İSTANBUL BİLGİ ÜNİVERSİTESİ
SOSYAL BİLİMLER ENSTİTÜSÜ
BİLİŞİM VE TEKNOLOJİ HUKUKU YÜKSEK LİSANS PROGRAMI

AVRUPA BİRLİĞİ GENEL VERİ KORUMA REGÜLASYONUNDAKİ VERİ KORUMA GÖREVLİSİ KAVRAMI İLE TÜRK HUKUKUNDAKİ VERİ SORUMLUSU TEMSİLCİSİ VE İRTİBAT KİŞİSİ KAVRAMLARININ KARŞILAŞTIRILMASI

Şeyma BAYRAK
115691017

Dr. Öğr. Üyesi Nilgün BAŞALP YILDIRIM

İSTANBUL
2019

Avrupa Birliği Genel Veri Koruma Regülasyonu'ndaki Veri Koruma Görevlisi Kavramı ile Türk Hukuku'ndaki Veri Sorumlusu Temsilcisi ve İrtibat Kişisi Kavramlarının Karşılaştırılması

Comparison of the Data Privacy Officer under General Data Protection Regulation to the Representative and the Contact Person under Turkish Law

Şeyma Bayrak
115691017

Tez Danışmanı : **Dr. Öğr. Üyesi Nilgün BAŞALP YILDIRIM** .....
İstanbul Bilgi Üniversitesi

Jüri Üyeleri : **Doç. Dr. Leyla KESER BERBER** .....
İstanbul Bilgi Üniversitesi

Dr. Öğr. Üyesi Mehmet Bedii KAYA .....
Yıldırım Beyazıt Üniversitesi

Tezin Onaylandığı Tarih : 01.04.2019
Toplam Sayfa Sayısı : 130

Anahtar Kelimeler (Türkçe)
1) Avrupa Birliği Genel Veri Koruma Regülasyonu
2) Kişisel Verilerin Korunması Kanunu
3) Veri Koruma Görevlisi
4) Veri Sorumlusu
5) Veri İşleyen

Anahtar Kelimeler (İngilizce)
1) General Data Protection Regulation
2) Protection of Personal Data
3) Data Privacy Officer
4) Data Controller
5) Data Processor

İÇİNDEKİLER

KISALTMALAR

AB	Avrupa Birliği (European Union-EU)
ABD	Amerika Birleşik Devletleri
AİHM	Avrupa İnsan Hakları Mahkemesi
AİHS	Avrupa İnsan Hakları Sözleşmesi
Art. 29 WP	Article 29 Working Party
BM	Birleşmiş Milletler (The United Nations-UN)
CD	Compact Disc
DPO	Data Privacy Officer
EUROJUST	European Union Agency for Criminal Justice Cooperation
EUROPOL	European Union Agency for Law Enforcement Cooperation
FTC	Federal Trade Commission
GDPR	General Data Protection Regulation
IAPP	International Associaton Privacy Professionals
ICO	Information Commissioner's Office
ISO	International Organization for Standardization
IT	Information Technology
İK	İnsan Kaynakları
Kanun	6698 Sayılı Kişisel Verileri Koruma Kanunu
Kurul	Kişisel Verileri Koruma Kurulu
Kurum	Kişisel Verileri Koruma Kurumu
KVKK	Kişisel Verileri Koruma Kanunu
OECD	Organisation for Economic Co-operation and Development
Opt-in	Opted in for receiving
Opt-out	Opted out for not receiving
Regülasyon	Avrupa Birliği Genel Veri Koruma Regülasyonu
Sicil	Veri Sorumluları Sicili
TBK	6098 Sayılı Türk Borçlar Kanunu
TBMM	Türkiye Büyük Millet Meclisi
TC	Türkiye Cumhuriyeti

TCK	5237 Sayılı Türk Ceza Kanunu
Tebliğ	Aydınlatma Yükümlülüğünün Yerine Getirilmesinde Uyulacak Usul ve Esaslar Hakkında Tebliğ
TMK	4721 Sayılı Türk Medeni Kanunu
Yönerge	95/46/EC Sayılı Yönerge
Yönetmelik	Veri Sorumluları Sicili Hakkında Yönetmelik

ŞEKİL LİSTESİ

ABSTRACT

Present study defines the designation, tasks and position of the Data Privacy Officer (DPO) which is regulated in Genaral Data Protection Regulation (GDPR). It also explains the responsabilities of the data controller in "Kişisel Verileri Koruma Kanunu (KVKK)" in Turkish Law that does not have DPO role. This study discusses the possible need of DPO in today and the future, in Turkish Law.

