanun hükümlerine aykırı olarak başkasına açıklayamaz ve işleme amacı dışında kullanamazlar. Bu yükümlülük görevden ayrılmalarından sonra da devam eder" şeklinde ifade edilen kanuna aykırı başkasına açıklama ve işleme amacı dışında kullanım yasağıdır.

Bir görüşe göre, ilgili fıkranın kaynağı 95/46/EC Sayılı Direktif ve KVKK'nın 2008'deki tasarısıdır, 2008 tasarısında "yetkisiz olarak açıklanmasını veya aktarılmasını" önlemeye ilişkin getirilen yükümlülüğün bir görünümü olduğunu ifade etmiştir.[266]

Maddenin gerekçesinde bu hüküm bir sır saklama yükümlülüğü olarak açıklanmıştır.[267] Buna göre, veri sorumlusunun öğrendiği kişisel verileri KVKK hükümlerine aykırı olarak başkalarına açıklaması veya şahsi çıkarlardı için kullanması

[263]Öztekin, s. 56; Yasemin Avcı, **Kişisel Verilerin Korunması**, Selçuk Üniversitesi, Yüksek Lisans Tezi, Konya 2019, s. 90.
[264]Öztekin, s. 56.
[265]Kişisel Verileri Koruma Kurulu'nun 02.05.2019 tarihli 2019/122 sayılı kararı. Bkz. https://www.kvkk.gov.tr/Icerik/5461/2019/122 (E.T.:15.03.2024).
[266]*Bkz*. Öztekin , s. 58, dn 278.
[267]KVKK, **Gerekçe ve Terimler Sözlüğü**, s. 31.

yasaktır. İlgili yükümlülük, söz konusu kişiler görevlerinden ayrıldıktan sonra da devam eder.[268] Burada amaç dışı kullanımı sır saklama yükümlülüğünün bir parçası olarak anmak, sır saklamanın daha geniş kapsamlı yorumlandığını gösterir.[269]

[268]KVKK, **Gerekçe ve Terimler Sözlüğü**, s. 31.
[269]Öztekin, s. 57.

3. VERİ GÜVENLİĞİ İHLALİNİN TESPİTİ VE VERİ SORUMLUSUNUN BİLDİRİM YÜKÜMLÜLÜĞÜ

3.1. Veri Güvenliği İhlali

Veri sorumlusunun veri güvenliğine ilişkin son yükümlülüğü KVKK m. 12/5'te ve GDPR m. 33 ve 34'te düzenlenen bildirim yükümlülüğüdür. Veri sorumlusunun, veri güvenliğini ihlali durumunda veri koruma otoritesine bildirim yükümlülüğü GDPR m. 33'te, ilgili kişiye yapacağı bildirim ise m. 34'te düzenlenmiştir.[270] Buna göre, bir veri ihlali durumunda veri sorumlusunun bu durumu en kısa sürede ilgili kişiye ve Kurul'a bildirmesi gerekir; böylece ilgili kişiler ve Kurum ihlal sonucuna yönelik önlem almak için imkana sahip olacak, zarar asgari düzeyde tutulabilecek ve ihlalin tekrarlanması engellenebilecektir.[271] Buradan hareketle bildirim yükümlülüğünün doğması için bir veri ihlalinin olması ve bunun tespit edilmesi gerekir. [272]

3.1.1. Veri İhlali Kavramı

Veri sorumlusunun ilgili bildirim yükümlülüğünün doğması için öncelikle kişisel veri güvenliğinin ihlal edilmesi gerekmektedir. Bu nedenle de veri ihlali kavramından ne anlaşılacağı incelenmelidir.

Tanımlar başlıklı GDPR m. 4/12'de kişisel veri ihlali "iletilen, depolanan veya başka bir şekilde işlenen kişisel verilerin kazara veya hukuk dışı yollarla yok edilmesi, kaybı, değiştirilmesi, izinsiz şekilde açıklanması veya bunlara erişime yol açan bir güvenlik ihlâli…" olarak tanımlanmaktadır. KVKK'nın "Tanımlar" başlıklı 3. maddesinde ise kişisel veri ihlali tanımlanmamıştır. Ancak "Veri Güvenliğine İlişkin Yükümlülükler" başlıklı 12. maddesinin 5. fıkrasında "…işlenen kişisel verilerin kanuni olmayan yollarla başkaları tarafından elde edilmesi…" olarak belirtilmiştir.

[270]Develioğlu, s. 108.
[271]Küzeci, s. 359.
[272]Develioğlu, s. 108.

EDPB, GDPR uyarınca kişisel veri ihlali bildirimine ilişkin Kılavuz İlkeleri'ni ("EDPB Kılavuz İlkeleri" veya "Kılavuz") yayınlamış, veri ihlali bildirimi yükümlülüğünün gerekliliklerini ve atılacak adımları açıklamıştır. [273]

EDPB Kılavuz İlkeleri uyarınca, GDPR'a göre 3 ayrı ihlal türü sayılmıştır. Bunlar: gizlilik ihlali, bütünlük ihlali ve kullanılabilirlik ihlalidir. Ayrıca Kılavuz'da somut duruma göre bir ihlalin bu üç durumu aynı anda veya bunların herhangi bir kombinasyonu ile ilgili olabileceği de ifade edilmiştir.[274] Veri ihlalinin gizlilik veya bütünlük ihlali olup olmadığının tespiti, erişilebilirlik ihlaline göre daha açık olabilir. Ancak Kılavuz uyarınca kişisel verilerin kalıcı olarak kaybedilmesi veya imha edilmesi her zaman kullanılabilirlik ihlali olarak değerlendirilmektedir.[275]

Ayrıca kişisel verilerin kullanılabilirliğinin geçici olarak kaybedilmesinin bir ihlal olarak değerlendirilip değerlendirilmeyeceği konusunda Kılavuz, GDPR m. 32'de sayılan işleme güvenliği hususlarına atıf yaparak kişisel verilerin bir süreliğine kullanılamaz hale gelmesiyle sonuçlanan bir güvenlik olayı da bir ihlal türü olduğunu ifade etmiştir. Ancak veri sorumlusunun IT sistemlerinin bakımı dolayısıyla geçici olarak verilere erişememe hali, bir güvenlik ihlali olmamaktadır.[276]

GDPR'ın tanımlaması ve EDPB Kılavuz İlkeleri incelendiğinde; bilgi güvenliğinin üç temel unsuru olan gizlilik, bütünlük ve erişilebilirlik kavramları kendini kişisel veri ihlali tanımında gösterdiği görülür. Ancak KVKK'daki tanımda bilgi güvenliğinin unsurlarından sadece gizlilik unsuru yer edinmiştir. Burada lafzi ve dar bir yorum yapılırsa bütünlük ve erişilebilirlik unsurlarının zarar görmesinin 'kişisel veri ihlali' tanımı kapsamına alınmadığı söylenebilecektir. Diğer bir deyişle KVKK bakımından veri ihlali, kişisel bilgilerin üçüncü kişiler tarafından ele geçirilmesi ve bu ele geçirilmenin kanuni olmayan yollarla gerçekleşmesi olarak ifade edilmektedir.[277]

---

[273]EDPB, "Guidelines 09/2022 on personal data breach notification under GDPR", Mart 2023, (Versiyon 2.0), s. 6. *Bkz.* https://www.edpb.europa.eu/system/files/2023-04/edpb_guidelines_202209_personal_data_breach_notification_v2.0_en.pdf (E.T.:28.03.2024) **["EDPB, Kılavuz İlkeler"].**
[274]EDPB**, Kılavuz İlkeler**, s. 8.
[275]EDPB, **Kılavuz İlkeler**, s. 8.
[276]EDPB, **Kılavuz İlkeler**, s. 9.
[277]Öztekin, s. 59; Sevindi, Ordu, s. 14.

Ayrıca KVKK'da yer alan "kanuni olmayan yollarla" ibaresi ile hukuka uygun olmayan tüm durumlar kapsanmıştır. Bu açıdan ilgili ibare sadece KVKK'yı değil, ayrıca ilgili her türlü mevzuatı kapsamaktadır. Bir başka ifade ile veri ihlali, yürürlükte olan bütün düzenlemelere aykırı eylemler ile meydana gelir.[278] Örneğin, Ticari İletişim ve Ticari Elektronik İletiler Hakkında Yönetmelik, Kişisel Sağlık Verilerinin İşlenmesi ve Mahremiyetinin Sağlanması Hakkında Yönetmelik, Sosyal Yardım Verilerinin Kaydedilmesi ve Paylaşılmasına İlişkin Yönetmelik gibi düzenlemelere aykırılık halleri de bu kapsamdadır.[279]

Görüldüğü gibi KVKK bakımından veri ihlali kavramı ile GDPR bakımından veri ihlali kavramları farklıdır. Bir düşünceye göre, KVKK'da düzenlenen veri ihlali kavramının tıpkı GDPR'da ifade edilen veri ihlali kavramı gibi geniş yorumlanması gerekmektedir.[280] Başka bir görüşe göre ise KVKK'da ifade edilen veri ihlali kavramı oldukça açıktır, geniş yorumlanması uygulamada belirsizliklere yol açacaktır.[281]

Ancak belirtilmelidir ki; veri ihlali kavramı, GDPR'da KVKK hükümlerine kıyasla daha detaylı düzenlenmiş olsa da veri ihlal bildirimine ilişkin usul ve süre büyük oranda örtüşmektedir.[282]

Bu noktada GDPR'da tanımlanan haliyle veri ihlalinin kişisel verilerin korunması açısından daha geniş ve faydalı bir koruma sağladığı kanaatindeyiz. Kurul'un bazı kararlar ve rehberler ile birtakım hususları standartlaştırmaya yönelik eylemleri düşünüldüğünde[283], KVKK'daki anlamın GDPR'daki gibi daha geniş yorumlanmasının da bu uyuma katkı sağlayabilecektir.

[278]Dülger, s. 30-31; Sevindi, Ordu, s. 13.
[279]Sevindi, Ordu, s. 13.
[280]Avcı, s. 91.
[281]Öztekin, s. 59.
[282]Sevindi, Ordu, s. 13.
[283]*Bkz*. Kişisel Verileri Koruma Kurulu'nun 24.01.2019 tarihli 2019/10 sayılı kararı. https://www.kvkk.gov.tr/Icerik/5362/Veri-Ihlali-Bildirimi (E.T.:20.03.2024). **["KVKK, 2019/10 sayılı Karar"].**

3.1.2. Veri İhlalinin Tespiti

KVKK m. 12/5 uyarınca, veri sorumlusunun işlenen kişisel verilerin kanuni olmayan yollarla başkaları tarafından elde edilmesi hâlinde, en kısa bildirim yükümlülüğü söz konusudur. Kurul, yayınladığı 24.01.2019 tarihli 2019/10 sayılı Karar'da ("Karar") veri sorumlusunun bildirim yükümlülüğünün "…veri sorumlusunun bu durumu öğrendiği tarihten itibaren…" başladığını ifade etmiştir.[284] Kurul tarafından yayınlanan Kişisel Veri İhlali Bildirim Kılavuzu'nda ise veri ihlalinin başlama tarihi, "veri sorumlusu tarafından yapılan incelemeler sonucunda veri ihlalinin başladığı tarih" olarak ifade edilmiştir.[285] Bu nedenle potansiyel ihlalin incelenmesi sonucunda varılacak tespit, veri ihlalinin de tespiti olacaktır.[286] Yine de, veri ihlalinin ne şekilde tespit edilmesi gerektiği ifade edilmemiş, aydınlatılmamıştır.

Bir ihlali tespit edebilmenin, ilgili kişilere yönelik riski değerlendirebilmenin ve gerekli olduğu durumlarda bildirimde bulunabilmenin önemi GDPR Resital 87'de de vurgulanmıştır. GDPR m. 33/1'de veri sorumlusunun "…ihlalden haberdar olduktan itibaren…" bildirim yükümlülüğünün doğduğunu ifade eder. EDPB Kılavuz İlkeleri'ne göre veri sorumlusunun kişisel verilerin tehlikeye girmesine yol açan bir güvenlik olayının meydana geldiğine dair makul bir kesinlik derecesine sahip olması halinde "haberdar" olacağı ifade edilmiştir.[287]

Veri ihlali; veri sorumlusunun kendisi, veri işleyen veya üçüncü bir kişi tarafından tespit edilebilir.