In the first chapter, the works that European Union (EU) has made until the GDPR about data protection are demonstrated. This study compares Directive 95/46/EC and the GDPR in terms of data protection regulations. Present study defines the contributions of GDPR and DPO which is the most significant change with this law, especially. To describe the deficiencies in Turkish Law, the designation, position and tasks of DPO are explained in the second and the third chapter.

In the second chapter, the studies within the scope of data protection law in Turkish law are explained and the obligations imposed on the data controller were analyzed in detail. To the comparison of Turkish Law and EU Law which is analyzed in the third chapter, the subjects who have the obligations as similar as the DPO's obligations are represented in Turkish Law.

In the third and final section, the reason for the differences between the current and the previous works is stated by a comparison between the two legal orders where data protection law is located in both legal orders. The benefits of having a DPO within a business is stated. In the context of Turkish law, it has been stated how enterprises that have not been assigned DPO can resolve this deficiency. Finally, opinions on whether Turkish law needs a DPO, how to address this need, legal regulations and a legal regulation that will regulate DPOs within the scope of compliance with the law are explained.

ÖZET

Bu çalışma, AB Genel Veri Koruma Regülasyon'u (Regülasyon) kapsamında düzenlenen "Data Privacy Officer (DPO)" yani Türkçe isimlendirmesiyle "Veri Koruma Görevlisi"nin Regülasyon kapsamında sahip olması gereken özellikleri, görevi ve konumu ile 6698 Sayılı Kişisel Verileri Koruma Kanunu (Kanun) içerisinde yer verilmeyen bu kurumun Türk Hukuku kapsamında oluşturacağı eksikliklerin belirlenmesi, veri sorumlusuna yüklenen görev, sorumluluk ve yükümlülüklerin, Veri Koruma Görevlisi olmadan ne şekilde yerine getirildiği ve Türk Hukuku'nun Veri Koruma Görevlisi kurumuna duyacağı muhtemel ihtiyacın belirlenmesini tartışır.

İlk bölümde, AB'nin Regülasyon yürürlüğe girene dek gerçekleştirdiği veri koruma hukuku kapsamındaki çalışmalar, 1995 yılında kabul edilen 95/46/EC sayılı AB Veri Koruma Yönergesi (Yönerge) ve Regülasyon'un karşılaştırması, Regülasyon'un getirdiği yeniliklerin genel ve kısa bir özeti, veri sorumlusu ve veri işleyene yüklenen yükümlülükler ve özellikle Regülasyon'un getirdiği yeniliklerden biri olan Veri Koruma Görevlisi anlatılmıştır. Veri Koruma Görevlisi'nin sahip olması gereken özellikler, görevleri ve Regülasyon kapsamındaki konumu, ikinci ve üçüncü bölümde anlatılan, Türk Hukuku'ndaki eksikliklerin net bir şekilde belirlenebilmesi adına detaylı bir şekilde anlatılmıştır.

İkinci bölümde, Türk Hukuku'nda veri koruma hukuku kapsamındaki çalışmalar anlatılarak veri sorumlusuna yüklenen yükümlülüklere detaylı olarak yer verilmiş ve üçüncü bölümde yapılacak değerlendirme için benzer yükümlülükler ve Kanun ve ilgili mevzuat kapsamında yer verilen veri sorumlusu temsilcisi ve irtibat kişileri kavramları irdelenerek Veri Koruma Görevlisi kurumu karşısındaki konumu anlatılmıştır.