Potansiyel ihlalin bir dış kaynaktan öğrenilmesi bildirim veya tesadüfi bir yolla gerçekleşebilir. Veri sorumlusunun bu durumda dış kaynaktan öğrendiği ihlalin gerçekliğini tespit etmesi gerekir. Kişisel Veri İhlali Bildirim Formu Kılavuzu uyarınca veri ihlalinin tespit tarihi, ihlalden haberdar olma tarihi olarak tanımlandığından, veri sorumlusunun dış kaynaktan veri ihlalini öğrendiği tarih veri

[284]KVKK**, 2019/10 sayılı Karar;** Sevindi, Ordu**,** s. 15.
[285]Kişisel Verileri Koruma Kurumu, **Kişisel Veri İhlali Bildirim Formu Kılavuzu**, KVKK Yayınları, Ankara, 2019, s. 6. ["**KVKK, Bildirim Formu Kılavuzu"**].
[286]Sevindi, Ordu, s. 15.
[287]EDPB, **Kılavuz İlkeleri,** s. 11.

ihlalinin tespit edildiği ve dolayısıyla bildirim yükümlülüğünün başladığı tarih olarak kabul edildiği görülebilir.[288]

EDPD Kılavuz İlkeler uyarınca ise veri sorumlusu üçüncü bir kaynak tarafından olası bir ihlal hakkında bilgilendirildiğinde bu durumu soruşturması gerekir. Bu soruşturma döneminde veri sorumlusunun ihlalden haberdar olma durumunun gerçekleştiği kabul edilmeyebilir. Ancak veri sorumlusunun bu soruşturmaya mümkün olan en kısa sürede başlaması ve bir ihlalin gerçekleşip gerçekleşmediğinin makul bir kesinlik derecesinde tespit etmesi gerekmektedir. Bu tespit sonrası veri ihlalinin aşırı gecikme olmaksızın ve mümkün olduğu hallerde en geç 72 saat içerisinde bildirilmesi gerekir. [289]

Veri işleyenin bu ihlali tespit ettiği an, Veri İhlali Bildirim Formu uyarınca veri ihlalinin başladığı tarihtir.[290] Karar uyarınca, veri işleyenin nezdinde bulunan kişisel verilerin kanuni olmayan yollarla başkalarınca elde edilmesi durumunda, veri işleyenin herhangi bir gecikmeye olmadan veri sorumlusuna bildirim yapma zorunluluğu bulunur. Veri işleyenin veri sorumlusuna ihlali bildirdiği tarih ise haberdar olma anı olarak sayılacaktır ve bildirim yükümlülüğü doğmuş olacaktır.[291]

GDPR m. 33/2 uyarınca veri işleyen "hiçbir gecikmeye yer vermeksizin" veri sorumlusuna ihlali bildirmelidir. Veri işleyenin veri sorumlusuna bildirim yapmadan önce ihlalden kaynaklanan riski değerlendirmesine gerek yoktur. Bu risk değerlendirmesi veri sorumlusunun görevidir.[292]

GDPR uyarınca veri işleyenin veri sorumlusuna yapacağı bu bildirim için bir süre öngörülmemiştir. Burada EDPB, veri işleyenin veri sorumlusuna derhal haber vermesini ve ihlal ile ilgili daha fazla bilgiye sahip oldukça bu bilgilerin de aşamalı olarak veri sorumlusuyla paylaşılmasını önermektedir.[293]

[288]Sevindi, Ordu, s. 16; .KVKK, **Bildirim Formu**, s. 6
[289]EDPB, **Kılavuz İlkeleri,** s. 12.
[290]KVKK, **Bildirim Formu**, s. 6.
[291]Sevindi, Ordu, s. 17.
[292]EDPB, **Kılavuz İlkeler**, s. 13.
[293]EDPB, **Kılavuz İlkeler,** s. 14.

Eğer veri sorumlusu veri işleyene bu açıdan açık yetki verdiyse, veri işleyen veri sorumlusu adına bildirimde bulunabilir, ancak bu durumda da yasal sorumluluk her halükarda veri sorumlusunundur.[294]

3.2. Veri Sorumlusunun Bildirim Yükümlülüğü

KVKK m. 12/5 uyarınca veri sorumlusunun işlediği kişisel verilerin kanuni olmayan yollarla başkaları tarafından ele geçirilmesi halinde bu durumu en kısa sürede ilgili kişiye ve Kurul'a bildirmesi gerekir. Kanun "en kısa süre" ibaresinin ne ifade ettiğini açıklamamış ancak bu süre Kurul'un 24.01.2019 tarih ve 2019/10 sayılı "Kişisel Veri İhlali Bildirim Usul ve Esaslarına İlişkin Kararı" ile 'en kısa süre ifadesi' 72 saat olarak belirlenmiştir.

Kanun, ilgili kişiye ve Kurul'a bildirilecek olan veri ihlallerini ayırmamıştır. KVKK m. 12/5 lafzından hareketle veri sorumlusunun risk ya da önem derecesine bakmaksızın her türlü ihlalin hem ilgili kişiye hem de Kurul'a bildirilme yükümlülüğü altında olduğunu ifade etmek yanlış olmayacaktır.[295] KVKK'nın risk değerlendirmesi ayrımı yapmamış olması ve ihlalin önlemesine yönelik değil, ihlalin gerçekleşmesi sonucunda yaptırım uygulanmasına yönelik bir tutum izlediği şeklinde yorumlanabilir.

Bildirim üzerine Kurul, gerektiği halde bu durumu kendi internet sitesinde ilan edebilir veya uygun gördüğü başka bir yöntemle ilan edilmesine karar verebilir.[296,297]

Bildirim yükümlülüğü, veri sorumlusunun kusurundan ya da özeninden bağımsız bir yükümlülüktür. Veri sorumlusu gerekli her türlü özeni göstermiş olsa dahi veri ihlali gerçekleştiğinde yine bildirim yükümlülüğü bulunur.[298] Burada, veri sorumlusunun kusur oranı, Kurul'un belirleyeceği idari para cezası bakımından önem arz edecektir.

---

[294]EDPB, **Kılavuz İlkeler,** s. 14.
[295]Develioğlu, s. 108.
[296]Kişisel Verileri Koruma Kurumu (KVKK), "Kanun Kapsamındaki Hak ve Yükümlülükler", 23 Nisan 2019, s. 11. *Bkz*. https://www.kvkk.gov.tr/Icerik/4192/Kanun-Kapsamindaki-Hak-ve-Yukumlulukler (E.T.: 21.03.2024) **[**
[297]**[KVKK, Hak ve Yükümlülükler];** Halıcıoğlu, s. 85**;** Zor, s. 114; Özkan, s. 177; Dülger, s. 240.
[298]Çekin, s. 152-153; Zor, s. 114**;** Avcı, s. 92.

GDPR m. 33 ve 34'te veri sorumlusunun veri koruma otoritesine ve ilgili kişiye yapacağı bildirimler düzenlenmiştir. GDPR m. 33'te "Kişisel veri ihlalinin denetim makamlarına bildirilmesi" başlıklı ilgili maddenin 1. fıkrasında "Bir kişisel veri ihlali olması durumunda, kişisel veri ihlalinin gerçek kişilerin hakları ve özgürlükleri açısından bir riske sebebiyet vermesinin muhtemel olmadığı haller dışında, veri sorumlusu, fazla gecikmesizin ve uygun olması hâlinde, ihlalden haberdar olduktan itibaren en geç 72 saat içinde, kişisel veri ihlalini 55. madde uyarınca yetkili denetim makamına bildirir. Denetim makamına yönelik bildirimin 72 saat içinde yapılmadığı hallerde, bu bildirimle birlikte gecikme sebeplerine de yer verilir…" ifadesi düzenlenmiştir.

GDPR m. 34'te ise "Kişisel veri ihlali hakkında veri öznesinin bilgilendirilmesi" başlıklı yükümlülük düzenlenmiştir. İlgili maddenin 1. fıkrasında "Kişisel veri ihlalinin gerçek kişilerin hakları ve özgürlükleri açısından yüksek bir riske sebebiyet vermesinin muhtemel olduğu hâllerde, veri sorumlusu kişisel veri ihlali hakkında fazla gecikmeksizin, veri öznesini bilgilendirir." ifadesi yer almaktadır.

GDPR ilgili kişiye sadece hak ve özgürlüklerinin kayba uğrama ihtimalinde bildirim yapılması öngörülüyor iken, KVKK ilgili kişiye yapılacak olan bildirim yükümlülüğünü her halükarda zorunlu tutulmuştur.[299] Başka bir deyişle GDPR, risk merkezli bir yaklaşım benimseyerek, düşük riskli veri işleme faaliyetlerinde bulunan veri sorumlularına etki analizi yapılmasını, ilgili kişilere bildirim yapılmasını, veri koruma otoritesine başvuru yapılmasını zorunlu kılmamıştır. Çünkü GDPR, m. 32 ile veri sorumlularının gerekli teknik ve idari tedbirleri alma yükümlülüğünü, veri işleme eyleminin doğuracağı risklerle doğru orantılı olacak sınırlarla düzenlemiştir. Buna paralel olarak veri sorumlusunun, veri işleme faaliyetindeki risk seviyesi yükseldikçe hesap verilebilirliğe ilişkin yükümlülükleri de ağırlaşmaktadır.

KVKK'da ve GDPR'da iki adet bildirim yükümlülüğü açıkça düzenlenmiştir. Bunlar, ilgili denetim kuruluna yapılacak bildirim ile ilgili kişiye yapılacak bildirimdir. Bu nedenle tezimizde de bu bildirim yükümlülükleri ayrı olarak incelenecektir.

[299]Dülger, s. 559.

3.2.1. Veri Koruma Otoritesine Yapılacak Bildirim

KVKK m. 12/5 uyarınca veri sorumlusu Kurul'a en kısa sürede bildirim yapmak yükümlülüğü altındadır ve ilgili ihlale ilişkin bildiri yayınlama konusu Kurul'un kanaatindedir.[300] Buna göre veri sorumlusunun Kurul'a yapacağı veri ihlali bildirimi ve Kurul'un bu konuya yönelik bildiri yayınlama hakkı olmak üzere iki ayrı durum söz konusudur: [301]

İlgili maddede yer alan "en kısa süre" ibaresi belirli bir zaman aralığını ifade etmemektedir ve bu da uygulamada nasıl anlaşılacağı tam olarak anlaşılamayan bir husus oluşturmaktaydı.[302] KVKK'ya temel teşkil eden Direktif'in aksine, GDPR'da veri ihlal bildirimlerine ilişkin olarak detaylı düzenlemelere yer verilmiştir ve 72 saat içerisinde bildirim yapılması gerektiği açıkça ifade edilmiştir. Bu durumda GDPR gözetilerek uygulamada bir standartlaşma sağlanabilmesi ve birtakım soru işaretlerinin giderilmesi amacıyla Kurul, Karar'ı yayınlamıştır.[303]

Karar'da; Kurul'a ve ihlalden etkilenen ilgili kişilere bildirim yapılmasındaki amacı, "ihlal nedeniyle bu kişiler hakkında ortaya çıkabilecek olumsuz sonuçların bir an önce önüne geçilmesi veya en aza indirilmesine imkân verecek önlemler alınmasını sağlamak" olarak ifade edilmiştir.

Karar uyarınca, KVKK m. 12/5'te yer alan "en kısa sürede" ifadesi, veri sorumlusunun bu durumu öğrendiği andan itibaren gecikmeksizin en geç 72 saat içerisinde Kurul'a bildirimde bulunması olarak yorumlanacağı ifade edilmiştir. Veri sorumlusunun ihlalden haberdar olması itibariyle 72 saat içerisinde Kurul'a bildirim yapmaması durumunda gecikme nedenlerini veri ihlali bildirim formunda açıklanması gerekir.

[300]Çekin, s. 152; Zor, s. 114.
[301]Çekin, s. 152; Halıcıoğlu, s. 85. Develioğlu, s. 107-108.
[302]Dülger, s. 240.
[303]Kişisel Verileri Koruma Kurulu'nun 24.01.2019 tarihli 2019/10 sayılı kararı. Bkz. https://www.kvkk.gov.tr/Icerik/5362/Veri-Ihlali-Bildirimi (E.T.:20.03.2024) **["KVKK, 2019/10 sayılı Karar"].**

Kurul'a yapılacak veri ihlal bildirimleri için "Kişisel Veri İhlal Bildirim Form"u kullanılır. Form'da istenen her bilgi anında sağlanamıyor ise ilk olarak veri sorumlusunun elindeki bilgileri İlk Bildirim olarak sunması, sonra aşamalı olarak diğer bilgileri de Takip Bildirimi olarak sunması gerekir.

Veri sorumlusunun veri ihlallerine dair bilgileri, ihlalin etkilerini ve aldığı önlemleri raporlaması Kurul tarafından beklenmektedir. Veri ihlalinin, yurtdışında yerleşik veri sorumlusu bünyesinde bulunan kişisel verilere yönelik yaşandığı hallerde, bu ihlalin sonuçları Türkiye'de yerleşik ilgili kişileri etkiliyorsa ve ilgili kişiler sunulan ürün ve hizmetlerden Türkiye'de faydalanıyorlarsa yine Kurul'a bildirimde bulunulması şarttır. Veri sorumlusunun veri ihlali durumunda içyapısından kime raporlama yapacağının belirli olması gerekir, bu çerçevede veri sorumlusunun bu gibi konuları içeren bir veri ihlali müdahale planı hazırlanması beklenmektedir.

GDPR m. 33 uyarınca ise veri sorumlusu bir kişisel veri ihlali olması durumunda, kişisel veri ihlalinin gerçek kişilerin hakları ve özgürlükleri açısından bir risk oluşturmadığı durumlar dışında, ihlalden haberdar olduktan itibaren en geç 72 saat içinde, kişisel veri ihlalini GDPR m. 55 uyarınca yetkili veri koruma otoritesine bildirmelidir. [304]

GDPR m. 33/3'te ise veri sorumlusu veri koruma otoritesine veri ihlali bildirimi yapacağında asgari olarak yapılması gerekenler ifade edilmiştir. Buna göre: Veri sorumlusunun mümkün olduğu hallerde, ilgili kişilerin verilerinin kategorileri ve yaklaşık sayısı ve ilgili kişisel veri kayıtlarının kategorileri ve yaklaşık sayısı da dâhil olmak üzere kişisel veri ihlalinin niteliğini açıklaması gerekir. Veri koruma görevlisinin veya daha fazla bilgi alınabilecek diğer irtibat noktasının adını ve irtibat bilgilerini iletmesi gerekir. Kişisel veri ihlalinin olası sonuçlarını açıklamalıdır. Uygun hallerde, olası olumsuz etkileri hafifletmeye yönelik tedbirler de dâhil olmak üzere kişisel veri ihlalini ele almak için aldığı veya alacağı tedbirleri açıklamalıdır.[305],'[306]

[304]OneTrust DataGuidance, Esin Attorney Partnership; "Comparing Privacy Laws: GDPR v. LPPD", Nisan 2023, s. 27.
[305]EDPB, **Kılavuz İlkeler**, s. 14
[306]M'Bia Hortense De-Yolande, Théo Doh-Djanhoundji, Gabo Yves Constant, **Breach Notification in the General Data Protection Regulation**, Université Virtuelle de Côte d'Ivoire, Abidjan, Cote d'Ivoire, 2023, s. 337.

İlgili madde uyarınca veri sorumlusu en azından bu bilgileri veri ihlali bildiriminde sağlamalıdır. Her bir somut olayın koşulları kendi içinde daha fazla bilginin sağlanmasını da gerektirebilir.[307]

GDPR m. 33/1 uyarınca veri sorumlusu 72 saat içinde bildirim yapamazsa gecikmeye ilişkin sebeplerini de bildiriminde belirtmelidir. Bu durum, pratikteki ilk edinilen bilgilerin iletilip yeni bilgilere sahip olunduğunda bir takip bildirimi ile onların da sunulması durumu ile beraber, bir veri sorumlusunun her zaman süresi içinde bildiremeyebileceğini kabul eden bir durum ortaya koymaktadır.[308] Veri sorumlusunun kısa bir sürede birden çok veri ihlali ile karşılaşması durumunda, ihlallerin kapsamının tespit edip aynı şekilde ihlal edilen aynı tür kişisel verilere ilişkin olmaları koşuluyla, tüm bu ihlalleri temsil eden bir "paket" bildirim yapması da mümkündür.[309] Paket bildirim yapılmasının önünün açılması son derece isabetlidir. Uygulamada veri ihlaline uğrayan kuruluşlar, bildirimde yer alması gereken bilgileri GDPR'da öngörülen süre içerisinde toplayamayabilir ve bu durum mevzuat gerekliliklerinin karşılanamamasına neden olabilir.[310]

GDPR ile KVKK açısından farklılık oluşturan husus ise GDPR'da gidilen ikili ayrımdır. Buna göre GDPR, temel hak ve özgürlüklere zarar veren veri ihlallerini zarar bakımından riskli ve yüksek riski olarak iki ayrı aşamada değerlendirmektedir.[311]

Madde 33/1 açıkça ilgili kişilerin hak ve özgürlükleri açısından bir riske sebep vermesinin düşük ihtimalli olduğu durumları bildirim yükümlülüğünün dışında tutmuştur. Oysaki KVKK'da bu şekilde bir ayrıma gidilmemiş, veri ihlali veya veri ihlali türleri dahi GDPR'da yer aldığı şekilde tanımlanmamıştır.

EDPB, kişisel veri ihlalinin gerçek kişilerin hakları ve özgürlükleri açısından bir riske sebebiyet vermesinin muhtemel olmadığı hallere, verilerin halihazırda kamuya açık olduğu ve bu verilerin ifşa edilmesinin birey için olası bir risk teşkil

[307]EDPB, **Kılavuz İlkeler**, s. 15.
[308]EDPB, **Kılavuz İlkeler**, s. 16.
[309]EDPB, **Kılavuz İlkeler**, s. 16.
[310]O'Brien, **Privacy and Security: The New European Data Protection Regulation and It's Data Breach Notification Requirements**, Business Information Review, 2016, s. 83.
[311]Sevindi, Ordu**,** s. 18.

etmediği durumları örnek olarak vermiştir. Aynı şekilde, kişisel verilerin yetkisiz taraflarca anlaşılamaz hale getirildiği ve verilerin bir yedeğinin bulunduğu durumları da örnek olarak belirtmiştir.[312]

Başta olası bir risk oluşturmayan veri ihlali zaman içerisinde risk taşır bir hale dönüşürse, burada yeniden bir bildirim yükünün doğması söz konusu olabilecektir. Bu durumda veri sorumlusunun yeniden bir değerlendirme yapması gerekir.[313] Bu halde veri sorumluları, güvenlik sistemlerinin veri ihlalleriyle baş edebilecek kapasiteye sahip olduğunu gösteren belgelere ihtiyaç duyacaktır ve ilgili veri koruma otoritesini ve veri ihlalinden olumsuz etkilenmesi muhtemel veri sahiplerini bilgilendirmelidir.[314]

Kanaatimizce, KVKK uyarınca risk taşımayan veri ihlallerinin de bildirilmesi hali, Kurum'un hâlihazırda çok olan iş yükünü daha da artırmakta, ilgili kişilerin korunması amacına ters düşmekte, Kurum'un incelemesi gereken dosya yükünü artırmakta ve daha ciddi bir risk yükü barındıran bazı olayların incelenmesini geciktirme ihtimali doğurmaktadır. Bu bakımdan GDPR'ın veri sorumlularının bildirim yükümlülüğü için risk merkezli yaklaşımını doğru bulmaktayız.

3.2.2. İlgili Kişiye Yapılacak Bildirim

Veri sorumlusunun yalnızca Kurul'a değil, ayrıca veri ihlalinden en çok etkilenen kişiler olan ilgili kişilere de bildirimde bulunması gerekmektedir. Karar uyarınca veri sorumlusunun yine, ihlalden etkilenen kişilerin belirlenmesi itibariyle onlara da makul olan en kısa süre içerisinde bildirimde bulunmalıdır. Bildirim süresinin Kanun'da yer almaması, konuya ilişkin verilen kararlarda çelişki yaratabilmekte olduğundan ilgililere yapılacak olan bildirim için makul bir sürenin belirlenmesi gerekmektedir.[315]

[312]EDPB, **Kılavuz İlkeler**, s. 18-19.
[313]EDPB, **Kılavuz İlkeler,** s. 19.
[314]Burton, s. 649.
[315]Kişisel Verileri Koruma Kurulu'nun 16.05.2019 tarih ve 2019/143 sayılı; 16.05.2019 tarih ve 2019/141 sayılı; 08.03.2019 tarih ve 2019/67 sayılı; 01.09.2022 tarih ve 2022/882 sayılı kararları.

İlgili kişilere yapılacak bildirim eğer ilgili kişinin adresine ulaşılabiliyorsa doğrudan, eğer ulaşılamıyorsa veri sorumlusunun kendi web sitesi üzerinden ilan yoluyla olmalıdır.

Veri sorumlusunun ilgili kişiye yapacağı bildirimde asgari olarak hangi hususların yer alması gerektiği Kurul'un 18.09.2019 tarih ve 2019/271 sayılı kararı ile belirlenmiştir.[316] Bu karardan hareketle veri ihlali bildirimi yapılmasındaki amacın ilgili kişilerin veri ihlali neticesinde maruz kalabileceği olumsuzlukları engellemek, en azından en aza indirmektir ve her halükarda ilgili kişiler nezdinde gerekli tedbirlerin alınmasını sağlamaktır. Buna göre; veri sorumlusunun ilgili kişiye oldukça açık ve sade bir dille bildirim yapması ve asgari olarak; ihlalinin ne zaman gerçekleştiği, kişisel veri kategorilerinden hangilerinin ihlalden etkilendiği, kişisel veri ihlalinin olası sonuçları, veri ihlalinin olumsuz etkilerinin azaltılması için alınmış olan ya da alınacak tedbirler, ilgili kişilerin veri ihlali ile ilgili bilgi almalarını sağlayacak irtibat kişilerinin isim ve iletişim detayları veya veri sorumlusunun web sayfasının adresi, çağrı merkezi gibi iletişim yolları unsurların bu bildirimde yer alması gerekir

GDPR m. 34 uyarınca, kişisel veri ihlali yaşandığında, veri ihlalinin ilgili kişilerin hak ve özgürlüklerine yönelik bir riske yol açma ihtimali yüksekse, veri sorumlusunun ihlalden etkilenen ilgili kişilerin bilgilendirilmesi gerekir. Bu bilgilendirme, gecikme olmaksızın, açık ve sade bir dille olmalıdır. Madde, veri sahiplerine Avrupa Birliğinin en temel ilkelerinden olan bilgi edinme hakkını sağlamaktadır.[317] Dikkat edilmesi gereken nokta, GDPR'ın bildirim yükümlülüğün yalnızca veri sorumlusu için geçerli olmasıdır. [318]

Bildirimde veri koruma görevlisi veya ihlale yönelik bilgi alınabilecek kişinin isim-irtibat bilgileri, kişisel veri ihlalinin olası sonuçları ve kişisel veri ihlalinin olası olumsuz etkilerinin azaltılmasına ve kontrol edilmesine yönelik alınan veya alınacak tedbirler yer almalıdır.

[316]Kişisel Verileri Koruma Kurulu'nun 18.09.2019 tarihli 2019/271 sayılı kararı. *Bkz*. https://www.kvkk.gov.tr/Icerik/5547/2019-271 (E.T.:31.03.2024).
[317]Esayas, **Breach Notification Requirements Under the European Union Legal Framework: Convergence, Conflicts, and Complexity in Compliance**, The John Marshall Journal of Information Technology & Privacy Law, (2014), s. 323.
[318] Burton, s. 659.

Resital 86'da ilgili kişilere yönelik yapılacak bildirim hakkında "Veri sahiplerine yönelik bu tür iletişimler, denetim makamı veya kolluk kuvvetleri gibi diğer ilgili makamlar tarafından sağlanan rehberliğe riayet edilerek, makul olarak mümkün olan en kısa sürede ve denetim makamı ile yakın işbirliği içerisinde yapılmalıdır. Örneğin, acil bir zarar riskini azaltma ihtiyacı veri sahipleriyle derhal iletişime geçilmesini gerektirirken, devam eden veya benzer kişisel veri ihlallerine karşı uygun tedbirlerin uygulanması ihtiyacı iletişim için daha fazla zamanı haklı gösterebilir" denilmiştir.[319]

İlgili kişiye her durumda bildirim yapılması gerekmez. GDPR m. 34/3 uyarınca; "(a) veri sorumlusunun uygun teknik ve kurumsal koruma tedbirleri uygulaması ve kişisel verileri bu verilere erişim izni bulunmayan hiç kimse tarafından anlaşılamaz hale getiren şifreleme gibi tedbirler başta olmak üzere, bu tedbirlerin kişisel veri ihlalinden etkilenen kişisel verilere uygulanmış olması; (b) veri sorumlusunun 1. paragrafta atıfta bulunulan veri öznelerinin hak ve özgürlüklerine ilişkin yüksek riskin gerçeğe dönüşmesinin artık muhtemel olmamasını sağlayan ek tedbirler alması; (c) bilgilendirmenin orantısız bir çaba gerektirecek olması" hallerinde ilgili kişiye bildirim yapılması gerekmemektedir. Bunun yerine ilgili kişiler, kamuya yönelik yapılacak bir bilgilendirme vb. bir tedbir aracılığı ile bilgi sahibi olacaktır.[320]

Veri sorumlusunun ilgili kişileri veri ihlaline yönelik bilgilendirmediği durumlarda, veri kuruma otoritesi gerekli görürse veri sorumlusunun ilgili kişileri bilgilendirmesini şart koşabilir veya gerekli olmayan hallerin varlığına hükmedebilir.

3.2.3. GDPR Bakımından Risk Değerlendirilmesi

GDPR bir ihlali bildirme yükümlülüğü getirse de, her koşulda bunu yapmak bir gereklilik değildir. Bir ihlalin bireylerin hak ve özgürlüklerine yönelik bir riskle sonuçlanma ihtimali düşük olursa ilgili veri koruma otoritesine bildirimde bulunma zorunluluğu bulunmamaktadır. İlgili kişiye ise veri ihlalinin bireyin hak ve

[319]Resital 86. *Bkz*. https://gdpr-info.eu/recitals/no-86/ (E.T.: 31.03.2024).
[320]Hortense De-Yolande, Doh-Djanhoundji, Constant, s. 338-339.