Üçüncü ve son bölümde ise, her iki hukuk düzeni açısından bir karşılaştırma ile önceki yıllarda yapılan çalışmaların günümüzde her iki hukuk düzeninde veri koruma hukukunun nerede konumlandırıldığı anlatılarak, güncel yasal düzenlemeler arasındaki farklılıkların nedeni belirtilmiştir. Veri Koruma Görevlisi'nin bir veri sorumlusuna bağlı olarak, görevleri kapsamında ne gibi faydalar sağlayacağı anlatılmış ve Türk Hukuku kapsamında Veri Koruma Görevlisi atanmamış veri sorumlularının bu eksikliği ne şekilde giderebileceği belirtilmiştir. Son olarak, Türk Hukuku'nun sahip olduğu veri sorumlusu temsilcisi ve irtibat kişisi kurumlarının görevlerinin Veri Koruma Görevlisi kurumunun görevleriyle örtüşüp örtüşmediği, Türk Hukuku'nun daha detaylı bir düzenlemeye ihtiyaç duyup duymadığı, bu ihtiyacın ne şekilde giderilebileceği, yasal düzenlemelerin ve veri sorumlularının Kanun'a uyumluluğu kapsamında Veri Koruma Görevlisi'ni düzenleyecek bir yasal düzenlemenin oluşturulması için doğru zamanın nasıl belirleneceği konusunda fikirlere yer verilmiştir.

1. GİRİŞ

Gün geçtikçe gelişen teknoloji ile hayatın değişimi her sektörü etkilemiştir. Her bir sektör için bu gelişmeler ile gelecek arasında bağlantılar kurulmuş, çalışmalar yapılmıştır. Ancak tüm bu gelişmelerin her sektör için tek bir ortak noktası olduğu unutulmamalıdır. Bu ortak nokta kişisel verilerin korunmasıdır. Hangi sektörde olunursa olunsun, veriyi işleyen ya da verisi işlenen kişi için dikkate değer ve oldukça önemli bir ortak noktadır. Veri işleme sürecinin hangi tarafında olursa olsun tüm kişiler için verilerin işlenmesi olağan, gündelik bir süreç halini almıştır. Bu nedenle verilerin işlenmesinin belirli kurallar altına alınması ve verilerin korunması adına da belirli yöntemlerin belirlenmesi için düzenlemeler oluşturulması gerekli hale gelmiştir.

Verilerin korunması adına oluşturulan yasal düzenlemeler ile verileri işleyen ve verileri işlenen kişiler görevlerini, hak ve yükümlülüklerini bilebilecek hale gelmişlerdir. Ancak nasıl ki teknoloji sürekli gelişmeye devam ediyorsa, veri koruması adına belirlenen yasal düzenlemeler de bu gelişmelere ayak uydurmak durumundadır. Örneğin bundan 50 yıl önce verilerin yurtdışına aktarılma oranı ile günümüz oranı karşılaştırıldığında görülecek fark yasal düzenlemelerde de muhtemel eksiklikleri bize gösterebilecektir. Her yeni gelişme ile verilerin korunması alanında da yenilikler yaratmak mümkün olmayacaktır. Bu nedenle temelinde teknoloji olan bu alanda yapılacak yasal düzenlemeler, gelişmelerle uyumlu olabilecek şekilde oluşturulmalı ve güncellenebilir bir halde tutulmalıdır. Veri koruması alanında belirlenen yasal düzenlemeler ile çift yönlü düşünülebilecek sistem yaratılmıştır. Bunlardan ilki; veri sorumlularının veri koruma alanında sahip oldukları yükümlülükler ve bu yükümlülüklere uygunluğun sağlanması iken diğer taraftan da bireylerin verilerinin korunmasına ilişkin sahip oldukları haklar olarak sayılabilir[1].

[1] Paul LAMBERT, The Data Protection Officer Profession, Rules and Role, CRC Press, 2016, s. 6.