özgürlüklerine yönelik yüksek bir riskle sonuçlanmasının muhtemel olduğu durumlarda ve GDPR m. 34/4'te sayılan hallerin dışında bildirimde bulunma zorunluluğu söz konusudur.

Bu nedenle GDPR'ın bir risk değerlendirmesi yapılmasını zorunlu kıldığı görülebilir. EDPB'ye göre burada bahsedilen risk, ihlalin verileri ihlal edilen bireyler için fiziksel, maddi veya maddi olmayan zarara yol açabileceği durumlarda bulunur. Bu tür zararlara örnek olarak da ayrımcılık, kimlik hırsızlığı veya dolandırıcılık, mali kayıp ve itibarın zedelenmesi gibi olgular sayılmıştır.[321]

EDPB uyarınca riskin değerlendirilmesinde; ihlalin türü, kişisel verilerin niteliği, hassasiyeti ve hacmi, bireylerin kimlik tespitinin ne kadar kolay olduğu, bireyler için sonuçların ciddiyeti, bireyin özel nitelikleri, veri sorumlusunun özel nitelikleri, etkilenen bireylerin sayısı göz önünde bulundurulmalıdır.[322]

GDPR'de neyin risk ve yüksek risk teşkil ettiğine ilişkin net bir tanım, açıklama, rehberlik veya içtihat bulunmamasıdır.

GDPR, veri sahiplerinin hak ve özgürlüklerine yönelik olası risklerin neler olduğunu bir şekilde tanımlasa da, veri koruma mevzuatında risk kavramının ne olduğuna dair ortak bir anlayış bulunmamakta ve risk ile yüksek risk kavramları ele alınmamaktadır. Bu durum Tüzük'teki yükümlülüklerin etkili bir şekilde yerine getirilmesini engellemekte ve karışıklık kaynağı oluşturmaktadır.[323] Neyin risk ve yüksek risk teşkil ettiğine ilişkin net bir tanım, açıklama, rehberlik veya içtihat bulunmaması eleştirilmekte; risk ve yüksek risk kavramların açık olmamasının "bildirim yorgunluğuna" sebep olabileceği düşünülmektedir.[324] Bildirim yorgunluğu, veri ihlallerinin etkilenen bireylere aşırı bildiriminin veri sahiplerini veri ihlalinin olası olumsuz etkilerine karşı duyarsızlaştırdığı durumdur.

[321]EDPB, **Kılavuz İlkeler,** s. 23.
[322]EDPB, **Kılavuz İlkeler,** s. 23-26.
[323]Wilson, **A Framework for Security Technology Cohesion in the Era of the GDPR**, Computer Fraud & Security (December 2018), s. 11.
[324]Demetzou, **Data Protection Impact Assessment: A Tool For Accountability and the Unclarified Concept of 'High Risk' in the General Data Protection Regulation,** Computer Law and Security Review, (2019), s. 6.

KVKK'da bu yönde bir risk değerlendirmesi yapılması öngörülmemiştir. Aksi husus ne maddenin lafzından anlaşılabilmektedir ne de Kurul'un yayımları ve kararları ile böyle bir ayrım ortaya konulmuştur. Bu bakımdan KVKK'daki düzenlemenin daha yüzeysel kaldığı; veri sorumlularının yapmış oldukları risk ölçümleri kapsamında, veri işleme faaliyetinin risk seviyesine göre, ilgililere bildirim değerlendirmesi yapılması gerekmektedir.[325]

Kanaatimizce de KVKK'da bir risk ölçümü ayrımının öngörülmemiş olması, uygulamada Kurul'un üzerinde iş yükü oluşturmaktadır. GDPR'daki değerlendirme kriterlerini veri sorumlusunun veri ihlalini önleyebilmesi açısından daha faydalı bulmaktayız. Veri sorumlusunun veri ihlalinden kaynaklanan riski değerlendirme aşamalarında gözden geçireceği kriterler, veri ihlalinin boyutunu ve nasıl önlenebileceğini anlamasına da yardımcı olacaktır ve bu nedenle uygulamada ilgili kişilerin zarar görmesinin önüne daha hızlı geçilebilecektir.

Öte yandan, GDPR risk merkezli bir yaklaşımla tasarlanmasına rağmen veri sahipleri nezdinde bildirim yorgunluğu yaratması ve ayrıntı eksikliğinden kaynaklı veri ihlali bildirim yükümlülüğünün pratikliğini azalttığı gerekçesi ile eleştirildiği gözetildiğinde, KVKK'ya tabi veri sahipleri için bu yorgunluğun had safhada olması beklenir; ancak ilginçtir, çok fazla bildirim aldığını ileri süren veri sahipleri enderdir. Bu husus, bildirim yükümlülüğü konusunda Kanun'un yeteri kadar uygulanabilir olmadığı şeklinde de yorumlanabilir.

3.3. Veri Güvenliğine İlişkin Yükümlülüğün Yerine Getirilmemesinde Sorumluluk

Veri güvenliğine ilişkin yükümlülüklerin yerine getirilmemesi halinde ilgili kişiler sözleşme sorumluluğu, kusura dayalı haksız fiil sorumluluğu ve kişisel verilerin korunması mevzuatlarına dayalı sorumluluk bağlamında zararlarının giderilmesini talep edebilir.

[325]Dülger, s. 559.

3.3.1. Sözleşme Sorumluluğu

Zarara uğrayan kişi ile arasında bir sözleşme var ise, veri sorumlusunun ya da işleyenin veri güvenliğine ilişkin yükümlülüklerini yerine getirmemesi durumunda sözleşmesel sorumluluk gündeme gelecektir. Esas itibariyle temerrüt, kusurlu sonraki ifa imkânsızlığı ve borcun gereği gibi ifa edilmemesi şeklinde vücut bulan sözleşmeye aykırılık; kişisel verilerin sözleşmeye aykırı işlenmesi halinde genel olarak sözleşmenin gereği gibi ifa edilmemesi şeklindedir.[326] Çünkü esasen ortada bir ifa olmasına karşın edim, olması gereken nitelik ve niceliğe taşımadığından kötü ifa sayılmakta ya da ilgili sözleşmedeki asli edimi yerine getirilmiş olsa da yan yükümlerin ihlal edilmektedir.[327]

Veri sorumlusunun ya da işleyenin yükümlülüklerini tam ve gereği gibi yerine getirmemiş olması sözleşme borcunun yerine getirilmediğinden bahisle 6098 Sayılı Türk Borçlar Kanunu[328] ("TBK") m. 112 uyarınca tazminat talebini gündeme getirebilecektir. Ancak, sözleşme sorumluluk doğurmak için bir sözleşmenin varlığı tek başına yeterli olmayıp, o sözleşmenin veri güvenliğine ilişkin yükümlülükleri ayrıca düzenlenmiş olması, veri güvenliği düzeyinin belirlenmiş ya da belirlenebilir hale getirilmiş olması gerekmektedir. Aksi halde borca aykırılığın tespiti zorlaşabilecek ve hatta imkânsızlaşabilecektir.[329]

Sözleşmede veri sorumlusunun ya da işleyenin sorumluluğunu sınırlandıran kayıtlar bulunabilir ya da ayrıca bir sorumsuzluk anlaşması imzalanmış olabilir. Bu tür kayıtlar, TBK 115 uyarınca borçlu statüsündeki veri sorumlusu ya da işleyenin ağır kusurlu olduğu her halde ve hafif kusurlu olduğu bazı hallerde geçersizdir. Bir sorumsuzluk kaydı TBK 115 tahtında geçerli olsa bile, ilgili kişi aleyhine getirilen genel işlem şartı mahiyetinde ise yine geçersiz kılınabilir.[330] Bunun yanı sıra, ilgili kişinin tüketici olduğu ihtimalinde, tüketicinin korunmasına ilişkin özel hükümlerin

[326]Özdemir, Hayrunisa, **Elektronik Haberleşme Alanında Kişisel Verilerin Özel Hukuk Hükümlerine Göre Korunması**, Ankara, Seçkin Yayıncılık, 2009, s. 104.
[327] Eren, Fikret, **Borçlar Hukuku Genel Hükümler**, Ankara, Yetkin Yayınları, 2018, s. 103 vd.
[328] Resmî Gazete Sayı: 27836, Tarih: 04.02.2011
[329] Kapancı, s. 58.
[330] Kapancı, s. 59.

de uygulama alanı bulacağı gözetilerek sorumsuzluk kayıt ve anlaşmalarının uygulamada işlevsel olmayacağı kanaatine varılabilecektir.

Veri sorumlusu nezdinde sözleşmesel sorumluluğun kurulabilmesi için borca aykırı fiil, zarar, kusur ve uygun nedensellik bağının bulunması şart olup; tazminat talebinde bulunulabilmesi için borca aykırı fiil, zarar ve nedensellik bağı varlığının talepte bulunan tarafından ispat edilebilmesi gerekmektedir.[331] Burada kusurun varlığı adi karine olarak esas alındığından talepte bulunanın zarar verenin kusurunu ispat etmesine gerek olmamakla birlikte, zarar veren borçlu kusursuzluğunu ispat etmek suretiyle sorumluluktan kurtulabilir[332] Bu halde, ilgili kişi kusuru kanıtlamak zorunda olmayacaktır ancak veri sorumlusu ya da işleyen, veri güvenliğine ilişkin yükümlülüklerini yerine getirmemesinde kusuru olmadığını ortaya koyarak tazminat talebini def edebilecektir.[333]

TMK m. 24/2'de kişilik haklarına yönelik her saldırının, kişilik hakkı zedelenen kimsenin rızası, daha üstün nitelikte özel veya kamusal yarar ya da kanunun verdiği yetkinin kullanılması halleri olarak sayılan hukuka uygunluk sebepleri bulunmadıkça hukuka aykırı olduğu belirtilmiştir. Bu doğrultuda sözleşmeye aykırı olarak kişilik hakkı ihlal edilen ilgili kişi, şartları oluşmuşsa TMK m. 25/3 kapsamında da maddi ve manevi tazminat davası açabilir.[334] Ancak sözleşmeye aykırılık, aynı zamanda kişilik hakkının ihlali anlamına gelmiyorsa, TMK m. 24 uygulama alanı bulamayacak ve ilgili kişi sözleşmeden kaynaklı olarak kişilik hakkının ihlal edildiğinden bahisle dava açamayacak, ancak sözleşmeden doğan diğer yaptırımlara başvurabilecektir.[335]

3.3.2. Haksız Fiil Sorumluluğu

Zarara uğrayan kişi ile veri sorumlusu ya da işleyenin arasında herhangi bir sözleşmesel ilişki bulunmadığı hallerde 6098 Sayılı Türk Borçlar Kanunu[336] ("TBK")

[331]Kapancı, s. 57.
[332]Kapancı, s. 57.
[333]Kapancı, s. 58.
[334]Zor, s. 175.
[335] Zor, s. 175.
[336] Resmî Gazete Sayı: 27836, Tarih: 04.02.2011

m.49 uyarınca kusura dayalı haksız fiil sorumluluğunun kurulmasında hukuka aykırı bir fiilin kusurlu olarak işlenmesi sonucu bir zararın meydana gelmesi ve fiille zarar arasında uygun bir nedensellik bağının bulunması gerekir. Tazminat talebinde bulunulabilmesi adına bu unsurların varlığı, kusur da dâhil olmak üzere, bizzat talepte bulunan kişi tarafından ispat edilmelidir.[337]

Bir sözleşmenin mevcudiyeti, veri sorumlusu ya da veri işleyenin kişisel veriler nezdindeki yükümlülüklerini yerine getirmemesi halinde zarara uğrayan ilgili kişinin haksız fiil sorumluluğuna dayanarak tazminat talep edemeyeceği anlamına gelmez. Ancak sözleşme borcuna aykırılık hükümleri uyarınca tazmin edilebilecek zarar kategorileri, haksız fiil sorumluluğuna göre nazaran daha geniş olduğundan, zarara uğrayan tarafından tercih sebebi olacaktır.