Çalışmanın ileriki bölümlerinde detaylı bir şekilde anlatılacağı üzere ülkemizde veri korumasına ilişkin yasal düzenlemeler Avrupa ve Avrupa Birliği ile karşılaştırıldığında yeni sayılabilecek bir konumdadır[2]. Bu durum göz önüne alındığında bazı eksikliklerin olması da kaçınılmaz hale gelmektedir. Bu tezde de Avrupa Birliği Genel Veri Koruma Regülasyonu (Regülasyon) ve 6698 Sayılı Kişisel Verileri Koruma Kanunu'nda (Kanun) kapsamında veri sorumlusuna yüklenen yükümlülükler incelenerek, bir Regülasyon yeniliği olan Data Privacy Officer (DPO)" yani Türkçe ifade ile Veri Koruma Görevlisi ve Kanun'da yer alan Veri Sorumlusu Temsilcisi ve İrtibat kişisi kurumlarının konumları tartışılacaktır.

[2] Bkz: s. 50.

2. AVRUPA BİRLİĞİ GENEL VERİ KORUMA REGÜLASYONU ve ÖZELLİKLE VERİ KORUMA GÖREVLİSİ

2.1.AB Genel Veri Koruma Regülasyonu

Kişisel verilerin korunması hakkı, temelde insan hakları kapsamında insanlara tanınan birçok hak ile yakından ilgilidir. Kişisel verilerin korunmasına ilişkin özel düzenlemelerin yokluğunda Avrupa İnsan Hakları Sözleşmesi (AİHS) kapsamında tanınmış haklar ile dahi kişisel verilerin korunması söz konusu olmuştur. Diğer tüm insan hakları gibi kişisel verilerin korunması hakkı da insan onuru ile bağdaşan bir haktır, bu kapsamda özel hayatın gizliliği, düşünceyi açıklama özgürlüğü, bilgi edinme hakkı, haberleşme özgürlüğü gibi başka temel hak ve özgürlüklerle kimi zaman karşılıklı destekleme, kimi zaman çatışma halinde bir hak olarak karşımıza çıkmaktadır[3].

Tüm bu ihtiyaçlar doğrultusunda Avrupa'da yerel bazlı çalışmalar sonrasında AB kapsamında kapsayıcı düzenlemeler yapılmış ve kişisel verilerin güvence altına alınması sağlanmıştır. 1995 yılında kabul edilen 95/46/EC sayılı AB Veri Koruma Yönergesi (Çalışmanın bundan sonraki bölümlerinde "Yönerge" olarak anılacaktır.) de uzun yıllar AB vatandaşlarının kişisel verilerinin korunması amacıyla yürürlükte kalmıştır. Kişisel verilerin korunması alanında AB sınırlarını aşan bir yetkiye sahip olan bu Yönerge kişisel verilerin korunması alanında bir dönüm noktası olarak değerlendirilebilir[4]. Ancak ekonomik ve teknolojik faaliyetlerin hızla gelişmesi ile verilerin toplanması, işlenmesi, saklanması gibi süreçlerin de değişime uğraması, tüm dünyada kişisel verilerin korunmasına ilişkin farkındalığın artması ve Yönergenin AB kapsamındaki üye ülkelerin her birinde ayrı bir uyumlu mevzuat öngörmesi ile yeknesaklığın olmaması ve bu farklılıkların uygulamada sorunlara yol açması sonucu yeni bir düzenleme yapma ihtiyacı hasıl olmuştur. Bu kapsamda tüm üye ülkelerde tek bir düzenlemenin

[3] Elif KÜZECİ, Kişisel Verilerin Korunması, Yenilenmiş ve Gözden Geçirilmiş 2. Baskı, Ankara, Şubat 2018, s. 62.
[4] KÜZECİ, s. 117.

geçerli olması ve uygulamadaki farklılıklardan doğan sorunların giderilmesi adına Yönerge yerine regülasyon çalışmaları gündeme gelmiştir.

Regülasyon'un amaçları şu şekilde sıralanabilir;

- Yönergenin uygulanmasında karşılaşılan problemleri giderebilmek adına yeknesak hukuk kuralları belirleme
- AB vatandaşlarının var olan haklarını daha da güçlü hale getirme
- AB vatandaşlarının dijital ortamdaki faaliyetleriyle ilgili yeni düzenlemeler belirleme
- Birden fazla AB üye devlet kapsamında faaliyet gösteren şirketler açısından idari prosedürü ve bürokrasi trafiğini azaltmak
- Şeffaflık, hesap verilebilirlik, öz denetim gibi ilkeleri geliştirmek
- Veri sorumlusu ve veri işleyenlerin sorumluluk ve yükümlülüklerini daha sıkı bir şekilde düzenlemek
- Kişisel verilerin üçüncü ülkelere transferini daha geniş bir şekilde düzenlemek
- Araştırma, yenilik ve teknolojiyi teşvik etmek, E-ticaret alanında AB'nin bütünleşmesine ve ekonomik gelişimine katkı sağlamak ve gizlilik, kişisel verilerin korunması konularına saygı duyulmasını sağlamak[5].
- Regülasyonun metninin kaleme alınışı incelendiğinde olabildiğince teknoloji nötr olarak ifade edilmiş olması göze çarpmaktadır. Bu da regülasyonun uzun süre yürürlükte kalması amacına hizmet etmek üzere regülasyonun temel özelliklerinden biri olarak görülmektedir[6].

General Data Protection Regulation (GDPR), Türkçe ifade ile; AB Genel Veri Koruma Regülasyonu (Çalışmanın bundan sonraki bölümlerinde "Regülasyon" olarak anılacaktır.) Avrupa Komisyonu 2012 yılında reform paketi gündeme

[5] Irene Loizidou Nicolaidou/ Constantinos Georgiades, "The GDPR: New Horizons, EU Internet Law Regulation And Enforcement", Cham, Switzerland, January 2017, s. 5.
[6] Shraddha KULHARI, Building-Blocks of a Data Protection Revolution, Nomos Verlag, Baden-Baden 2018, s. 38.

getirmiştir ve yoğun lobicilik faaliyetlerinin merkezi haline gelerek[7] kimi değişikliklerle birlikte Nisan 2016'da AB Konseyi ve Avrupa Parlamentosu tarafından Regülasyon kabul edilmiştir. Regülasyon 4 Mayıs 2016'da tüm üye devletlerde 25 Mayıs 2018 tarihinde doğrudan uygulanmak üzere Resmî Gazete'de yayınlanmıştır.

2.2. AB Genel Veri Koruma Regülasyonu'nun Getirdiği Yenilikler

Regülasyon, Yönerge'nin cevap vermediği konularda düzenlemeler yapmasının yanı sıra birçok yenilik getirmiş ve var olan yükümlülükler, idari ve cezai yaptırımlar konusunda da daha sıkı ve ağır şartlar içeren düzenlemelere yer vermiştir. Regülasyon ile veri sorumlularına daha fazla yükümlülük öngörülürken, bireylerin tanınan haklarla daha fazla korunması imkanını sağlamaktadır[8].

Regülasyon ile birlikte veri koruması alanına kişisel verilerin işlenmesi ve bireylerin bu konuya ilişkin sahip olduğu haklar bakımından yeni bir soluk gelmiştir. Çalışma her ne kadar Yönerge ile aynı eksende olsa da Yönerge'den farklı olarak çok daha detaylı ve problemlere cevap verebilen, üye devletlere ve AB kapsamında bulunmayan devletlere yüklediği sorumluluklarla veri koruması alanında dikkat çeken yeniliklere sahip bir çalışmadır.

Bu yeniliklerin ortaya çıkmasındaki en büyük etkenler; küreselleşen dünyada ilgili kişilerin haklarının korunmasında ortaya çıkan güçlük, gelişen teknoloji ile birlikte çağı yakalama gereksinimi, AB dışındaki ülkelere veri transferi ve AB üye ülkeleri arasında veri korumasına ilişkin yeknesak bir çalışmanın yokluğu ile çıkan uygulama farklılıkları ve bürokratik süreç temel olarak gösterilebilir.