Sözleşmeye aykırılık ile kişilik hakları da ihlal ediliyor ise manevi tazminat talep edilebilecektir çünkü ortada aynı zamanda bir hukuka aykırılık vardır[338] ve TBK m.114/2 uyarınca haksız fiil sorumluluğuna ilişkin hükümler, kıyas yoluyla sözleşmeye aykırılık hâllerine de uygulanır.[339]

Sözleşmesel sorumluluğa yol açan borca aykırı fiil ile uygun nedensellik bağı içinde olan tüm zararlar tazminat talebine konu edilebilirken, haksız fiil sorumluluğu hükümleri uyarınca bir zararın tazminat talebine konu edilebilmesi için zarar görenin malvarlığında mutlak bir hak ihlali gerçekleşmiş olmalı ya da en azından zarar gören değeri koruyan özel bir koruma normu mevcut olmalıdır.[340] Kişisel veri ihlallerinde, bu verilerin mutlak hak oluşturan kişilik hakkının uzantısı olduğu ve TBK 49/1 kapsamında "hukuka aykırılık" şartını sağladığı kabul edilir.[341]

KVKK'nın zarar görenin malvarlığını da korumaya yönelik özel bir koruma normu olarak değerlendirilmesi sebebi ile; ortaya çıkan zararın ilgilinin kişisel değerlerinin değil de malvarlığı değerlerinin eksilmesi biçiminde oluşması halinde

[337] Kapancı, s. 62.
[338] Özdemir, s. 106.
[339] Kılıçoğlu, Ahmet M., **Borçlar Hukuku Genel Hükümler**, Ankara, Turhan Kitabevi, 2019, s. 393.
[340] Kapancı, Kadir Berk, Ahlaka Aykırı Bir Fiille Kasten Verilen Zararın Tazmini (TBK 49 II), Vedat Kitapçılık, İstanbul, 2016, s. 35-36.
[341] Kapancı, s. 70.

zarar görenin mülkiyet ve zilyetlik gibi temel koruma normları tarafından korunan hukuki değerlerinden biri ihlal edilmiş olmasa da, maddi zararın tazmini mümkün olacaktır.[342] Bu halde verilerin hukuka aykırı olarak işlenmesi ya da korunamamasından dolayı örneğin müşteri kaybeden ilgililer, TBK 49/1 uyarınca yoksun kalınan kâr tazminatı da talep edebilecektir.[343]

Kapancı; haksız fiil sorumluluğuna başvurabilmek adına özel bir koruma normu arayışı kapsamında ceza hukuku kurallarına bakılması gerektiğini, çünkü suç teşkil eden bir fiilin yasaklanması ile korunmak istenen menfaatin haksız fiil sorumluluğu talebi için de dayanak teşkil edeceğini ifade etmektedir.[344 , 345]

Buna göre, 5237 Sayılı Türk Ceza Kanunu'nun[346] (TCK) 141. maddesinde düzenlenen hırsızlık suçu taşınır mal mülkiyetini ve zilyetliği korumayı hedeflediğinden, soyut ve maddi olmayan bir değerden ibaret olan kişisel verileri korumamaktadır. Bu anlamda madde, verilerin içinde kaydedildiği bir taşınır malın çalınması halinde bir fayda sağlayabilecektir. TCK m. 157'de düzenlenen dolandırıcılık suçuna bakıldığında ise, hırsızlık suçunun aksine korunmak istenen hukuki menfaatin genel olarak malvarlığının bütünü olduğu görülmektedir. Kişisel verileri kullanılarak ilgili kişiye yönlendirilmiş bir aldatma eylemi mevcutsa ve bu kapsamda bir zarar meydana geldi ise TCK m. 157 özel bir koruma normu kabul edilecek ve ilgili kişi tarafından haksız fiil temeline dayanarak tazminat talep edilebilecektir. TCK m. 244'de düzenlenen bir bilişim sistemine girerek haksız yarar elde etmeye ilişkin suç kapsamında, bilişim sistemine giriş yapılarak herhangi bir aldatma eylemi olmadan ya da doğrudan bilişim sistemine yöneltilen bir aldatma eylemi neticesinde dijital verilerin ele geçirilmesi halinde, kaybedilen veriler için haksız fiil sorumluluğu kapsamında tazminat talep edilebilecektir. Eylemin, sadece bilişim haksız olarak sistemine girmek ve sistemde kalmaktan ibaret olduğu halde ise TCK m. 243, zarar gören ilgili kişi için özel koruma normu teşkil edebilecektir. [347]

[342]Gürpınar, s. 690.
[343]Gürpınar, s. 690.
[344]Kapancı, s. 63.
[345]Bu konuda ayrıca bkz. Kapancı, Kadir Berk, "Özel Hukuk Penceresinden Blokzincir: "Sanal Para (Varlık)" Değerleri ve "Akıllı Sözleşmeler" Üzerine Değerlendirmeler", Gelişen Teknolojiler Ve Hukuk I: Blokzincir, Oniki Levha Yayınları, 2. Bası, İstanbul, 2021, p. 163-215, s. 174 vd.
[346] Resmî Gazete Sayı: 25611, Tarih: 12.10.2004
[347] Kapancı, s. 63-66.

Kişisel veriler için mutlak bir hak olan kişilik hakkı dâhilinde olsa da, diğer veriler için; ilgili kişinin zararı malvarlığında mutlak bir hak ihlaline vücut verecek şekilde gerçekleşmemiş ve zarar gören değeri koruyan özel bir koruma normu da mevcut değil ise "hukuka aykırı bir fiil" şartı sağlanamamış olacağından TBK m. 49/1 uyarınca sorumluluk affetmek mümkün olmayacaksa da, "ahlaka aykırı bir fiil" şartını arayan TBK m. 49/2 uyarınca haksız fiil sorumluluğunun kapısını çalmak mümkün olabilecektir. Bunun için "ahlaka aykırı bir fiil" ile birlikte zarar verme kastı ile meydana gelen bir zararın ve bu zarar ile ahlaka aykırı bir fiil arasında nedensellik bağının da oluşması gerekecektir.[348]

3.3.3. Kişisel Verilerin Korunması Mevzuatlarına Dayalı Sorumluluk

GDPR, "Sorumluluk ve Zararının Tazminini İsteme Hakkı" başlığını taşıyan 82. maddesi ile tüzüğe aykırılık nedeni ile maddi ya da manevi zarar gören herkesin veri sorumlularından ve işleyenlerden zararının tazmin edilmesini isteme hakkına sahip olduğunu açıkça düzenlemektedir.[349] Maddeye göre veri sorumlusu veya veri işleyen kişi bu sorumluluktan, zararı doğuran duruma hiçbir şekilde sebep olmadığını kanıtlayarak kurtulabilir.[350] Ancak madde, tazminat hakkının doğması için kusur sorumluluğunun mu yoksa kusursuz sorumluluğun mu kabul edildiğini belirtmemiştir.

Benzer şekilde, Direktif m. 23'e göre veri sorumlusunun hukuka aykırı eyleminden zarar gören bireylerin tazminat talep etme hakkı vardı ancak veri sorumlusu zarara yol açan olaydan sorumlu olmadığını ispat ederse yükümlülükten kısmen veya tamamen muaf olacaktı.[351]

KVKK ise, kişisel verilerin hukuka aykırı olarak işlenmesinden doğacak zararlardan sorumluluk bakımından özel bir madde içermemekle Avrupa Birliği düzenlemesinden farklılaşmaktadır.[352]

---

[348]Kapancı, s. 67.
[349]https://gdprhub.eu/Article_82_GDPR (E.T:01.07.2024).
[350] https://gdprhub.eu/Article_82_GDPR (E.T:01.07.2024).
[351]Kaya, s.81.
[352]Gürpınar, Damla, **Kişisel Verilerin Korunmasından Doğan Hukuki Sorumluluk**, Dokuz Eylül Üniversitesi Hukuk Fakültesi Dergisi, Cilt 19, Sayı 3, 2017, s. 689.

Kişisel verilerin korunması mevzuatı bağlamında güvenliğinin sağlanması yükümlülüğünün; bir sonucun mutlak olarak gerçekleşmesini hedef tutmadığını, veri sorumlusu ve duruma göre veri işleyenin her türlü saldırıyı bertaraf etmek durumunda olmadığını ve yükümlülüğün güvenliğin sağlanmasındaki süreçte gerekli önlemlerin alınmasına odaklanmakta olduğunu, her durumda alınması gereken önlemleri somut olayın şartlarına göre değişkenlik gösterdiğini ve bu şartlara uygun tedbirlerin alınmasının sorumluluğu kaldıracağını ifade etmiş idik.

Gerekli önlemler tam ve eksiksiz alınmadığı için ilgili kişilerin zarara uğramaları söz konusu olmuşsa, KVKK m. 11 ve 14[353] atfıyla ilgili kişi uğradığı zararın giderilmesini "genel hükümlere göre" talep edebilecektir.[354]

Kişisel verilerin korunması mevzuatlarına dayalı veri sorumlusunun tazminat yükümlülüğünün kusur sorumluluğu mu, yoksa özen sorumluluğu mu niteliği taşıdığı özellikle ispat hukuku bakımından uygulamada önem taşımakta olup; kusur sorumluluğunun benimsenmesi halinde zarara uğrayan ilgili kişi veri sorumlusunun kusurunu ispat etmek zorunda olacak, özen sorumluluğunun benimsenmesi halinde ise zarar gören ilgili kişi hukuka aykırı fiili ve zararını ispat etmekle yetinebilecek, özenli davrandığını ispat yükü ise veri sorumlusuna ait olacaktır.[355]

Doktrindeki baskın görüş uyarınca; maddenin düzenlenişinde kusur kavramına yer verilmemiş olsa bile, Türk sorumluluk hukukunda kusurun esas olması sebebi ile kişisel verilerin korunması mevzuatı bağlamında kusursuz sorumluluk hali düzenlenmedikçe doğacak sorumluluk kusur sorumluluğu niteliğindedir ve TBK m. 49/1 kapsamında değerlendirmeye alınması gerekmektedir.[356] Gerçekten de Türk Borçlar Kanunu'nda haksız fiilden sorumlulukta kusur esası kabul edilmekte ve kusursuz sorumluluk halleri istisnaen düzenlenmektedir.

[353]Burada sözü edilen genel hükümler, 4721 sayılı Türk Medeni Kanunu'nun 24. ve 25. maddeleri ile 6098 sayılı Türk Borçlar Kanunu'nun 53, 54, 56 ve 58. maddeleridir.
[354]Kapancı, s. 69; Gürpınar, s. 689.
[355]Çekin, s. 138, 139.
[356]Ayözger Öngün, s. 267; Özdemir, s. 207; Kaya, s. 106.

Gürpınar'a[357] göre ise mevcut düzenlemede kusur sorumluluğu söz konusu olsa da menfaatler dengesine uygun olarak tazminat yükümlülüğü TBK m. 71 kapsamında tehlike sorumluluğu çerçevesinde değerlendirilmedir.[358]

En ağır kusursuz sorumluluk hali olan tehlike sorumluluğunun uygulanması gerektiğini savunan görüşüne göre; veri sorumlusu dijital ortamda faaliyet göstererek kişisel verileri toplamayı, işlemeyi ve saklamayı üstlenmiş ise, verileri gerektiği gibi koruyamama riskini de üstlenmiştir ve kusurlu olmasa dahi bu sorumluluğu üstlenecektir. Çünkü tüm önlemler en yüksek derece özenle alınmış olsa dahi ağır zararlar meydana getirebilecek tipik bir veri ihlali tehlikesi bulunmaktadır.[359]

Zarar görenin yararı gözetilerek benimsenen tehlike sorumluluğu esasına göre üçüncü kişinin ağır kusuru halinde de veri sorumlusu ya da işleyen, ilgi kişinin tazminat talebinin hedefi olmaktan kurtulamayacak ve sık sık ciddi tazminatlar ödemek zorunda kalacaktır. Oysa ki, veri sorumlularının ya da işleyenlerin fiilleri çoğu zaman zarar doğurmaya tek başına elverişli değildir ve kişisel verilerin hukuka aykırı olarak işlenmeleri çoğu zaman ancak bir başkasının davranışı ile birleşerek zarara yol açabilir.[360] Bu halde veri sorumluları ve işleyenlerin, üçüncü kişiler ile müteselsilen sorumlu tutulmaları gerekse de, elbette rücu olanağı mevcut bulunacaktır. [361]

Çekin'e göre, veri koruma işlemlerinin her geçen gün daha da karmaşık hale geldiği ve kanunda veri sorumlularına gerekli idari ve teknik tedbirleri almaları hususunda yükümlülükler getirildiği dikkate alındığında bu çerçevede bir özen yükümlülüğünden bahis açmak, dolayısıyla özenli davrandığını ispat etme külfetini veri sorumlusuna yüklemek, bu sayede veri sorumlusunun organizasyonuna vakıf olmayan ilgili kişiyi kusuru ispat etme zorunluluğundan muaf tutmak daha isabetlidir.[362] Bununla birlikte Çekin, söz konusu sorumluluğun tehlike sorumluluğu niteliği de taşıdığını; veri sorumlusu her türlü özeni göstermesine rağmen sorumluluktan kurtulamayacaksa uygun idari ve teknik tedbir almasının hiçbir anlamı

[357]Gürpınar, s. 689-693.
[358]Kapancı, s. 70.
[359] Gürpınar, s. 691-692; Kapancı, s. 70-73.
[360]Gürpınar, s. 691-692.
[361]Gürpınar, s. 691-693.
[362]Çekin, Mesut Serdar, **Veri Hukuku**, On İki Levha Yayıncılık, 2. Baskı, Ekim 2019, s. 268-271. ["Çekin, Veri Hukuku"].

kalmayacağını, tehlike sorumluluğu rejiminin hukukun ekonomik analizi açısından tersine bir etkiye sebebiyet vereceğini ifade etmektedir.[363]

Kanımızca, göre kişisel verilerin korunması mevzuatı bağlamında doğacak sorumluluğun tehlike sorumluluğu çerçevesinde değerlendirilmesi gerektiği görüşü, Kanun'un 12. Maddesinin veri sorumlusunun güvenliğin sağlanması sürecinde gerekli önlemlerin alınmasında aranan özen düzeyini göstermiş olması gerektiğinden bahisle her türlü saldırıyı bertaraf etmek zorunda olmadığı yönündeki lafzı ile uyumlu olmaması sebebi ile isabetli değildir.