---

[7] Konuyla ilgili akademik bir inceleme için bkz: Atikcan, E., & Chalmers, A. (n.d.). Choosing lobbying sides: The General Data Protection Regulation of the European Union. Journal of Public Policy, 1-22.

[8] GILBERT, Francoise. European data protection 2.0: new compliance requirements in sight-what the proposed EU data protection regulation means for us companies. Santa Clara Computer & High Tech. LJ, 2011, s. 818.

2.2.1. Uygulamada Yeknesaklık

Üye devletler, yönerge kurallarını, kendi iç hukuk düzenlerine nasıl aktaracakları konusunda regülasyona göre daha esnek imkanlara sahiptirler. Regülasyon ile birlikte, aktarımda esnekliğe izin vermeyen ya da kısıtlı bir şekilde izin veren daha katı bir yasal araç üye devletler için gündeme gelmiştir. Yönerge'nin üye devletlerde farklı şekillerde uygulanması, veri koruma kurallarının bölünmesine, yasal belirsizliğe ve mevzuatın, özellikle çevrimiçi faaliyetlerle ilgili olarak etkin bir koruma sağlamadığı algısına yol açmıştır. AB, veri koruma kurallarına ilişkin yaptığı yeni çalışmalarda, yönerge yerine regülasyonu tercih ederek, belirlenmiş olan veri koruma kurallarının tek bir uygulama şekli ile tüm üye devletlerde uygulanmasını tercih ettiğini açıkça göstermektedir[9]. Ancak böyle olmakla regülasyon içeresinde önemli sayıda düzenlemede üye devletlere takdir marjları da bırakılmıştır. Örneğin, çocukların kişisel verilerin sanal ortamda işlenmesine ilişkin rızaları bakımından yaş sınırı 16 olarak belirlenmekle birlikte, üye devletlerce 13 yaşa kadar indirilmesine izin verilmektedir.

Yönerge ile her bir üye devletin oluşturduğu iç hukuk metni uygulamada ciddi anlamda farklılık ortaya çıkmasına sebep olması nedeniyle yeni düzenleme regülasyon şeklinde hazırlanarak, tüm üye devletlerde tek bir hukuki metnin geçerliliği sağlanmak istenmiştir. Bu kapsamda uygulamadaki tekliğin daha sağlam temellerde uygulanması adına denetim makamlarının dahi iş birliği içinde olması için kaleme alınmış Regülasyon'un "Yeknesaklık Mekanizması" başlıklı 63. Maddesi'ne göre;

"*Bu Regülasyon'un AB dahilinde yeknesak şekilde uygulanmasına katkı sağlamak için, denetim makamları birbirleri ile ve ilgili hallerde Komisyon ile, bu Kısım'da öngörülen yeknesaklık mekanizması aracılığıyla, iş birliği yapar*."

[9] NICOLADOU/GEORGIADES, s. 5-6.

2.2.2. Yer Bakımından Uygulanma

Regülasyon ile birlikte getirilen bir diğer yenilik ise 3. maddede yer alan "Yer bakımından uygulanma" başlığı altında yer almaktadır.

Buna göre;

1. Bu Regülasyon kişisel veri işlemenin Birlik dahilinde gerçekleştirilip gerçekleştirilmediğine bakılmaksızın, kişisel verilerin bir veri sorumlusunun veya veri işleyenin Birlik dahilindeki merkezinin faaliyetleri kapsamında işlenmesine uygulanır.
2. Bu Regülasyon Birlik dahilindeki ilgili kişilerin kişisel verilerinin Birlik dahilinde merkezi bulunmayan bir veri sorumlusu veya veri işleyen tarafından işlenmesi halinde, işleme faaliyetlerinin:

(a) İlgili kişiden bir ödeme istenip istenmediğine bakılmaksızın, Birlik dahilinde bulunan ilgili kişilere mal ve hizmet sunulmasına

(b) Birlik dahilinde gerçekleşen davranışlarının izlenmesine ilişkin olması halinde uygulanır.