3.4. Veri Güvenliğine İlişkin Yükümlülüğün Yerine Getirilmemesi Kabahati

KVKK'da dört farklı kabahat türü düzenlenmiştir. KVKK m. 18 uyarınca bunlar aydınlatma yükümlüğünün yerine getirilmemesi, kişisel veri güvenliğine ilişkin yükümlülüklerin yerine getirilmemesi, kurul tarafından verilen kararların yerine getirilmemesi ve veri siciline kayıt ve bildirim yükümlülüğüne aykırı hareket etme kabahatleridir. Tez konumuzla sınırlamak amacıyla sadece veri güvenliği yükümlülüğüne uyulmama kabahati incelenecektir.

Bir görüşe göre, bu kabahat diğer kabahatlere göre daha özel bir yere sahiptir: "Bu durumun başlıca iki sebebi, kanaatimizce kişisel veri güvenliği kapsamında öngörülen yükümlülüklerin veri güvenliğinin kavramsal yapısını aşar şekilde geniş bir şekilde düzenlenmesi ve bunun dolaylı bir sonucu olarak kişisel verilerin işlenmesinin hukukiliği dâhil olmak üzere birçok yükümlülüğün veri güvenliği kapsamında yorumlanması ve değerlendirilmesidir. Böylece KVKK'ya aykırılık teşkil edecek birçok işlem ve eylem bu kabahatin kapsamında incelenmektedir."[364]

KVKK m. 18/1-b uyarınca "Bu kanunun … b) 12 nci maddesinde öngörülen veri güvenliğine ilişkin yükümlülükleri yerine getirmeyenler hakkında 15.000 Türk lirasından 1.000.000 Türk lirasına kadar… idari para cezası verilir." Denilmiştir.

[363]Çekin, Veri Hukuku, s. 270.
[364]Öztekin, s. 61.

Burada bahsedilen idari para cezası miktarı, Kurum tarafından 2024 yılı için alt sınır 141.934 Türk lirası ve üst sınır 9.463.213 Türk lirası olarak belirlenmiştir.

7499 sayılı Ceza Muhakemesi Kanunu İle Bazı Kanunlarda Değişiklik Yapılmasına Dair Kanun'un 35'inci maddesiyle 01.06.2024 tarihinde yürürlüğe girmek üzere KVKK m.18'de değişiklik yapılmıştır. Bu hususta Kurum yönetmelik ve rehber çalışmalarına başladıklarını bildirmiştir.

Yapılan değişiklik ile m. 18/1'e şu bent eklenmiştir: "d) 9 uncu maddenin beşinci fıkrasında öngörülen bildirim yükümlülüğünü yerine getirmeyenler hakkında 50.000 Türk lirasından 1.000.000 Türk lirasına kadar,". KVKK m. 18/2'de değişiklik yapılmış, maddeye ikinci fıkrasından sonra gelmek üzere şu fıkra eklenmiş ve diğer fıkra buna göre teselsül ettirilmiştir: "(2) Birinci fıkranın (a), (b), (c) ve (ç) bentlerinde öngörülen idari para cezaları veri sorumlusu, (d) bendinde öngörülen idari para cezası veri sorumlusu veya veri işleyen gerçek kişiler ile özel hukuk tüzel kişileri hakkında uygulanır. (3) Kurulca verilen idari para cezalarına karşı, idare mahkemelerinde dava açılabilir."

Kurul'un KVKK m. 12/5'in ihlal edilmesi hakkında birçok kararı mevcuttur. Örneğin Kurul, bir araç kiralama internet sitesindeki hesabına giriş yapan ilgili kişi, kendi giriş bilgilerini girmesine rağmen başka bir kişinin hesabına giriş yapıp o kişiye ait kişisel verileri görüntülediği somut olayı konu alan 24/08/2023 Tarihli ve 2023/1465 Sayılı kararında, veri sorumlusunun veri ihlalini bildirmesi sebebiyle KVKK m. 18/1-b uyarınca 200.000 TL idari para cezası uygulanmasına hükmetmiştir.[365]

Yine benzer şekilde, Kurul'un 27/04/2021 tarih ve 2021/427 sayılı kararında veri sorumlusu tarafından kendi tedarikçisi konumunda olan firma yetkilerinin, veri sorumlusunun sistemine giriş yaptıklarında üçüncü kişilere ait kişisel verilere yetkisiz erişim sağladıkları somut olay konu olmuştur ve Kurul veri sorumlusu hakkında 72

[365]Kişisel Verileri Koruma Kurulu'nun 24.08.2023 tarihli 2023/1465 sayılı kararı. *Bkz.* https://www.kvkk.gov.tr/Icerik/7784/2023-1465 (E.T.:31.03.2024).

saat içerisinde bildirimde bulunma yükümlülüğüne aykırı davranılması sebebiyle 200.000,00-TL idari para cezası uygulanmasına karar verilmiştir.[366]

GDPR'da ise idari para cezaları kesilmesine ilişkin genel koşullar m. 83'te düzenlenmiştir. Buna göre belirlenecek olan idari para cezasının miktarının hesaplanması GDPR'de öngörülen kurallara tabi olarak ilgili veri koruma kurulunun takdirindedir. GDPR m. 83/1 uyarınca para cezası miktarının her bir münferit durumda etkili, orantılı ve caydırıcı olmalıdır. 2. fıkrada ifade edildiği üzere ise para cezasının miktarını belirlerken, veri koruma otoritesi veri ihlalin özelliklerine veya failin karakterine atıfta bulunan bir koşullar listesini gerekli şekilde dikkate alacaktır. Verilecek para cezası GDPR m. 83'ün 4., 5. ve 6. fıkralarında öngörülen azami miktarları aşamaz. Bu nedenle, para cezasının miktarının belirlenmesi, GDPR tarafından öngörülen parametreler dâhilinde her bir vaka için gerçekleştirilen özel bir değerlendirmeye dayanmaktadır ve bu nedenle EDPB, idari para cezasının hesaplanmasına ilişkin ayrı bir kılavuz yayımlamıştır ("İdari Para Cezası Kılavuzu").

İdari Para Cezası Kılavuzu uyarınca veri otoritesi somut olayda öncelikle veri işleme faaliyetlerinin tanımlayacak ve GDPR m. 83/3'ün uygulanıp uygulanmayacağını değerlendirecektir. İkinci adım para cezasının miktarının hesaplanması için bir alt sınırı belirlemektir. Bunun yapılabilmesi için ihlalin GDPR'a göre sınıflandırılması, ihlalin ciddiyetinin değerlendirilmesi ve teşebbüsün cirosunun değerlendirilmesi gerekmektedir. Üçüncü adım, veri sorumlusunun ya da veri işleyenin geçmiş veya mevcut davranışlarına ilişkin ağırlaştırıcı ve hafifletici koşulların değerlendirilmesi ve buna göre cezanın artırılması ya da azaltılmasıdır. Dördüncü olarak Kurul, farklı ihlaller için ilgili yasal azami miktarları belirlemelidir. Son olarak ise hesaplanan nihai miktarın etkililik, caydırıcılık ve orantılılık gerekliliklerini karşılayıp karşılamadığının analiz edilmesi gerekmektedir.[367]

[366] Kişisel Verileri Koruma Kurulu'nun 27.04.2021 tarihli 2021/427 sayılı kararı. *Bkz*. https://kvkk.gov.tr/Icerik/6981/2021-427 (E.T.:31.03.2024).
[367]EDPB, **İdari Para Cezası Kılavuzu**, s. 3.

İdari Para Cezası Kılavuzu'nun "GDPR Kapsamındaki İdari Para Cezalarının Hesaplanmasına İlişkin 04/2022 Sayılı Kılavuzun Gösterimine İlişkin Tablo" başlıklı son ekinde ise alt sınırlar ve ilgili birtakım değerlendirmeler tablolaştırılmıştır.[368]

Veri sorumlusunun bildirim yükümlülüğünü gerçekleştirmemesi üzerine hakkında GDPR m. 83 uyarınca idari para cezası verildiği birçok karar bulunmaktadır. Örneğin Norveç Veri Koruma Otoritesi, GDPR m. 33/1'i ihlal ederek veri ihlalini zamanında bildirmeyen veri sorumlusuna GDPR m. 83 uyarınca 220.337 € idari para cezası vermiştir.[369]

Bir başka güncel kararda ise Polonya Veri Koruma Otoritesi, GDPR m. 34/1 uyarınca ilgili kişiye veri ihlali sebebiyle bildirim yapmayan veri sorumlusu hakkında GDPR m. 83 uyarınca 120.000 € idari para cezasına hükmetmiştir.[370]

[368]EDPB, **İdari Para Cezası Kılavuzu,** s. 43 vd.
[369]Datatilsynet (Norway) - 21/03126. (2023, March 24). *GDPRhub*. *Bkz*. https://gdprhub.eu/index.php?title=Datatilsynet_(Norway)_-_21/03126&oldid=31837 (E.T.: 19.04.2024).
[370]UODO (Poland) - DKN.5131.33.2021. (2022, March 2). GDPRhub, . *Bkz*. https://gdprhub.eu/index.php?title=UODO_(Poland)_-_DKN.5131.33.2021&oldid=23955 (E.T.: 19.04.2024).

SONUÇ

GDPR kapsamında "kimliği tespit edilmiş ya da teşhis edilebilir bir gerçek kişiye ilişkin her türlü bilgi" ve KVKK kapsamında da "Kimliği belirli veya belirlenebilir gerçek kişiye ilişkin her türlü bilgi" olarak tanımlanan kişisel veri kavramı; bir veri bulunması, kimliği belirli ya da belirlenebilir bir kişi olması ve verinin kişiye ait olması temellerinden oluşur.

Kişisel verilerin korunması kavramı, bireylerin korunmasını amaçlar. Veri güvenliği ve bilgi güvenliği kavramları ise bu amaca hizmet eden bir araçlardandır.

KVKK'da veri sorumlusunun veri güvenliğine ilişkin dört farklı yükümlülüğü düzenlenmiştir. Bunlar; veri sorumlusunun gerekli teknik ve idari tedbirleri alması, veri sorumlusunun kanun hükümlerinin uygulanmasına ilişkin kendi kurum ve kuruluşlarında gerekli denetimleri yapması veya yaptırması, kişisel verilerin amacı dışında kullanılmaması veya hukuka aykırı başkalarına açıklanmaması ve son olarak veri ihlal bildiriminin yapılması olarak ifade edilir.

KVKK'da olduğu gibi GDPR'da da veri güvenliğinin sağlanması için, veri sorumlusunun her türlü idari ve teknik tedbirleri almasını gerekir. Veri sorumlusu, kişisel verilerin korunması hukukuna aykırı olan veri işleme faaliyetlerinin tümünün sonucunda uğranılan tüm zararlardan sorumludur. Direktif'in aksine KVKK ve GDPR'da veri işleme faaliyetinde bulunması halinde veri işleyen de veri sorumlusu ile birlikte gerekli teknik ve idari tedbirleri alma konusunda müşterek olarak sorumludur.

Ancak, KVKK'da düzenlenen sorumluluk halleri sonuca bağlı değildir; veri güvenliğinin sağlanması yükümlülüğü, mutlak bir sonucu gerekli kılmaz. Bu durum, veri sorumlusunun üzerine düşen görevleri yapmakla sorumluluktan kurtulabileceği anlamına gelir çünkü esas olan veri sorumlusunun kişinin temel hak ve özgürlükleri için gerekli değerlendirmeyi yapıp, buna uygun ve makul bir tedbiri almasıdır.

Ancak ilgili hükmün kusur sorumluluğu mu yoksa özen sorumluluğu niteliği mi taşıdığı hususu uygulamada yine de büyük önem taşımaktadır. Nitekim kişisel

verilerin ihlali bağlamında yaşanan en büyük sorunlardan birisi de ispat konusundadır. Şayet veri sorumlusunun tazminat yükümlülüğü kusur sorumluluğu niteliğindeyse, veri sorumlusunun kusurunu zarara uğrayan ilgili kişi ispat etmek zorunda olacak, sebep sorumluluğu halinde ise kural olarak zararın meydana gelmesi, veri sorumlusunun özensiz davrandığına işaret edecektir. Dolayısıyla ikinci ihtimalde ilgili kişi hukuka aykırı fiili ve zararını ispat etmekle yetinebilecek, özenli davrandığını ispat yükü ise veri sorumlusuna ait olacaktır.[371]

Kişisel verilerin güvenliğinin sağlanması araçlarından bir diğeri olan bilgi güvenliği GDPR'a göre üç temelden oluşmaktadır. Bunlar; gizlilik, bütünlük ve erişilebilirliktir. KVKK'daki tanımda ise sadece gizlilik unsuru yer edinmiştir. Bilgi güvenliğinin sağlanmasına yönelik uygulanacak eylemler, veri güvenliğinin sağlanması için uygulanacak eylemlerle paraleldir.

GDPR'da düzenlenen veri işleme güvenliği hükmü, teknik ve idari önlemleri detaylıca ve somutlaştırılarak ele alırken; KVKK'da GDPR'ın aksine oldukça genel bir düzenleme söz konusudur ve ne gibi teknik ve idari önlemlerin alınabileceği tek tek belirtilmemiştir.

KVKK'da farklı düzenlenen bir diğer yükümlülük ise GDPR'da yer alan veri ihlal bildirimi başlığıdır.

KVKK bakımından veri ihlali, kişisel bilgilerin üçüncü kişiler tarafından ele geçirilmesi ve bu ele geçirilmenin kanuni olmayan yollarla gerçekleşmesi olarak ifade edilmektedir ve "kanuni olmayan yollarla" ibaresi ile hukuka uygun olmayan tüm durumlar kapsamaktadır. Buna halde, bir veri ihlali durumunda veri sorumlusunun bu durumu en kısa sürede ilgili kişiye ve Kurul'a bildirmesi gerekir.

EDPD Kılavuz İlkeler uyarınca ise veri sorumlusu üçüncü bir kaynak tarafından olası bir ihlal hakkında bilgilendirildiğinde bu durumu soruşturması gerekir. Veri sorumlusunun bu soruşturmaya mümkün olan en kısa sürede başlaması ve bir ihlalin gerçekleşip gerçekleşmediğinin makul bir kesinlik derecesinde tespit etmesi

[371] Çekin, Veri Hukuku, s. 270.

gerekmektedir. Bu tespit sonrası veri ihlalinin aşırı gecikme olmaksızın ve mümkün olduğu hallerde en geç 72 saat içerisinde bildirilmesi gerekir. İhlalin başladığı tarih, veri işleyenin bu ihlali tespit ettiği an kabul edilir. Veri İhlali Bildirim Formu'nda istenen her bilgi anında sağlanamıyor ise ilk olarak veri sorumlusunun elindeki bilgileri İlk Bildirim olarak sunması, sonra aşamalı olarak diğer bilgileri de Takip Bildirimi olarak sunması gerekir. Kurul tarafından Veri sorumlusunun veri ihlallerine dair bilgileri, ihlalin etkilerini ve aldığı önlemleri raporlaması beklenmektedir.

GDPR uyarınca da veri işleyenin veri ihlalini tespit etmesi durumunda "hiçbir gecikmeye yer vermeksizin" veri sorumlusuna bildirim yükümlülüğü bulunmakta olup bu bildirim için belirli bir süre öngörülmemiştir. Tıpkı KVKK'da olduğu gibi GDPR'da da hem ilgili denetim kuruluna hem de ilgili kişiye yapılacak bildirim açıkça düzenlenmiştir. GDPR uyarınca veri sorumlusu 72 saat içinde bildirim yapamazsa gecikmeye ilişkin sebeplerini de bildiriminde belirtmelidir.

GDPR uyarınca ise bir kişisel veri ihlali olması durumunda gerçek kişilerin hakları ve özgürlükleri açısından bir risk oluşuyor ise veri sorumlusu ihlali etkili veri koruma otoritesine bildirmelidir. KVKK'dan farklı olarak GDPR, temel hak ve özgürlüklere zarar veren veri ihlallerini zarar bakımından riskli ve yüksek riski olarak iki ayrı aşamada değerlendirmektedir ve ilgili kişilerin hak ve özgürlükleri açısından bir riske sebep vermesinin düşük ihtimalli olduğu durumları bildirim yükümlülüğünün dışında tutmuştur.

Başta olası bir risk oluşturmayan veri ihlali zaman içerisinde risk taşır bir hale dönüşürse bildirim yükü doğacağından veri sorumlusunun yeniden bir değerlendirme yapması gerekir.

Oysaki KVKK'da bu şekilde bir risk ayrıma gidilmediğinden risk değerlendirmesi yapılması söz konusu değildir. Bu husus ne maddenin lafzından anlaşılabilmektedir, ne de Kurul'un yayımları ve kararları ile böyle bir ayrım ortaya konulmuştur.

Kanaatimizce, KVKK'daki risk taşımayan veri ihlallerinin de bildirilmesi yükümlülüğü, Kurum'un incelemesi gereken dosya yükünü artırmakta, daha yüksek

bir risk barındıran bazı olayların incelenmesini geciktirme ihtimali yaratmaktadır. Bu sonuç ise ilgili kişilerin korunması amacıyla örtüşmemektedir. Bu bakımdan GDPR'ın bildirim yükümlülüğünde risk merkezli yaklaşımını doğru bulmaktayız.

Bildirim yükümlülüğünde risk ayrımı benimsemeyen KVKK'ya tabi veri sahipleri için bildirim yorgunluğun had safhada olması beklenirken; çok fazla bildirim aldığını ileri süren veri sahiplerinin yok denecek kadar az olması, tarafımızca bildirim yükümlülüğü konusunda Kanun'un yeteri kadar uygulanabilir olmadığı sonucuna bağlanmaktadır.

KAYNAKÇA

Akıncı, Ayşe Nur, **Avrupa Birliği Genel Veri Koruma Tüzüğü'nün Getirdiği Yenilikler Ve Türk Hukuku Bakımından Değerlendirilmesi**, T.C. Kalkınma Bakanlığı İktisadi Sektörler ve Koordinasyon Genel Müdürlüğü Çalışma Raporu 6, Haziran 2017.

Anı, Nevzat Ali, **Kişisel Verilerin İşlenmesi ve Açık Rıza,** Yayınlanmamış Yüksek Lisans Tezi, İstanbul Üniversitesi, İstanbul, 2018.

Avcı, **Yasemin, Kişisel Verilerin Korunması**, Yayınlanmamış Yüksek Lisans Tezi, Selçuk Üniversitesi, Konya, 2019.

Ayözger Öngün, Çiğdem, **Kişisel Verilerin Korunması Hukuku Elektronik Haberleşme Sektörüne İlişkin Özel Düzenlemeler Dahil**, Ertem Basım Yayın Dağıtım San. Tic. Ltd. Şti., 2. Baskı, Ankara, 2019.

Bakırel, Nur Buğçe, **Veri Sorumlusu Ve Veri İşleyen Arasındaki Sorumluluk Paylaşımının Avrupa Birliği Genel Veri Koruma Tüzüğü ve Kişisel Verilerin Korunması Kanunu Çerçevesinde Değerlendirilmesi**, Yayınlanmamış Yüksek Lisans Tezi, Hacettepe Üniversitesi, Ankara, 2020.

Baskın, Onur, **Türk Hukuku Bakımından Kişilik Hakkı Kapsamında Kişisel Verilerin Korunması**, Seçkin Yayıncılık, Ankara, 2021.

Blythe, John M, **Cyber Security In The Workplace: Understanding and Promoting Behaviour Change,** Conference: Proceedings of CHItaly 2013 Doctoral Consortium, 2013.

Budak, Özlem, **Kişisel Verilerin KVKK ve GDPR Kapsamında Yurt Dışına Aktarılması**, Yayınlanmamış Yüksek Lisans Tezi, Marmara Üniversitesi, İstanbul, 2023.

Bulut, Metin, **Özel Bir Hukuksal Koruma Ve Veri Kategorisi Alanı: Hassas Kişisel Veriler**, Ankara Barosu Dergisi, Cilt 78, Sayı 3, 2020, ss. 99-150.

Burda, Jan, **The Principle of Proportionality in EU Law,** Yayınlanmamış Yüksek Lisans Tezi, Masaryk Üniversitesi, 2018-2019.

Canbek, Gürol / Sağıroğlu, Şeref, **Bilgi, Bilgi Güvenliği ve Süreçleri Üzerine Bir İnceleme**, Politeknik Dergisi Journal of Polytechnic, Cilt 9, Sayı 3, 2006.

Çekin, Mesut Serdar, **Avrupa Birliği Hukukuyla Mukayeseli Olarak 6698 Sayılı Kanun Çerçevesinde Kişisel Verilerin Korunması Hukuku,** On İki Levha Yayıncılık, 2. Baskı, Ekim 2019.

Çekin, Mesut Serdar, **Veri Hukuku**, On İki Levha Yayıncılık, 2. Baskı, Ekim 2019. ["Çekin, Veri Hukuku"].

Çelikel, Serdar, **Kişisel Verilerin Korunması Hukuku Kapsamında Veri Sorumlusu ve Veri Sorumlusunun Yükümlülükleri,** Doktora Tezi, Ankara Üniversitesi, Ankara, 2021.

Dal, Ufuk, **Avrupa Birliği Genel Veri Koruma Tüzüğü'nün Ülke Dışı Uygulama Yetkisi ve Bu Yetkinin Uluslararası Hukukta Meşruiyeti**, Kişisel Verileri Koruma Dergisi, Cilt 1, Sayı 1, 2019, ss. 21-33.

Develioğlu, Hüseyin Murat, **6698 sayılı Kişisel Verilerin Korunması Kanunu ile Karşılaştırmalı Olarak Avrupa Birliği Genel Veri Koruma Tüzüğü uyarınca Kişisel Verilerin Korunması Hukuku,** 1. Baskı, On İki Levha Yayıncılık, İstanbul, 2017.

De-Yolande, M'Bia Hortense; Doh-Djanhoundji, Théo; Constant, Gabo Yves, **Breach Notification in the General Data Protection Regulation**, Université Virtuelle de Côte d'Ivoire, Abidjan, Cote d'Ivoire, 2023.

Dinç, Engin, **Kişisel Verilerin Korunmasında Uluslararası Düzenlemeler Ve Türkiye'nin Durumu**, Yüksek Lisans Tezi, Dicle Üniversitesi, Diyarbakır, 2006.

Dülger, Murat Volkan, **Kişisel Verilerin Korunması Hukuku**, Hukuk Akademisi Eğitim ve Yayıncılık Ltd. Şti, 1. Baskı, İstanbul, Ocak 2019.

Ersoy Kekevi, Çiçek, **Genel Kavramlar**, Kişisel verilerin Korunmasına Akademik Bakış KVKK Akademi Derleme Çalışması, Kişisel Verilerin Koruma Kurumu, Yayın No: 42, Ankara, 2023.

Geko, Melisa; Tjoa, Simon, **An Ontology Capturing the Interdependence of the General Data Protection Regulation (GDPR) and Information Security,** The Central European Cybersecurity Conference, No: 19, 2018.

Gürpınar, Damla, **Kişisel Verilerin Korunmasından Doğan Hukuki Sorumluluk**, Dokuz Eylül Üniversitesi Hukuk Fakültesi Dergisi, Cilt 19, Sayı 3, 2017, s. 679-694.

Halıcıoğlu, Mesut, **Türk Hukukunda Veri Sorumlusu**, Yüksek Lisans Tezi, Hacettepe Üniversitesi, Ankara, 2019.

Henkoğlu, Türkay, **Kişisel Verileriniz Ne Kadar Güvende? Bilgi Güvenliği Kapsamında Bir Değerlendirme**, Arşiv Dünyası Dergisi, Sayı 18-19, 2017, ss. 36-47.

Kapancı, Kadir Berk, **Ahlaka Aykırı Bir Fiille Kasten Verilen Zararın Tazmini (TBK 49 II),** Vedat Kitapçılık, İstanbul, 2016, s. 35-36.

Kapancı, Kadir Berk, **Gelişen Teknolojiler Ve Hukuk Iv : Siber Güvenlik**, Siber Güvenlik Ve Özel Hukuk Sorumluluğu Üzerine Değerlendirmeler, On İki Levha Yayıncılık, 2023, s.49-83.

Kara, Şahin, **Veri Kurtarma Yöntemlerinin Başarımlarının Değerlendirilmesi**, Yüksek Lisans Tezi, Fırat Üniversitesi, 2013.

Kaya, Cemil, **Avrupa Birliği Veri Koruma Direktifi Ekseninde Hassas (Kişisel) Veriler ve İşlenmes**", İÜHFM, Cilt 69, Sayı 1-2, 2011, ss. 317 – 334.

Kılınç, Doğan, **Anayasal Bir Hak Olarak Kişisel Verilerin Korunması**, Ankara Üniversitesi Hukuk Fakültesi Dergisi, Cilt 61, Sayı 3, 2012, ss. 1089-1172.

Korkmaz, İbrahim, **Kişisel Verilerin Korunması Kanunu Hakkında Bir Değerlendirme**, Türkiye Barolar Birliği Dergisi, Sayı 124, Mayıs-Haziran 2016, ss. 81-152.

Koseff, Jeff, **Defining Cybersecurity Law**, Iowa Law Review, Cilt 103, Sayı 985, 2018.

Kuner, Christopher, Lee A Bygrave, Christopher Docksey, Laura Drechsler, **The EU General Data Protection Regulation (GDPR): A Commentary, "GDPR Article 32" Section**", Oxford University Press, 2020.

Küzeci, Elif, **Kişisel Verilerin Korunması**, Oniki Levha Yayınları, 4. Baskı, İstanbul, 2018.

Lloyd, Ian J., **Information Texhnology Law**, Oxford University Press, 7. Bası, Oxford, 2014.

Oğuzman, M. Kemal; Oktay, Saibe, **Kişiler Hukuku (Gerçek ve Tüzel Kişiler),** Filiz Kitabevi, 15. Baskı, 2015.

Özbek, Veli Özer, **Elektronik Ortamda Saklı Bulunan Verilerin Ceza Muhakemesinde Delil Niteliği ve Değerlendirilmesi**, İÜHFM, Cilt 59, Sayı 1 -2, 2001, ss. 181-202.

Özdemir, Hayrunisa, **Elektronik Haberleşme Alanında Kişisel Verilerin Özel Hukuk Hükümlerine Göre Korunması**, Ankara, Seçkin Yayıncılık, 2009.

Özkan, Oğulcan, **Kişisel Verilerin Korunması**, Yayınlanmamış Yüksek Lisans Tezi, Ankara Üniversitesi, Ankara, 2020.

Öztekin, Mehmet Semih, **Kişisel Veri Güvenliğine İlişkin Yükümlülüklerin Yerine Getirilmemesi Kabahati,** Yayınlanmamış Yüksek Lisans Tezi, Galatasaray Üniversitesi, İstanbul, Haziran, 2023.

Portuese, Aurelien, **Principle of Proportionality as Principle of Economic Efficiency**, European Law Journal, Cilt 19, Sayı 5, 2013.

Quinn, Paul; Malgieri, Gianclaudio, **The Difficulty of Defining Sensitive Data – The Concept of Sensitive Data in the EU Data Protection Framework**, German Law Journal, 2020, (Son güncelleme tarihi 2021).

Sahar, Noor Talaat Azzat, **6698 Sayılı Kişisel Verilerin Korunması Kanununda Yer Alan Temel Kavramlar ile Terminoloji**, Selçuk Üniversitesi Adalet Meslek Yüksekokulu Dergisi, 2011, ss. 35-52.

Sevindi, Nur Sena; Ordu, Muhammed Emin, **AB Ve Türk Hukukunda Veri İhlalinin Tespiti Ve Bildirim Süresinin Karşılaştırmalı Değerlendirmesi,** Kişisel Verileri Koruma Dergisi, Cilt 5, Sayı 1, 2023, ss. 12-22.

Smedinghoff, Thomas J., **The State of Information Security Law: A Focus on the Key Legal Trends**, Locke Lord LLP, 2008.

Şahin, Osman, **Elektronik Haberleşme Sektöründe Kişisel Verilerin İşlenmesi, Saklanması ve Gizliliğin Korunması**, Bilgi Teknolojileri ve İletişim Kurumu, Bilişim Uzmanlığı Tezi, Ankara, Haziran, 2011.

Şen, Ersan, **Kişisel Verilerin Korunması Kanunu Tasarısı'nın Anayasa ve Türk Ceza Kanunu Hükümleri Çerçevesinde Değerlendirilmesi,** İstanbul Barosu Dergisi, Cilt 83, Sayı 3, 2009, ss. 1197-1214.

Tekerek, Mehmet, **Bilgi Güvenliği Yönetimi**, KSÜ Fen ve Mühendislik Dergisi, Cilt 1 Sayı 11, 2008, ss. 132-137.

Tezcan, Durmuş, **Bilgisayar Karşısında Özel Hayatın Korunması**, Anayasa Yargısı, Ankara 1991.

Tunca, Sibel, **Modern Çağda Siber Güvenlik Kavramı**, Dumlupınar Üniversitesi İktisadi ve İdari Bilimler Fakültesi Dergisi, Sayı: 3-4, 2019, s. 1-7.

Uçak, Murat, **Civil Liability Of Data Controller For Unlawful Processıng Of Personal Data**, Yüksek Lisans Tezi, İstanbul Medeniyet Üniversitesi, 2019.

Zor, Abdülhamit, **Veri Sorumlusunun Yükümlülükleri Ve Bu Yükümlülükleri İhlalinden Doğan Özel Hukuk Sorumluluğu**, Yüksek Lisans Tezi, İstanbul Üniversitesi, İstanbul, 2020.

KARARLAR

AEPD (Spain) - EXP202104875, GDPRhub.

CNIL (France) - SAN-2023-023," GDPRhub.

Datatilsynet (Denmark) - 2021-442-13989, GDPRhub.

Datatilsynet (Norway) - 21/03126. (2023, March 24). GDPRhub.

UODO (Poland) - DKN.5131.33.2021. (2022, March 2). GDPRhub.

Kişisel Verileri Koruma Kurulu, 31.01.2018 Tarih, 2018/10 Sayılı Kararı.

Kişisel Verileri Koruma Kurulu'nun 19.11.2018 tarihli ve 2018/131 sayılı kararı.

Kişisel Verileri Koruma Kurulu'nun 24.01.2019 tarihli 2019/10 sayılı kararı. ["KVKK, 2019/10 sayılı Karar"].

Kişisel Verileri Koruma Kurulu'nun 14.02.2019 tarihli 2019/23 sayılı kararı.

Kişisel Verileri Koruma Kurulu'nun 02.05.2019 tarihli 2019/122 sayılı kararı.

Kişisel Verileri Koruma Kurulu'nun 18.09.2019 tarihli 2019/271 sayılı kararı.

Kişisel Verileri Koruma Kurulu'nun 18.09.2019 tarihli ve 2019/273 sayılı kararı.

Kişisel Verileri Koruma Kurulu, 30.01.2020 Tarih, 2020/71 Sayılı Kararı.

Kişisel Verileri Koruma Kurulu'nun 27.02.2020 tarihli ve 2020/166 sayılı kararı.

Kişisel Verileri Koruma Kurulu'nun 13.02.2020 tarihli 2020/124 sayılı kararı.

Kişisel Verileri Koruma Kurulu'nun 03.03.2020 tarihli ve 2020/191,192,193,194 sayılı kararları.

Kişisel Verileri Koruma Kurulu'nun 27.04.2021 tarihli 2021/427 sayılı kararı.

Kişisel Verileri Koruma Kurulu'nun 06.07.2021 tarihli 2021/670 sayılı kararı.

Kişisel Verileri Koruma Kurulu'nun 03.09.2021 tarihli 2021/889 sayılı kararı.

Kişisel Verileri Koruma Kurulu'nun 21.09.2021 tarihli 2021/962 sayılı kararı.

Kişisel Verileri Koruma Kurulu'nun 09.12.2021 tarihli 2021/1243 sayılı kararı.

Kişisel Verileri Koruma Kurulu'nun 06.01.2022 tarihli ve 2022/13 sayılı kararı.

Kişisel Verileri Koruma Kurulu'nun 17.03.2022 tarihli 2022/243 sayılı kararı.

Kişisel Verileri Koruma Kurulu'nun 24.08.2023 tarihli 2023/1465 sayılı kararı.

ELEKTRONİK KAYNAKLAR

https://sozluk.gov.tr/

https://en.oxforddictionaries.com/

https://gdprhub.eu/index.php?title=Welcome_to_GDPRhub

https://gdpr-info.eu/

https://www.ab.gov.tr/siteima.g.e.,s/resimler/Nihai-ABB-HCDB-GDPR.pdf

https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:en:HTML

https://www.ab.gov.tr/siteima.g.e.,s/resimler/Nihai-ABB-HCDB-GDPR.pdf

https://www.privacy-regulation.eu/en/recital-78-GDPR.htm

https://data2.eu/en/gdpr/what-technical-and-organisational-measures-do-we-need-to-take

https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A31995L0046

Anna Levitina, "Understanding GDPR Technical and Organisational Measures", Logan & Partners Law Office, Elektronik Kaynak, Ekim 2022. Bkz. https://www.loganpartners.com/understanding-gdpr-technical-and-organisational-measures/?utm_source=mondaq&utm_medium=syndication&utm_term=Privacy&utm_content=articleoriginal&utm_campaign=article

British Legal Technology Forum, "The Main Differences Between The DPD And The GDPR And How To Address Those Moving Forward", London UK, 2017, s. 1. Bkz. https://britishlegalitforum.com/wp-content/uploads/2017/02/GDPR-Whitepaper-British-Legal-Technology-Forum-2017-Sponsor.pdf

Kişisel Verileri Koruma Kurumu (KVKK), "Kanun Kapsamındaki Hak ve Yükümlülükler", 23 Nisan 2019. https://www.kvkk.gov.tr/Icerik/4192/Kanun-Kapsamindaki-Hak-ve-Yukumlulukler ["KVKK, Hak ve Yükümlülükler"]

Kişisel Verileri Koruma Kurumu, "İlgili Kişi Kimdir?", Bkz. https://www.kvkk.gov.tr/Icerik/2034/Ilgili-Kisi-Kimdir

Kişisel Verileri Koruma Kurumu (KVKK), "Veri Sorumlusu ve Veri İşleyen", (Çevrimiçi), https://www.kvkk.gov.tr/SharedFolderServer/CM

Leonard Willis, 'Very Brief Introduction to GDPR', American Bar Association. Bkz. https://www.americanbar.org/groups/litigation/resources/newsletters/minority-trial/very-brief-introduction-gdpr-

recitals/#:~:text=As%20mentioned%2C%20the%20GDPR%20consists,context%20to%20supplement%20the%20articles.

TBMM, Kanun Tasarısı, 2016. https://www5.tbmm.gov.tr/sirasayi/donem26/yil01/ss117.pdf

Yaşar K. Canpolat, "KVKK ve GDPR ekseninde "Veri İhlali" kavramı", Canpolat Legal, 2018. Elektronik Kaynak, Bkz. https://medium.com/canpolat-legal/kvkk-ve-gdpr-kapsam%C4%B1nda-veri-i%CC%87hlali-nedir-c2450ff718e9

DİĞER KAYNAKLAR

Article 29 Data Protection Working Party Opinion 4/2007 on the Concept of Personal Data, Haziran 2007, 01248/07/EN, WP 136.

Article 29 Working Party, Opinion 1/2010 on the Concepts of "Controller" and "Processor".

Avrupa Konseyi, "Explanatory Report to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data", Strasbourg 1981.

EDPB, "Guidelines 09/2022 on personal data breach notification under GDPR", Mart 2023, (Versiyon 2.0) ["EDPB, Kılavuz İlkeler"].

IT Governance Prıvacy Team, "EU General Data Protection Regulation (GDPR): An Implementation and Compliance Guide - Second Edition", IT Governance Yayımları, 2. Baskı, 2017.

Kişisel Verileri Koruma Kurumu, "100 Soruda Kişisel Verilerin Korunması Kanunu", KVKK Yayınları, Ankara, 2019 ["KVKK, Soru Cevap"].

Kişisel Verileri Koruma Kurumu, "6698 Sayılı Kişisel Verilerin Korunması Kanunu Hakkında Doğru Bilinen Yanlışlar, KVKK Yayınları, Ankara, 2019 ["KVKK, Doğru Bilinen Yanlışlar "].

Kişisel Verileri Koruma Kurumu, "Kişisel Verilerin İşlenmesine İlişkin Temel İlkeler", KVKK Yayınları, Ankara, 2019. ["KVKK, Temel İlkeler"].

Kişisel Verileri Koruma Kurumu, "Madde ve Gerekçesi ile Kişisel Verilerin Korunması Kanunu (Bilgi Notu) ve Kişisel Verilerin Korunmasına İlişkin Terimler Sözlüğü, KVKK Yayınları, Ankara, 2019. ["KVKK, Gerekçe ve Terimler Sözlüğü"].

Kişisel Verileri Koruma Kurumu, "Örneklerle Kişisel Verilerin Korunması, KVKK Yayınları, Ankara 2019. ["KVKK, Örneklerle Kişisel Verilerin Korunması"].

Kişisel Verileri Koruma Kurumu, 6698 Sayılı Kişisel Verilerin Korunması Kanunu Hakkında Doğru Bilinen Yanlışlar – 2, KVKK Yayınları, Ankara, 2020. ["KVKK, Doğru Bilinen Yanlışlar 2"].

Kişisel Verileri Koruma Kurumu, Kişisel Veri İhlali Bildirim Formu Kılavuzu, KVKK Yayınları, Ankara, 2019. ["KVKK, Bildirim Formu Kılavuzu"].

Kişisel Verileri Koruma Kurumu, Kişisel Verilerin Korunması Kanunu Hakkında Sıkça Sorulan Sorular, KVKK Yayınları, Ankara, 2019. ["KVKK, Sıkça Sorulan Sorular"].

Kişisel Verilerin Korunması Kurumu, Kişisel Verilerin Korunması Alanında Uluslararası ve Ulusal Düzenlemeler, KVKK Yayınları, Ankara 2018. [“KVKK, Düzenlemeler”].

Kişisel Verilerin Korunması Kurumu, Kişisel Verilerin Korunması Kanununa İlişkin Uygulama Rehberi, KVKK Yayınları, 2019, s. 56. [“KVKK, Uygulama Rehberi”].

OneTrust DataGuidance, Esin Attorney Partnership; “Comparing Privacy Laws: GDPR v. LPPD”, Nisan 2023.