3. Bu Regülasyon, Birlik dahilinde merkezi bulunmayan ancak uluslararası kamu hukuku sebebiyle üye devlet hukukunun uygulandığı bir yerde bulunan veri sorumlusu tarafından kişisel verilerin işlenmesi halinde uygulanır.

Regülasyon'un yürürlüğe girmesi öncesinde, Çalışma Grubu gelişen teknoloji ve uluslararası ekonomik işbirliği kapsamında yapılacak kapsamlı bir çalışmanın geciktirilmeden hazırlanması yönünde çağrılarda bulunmaktaydı, bu çağrının önemli bir sebebi de gelişen teknoloji ve ekonomik ilişkiler ile birlikte, AB içerisinde yer almayan veri sorumlularının AB içerisindeki ilgili kişilere hizmet

sunması sonucu bu kişilerin temel haklarının koruma altına alınmasını sağlamaktı[10].

Madde ile birlikte anlaşılmaktadır ki; Regülasyon, yalnızca AB içerisindeki şirketler bakımından geçerli değildir. Nerede hizmet verirse versin, AB vatandaşlarına ve AB içerisinde ikamet edenlere ait verileri işleyen bir şirket, Regülasyon'un uygulama alanı içerisine girecektir. Bir başka ifade ile şirketlerin Regülasyon kapsamındaki sorumlulukları değerlendirilirken, AB merkezli olmaları değil, AB dahilinde veri işleme faaliyeti yapıp yapmadıkları dikkate alınacaktır[11]. AB üyesi olmayan bir ülkede elektronik ticaret hizmeti vermekte olan veri sorumlusunun hizmet verdiği web sitesine AB'den erişilebiliyor olması AB'ye hizmet sunuluyor olduğunun bir göstergesi olmamalıdır, web sitesine bakıldığı zaman, dil seçeneklerinin, kargo imkanının olup olmaması gibi değişkenlerle Regülasyon kapsamına dahil olup olmadığı değerlendirilebileceği gibi, elektronik ticaret hizmeti veren Türk bir işletmenin hedef kitlesinin; Almanya'da yaşayan ve Türkçe konuşan müşteriler olması, web sitesinin yalnızca Türkçe dil seçeneği olmasına rağmen Regülasyon kapsamında değerlendirilmesine yol açacaktır[12].

Maddede bahsedilen mal ve hizmet sunulması yalnızca veriye erişimden daha fazlasını ifade etmektedir. Örneğin, çevrimiçi davranışsal reklamcılık[13] olarak

[10] Leyla KESER, Article 29 Working Party calls fort he swift adoption of the data protection reform package, Bilişim Hukuku Günlüğü, 04.12.2013, http://www.leylakeser.org/2013/12/article-29-working-party-calls-for.html, Erişim Tarihi: 10.03.2019.
[11] KÜZECİ, s. 203.
[12] KARADUMAN, Ozan. The General Data Protection Regulation: Achieving Compliance for EU and non-EU Companies. Business Law International, 2017, s. 226.
[13] Çevrimiçi davranışsal reklamcılık, geleneksel reklamcılıktan ölçülebilirlik ve hedefleme özellikleriyle ayrılmaktadır. Çevrimiçi davranışsal reklamcılık ile birlikte yayınlanan reklama ilişkin performans kriterleri takip edilerek hedefleme modeli kullanılmaktadır. Ayrıntılı bilgi için bkz: KESER BERBER, Çevrimiçi Davranışsal Reklamcılık (Online Behavioral Advertising) Uygulamaları Özelinde Kişisel Verilerin Korunması, İstanbul 2014, s. 19.

bildiğimiz kullanıcıların davranışlarının izlenmesi, bu izleme sonucu ihtiyaçların kişiselleştirilmesi de bu kapsama girecektir[14].

Birlik dahilinde merkezi bulunmayan veri sorumlularının ve veri işleyenlerin 3. madde kapsamında sorumluluklarının doğması nedeniyle 27. madde gereği Birlik dahilinde temsilci atamaları gerekmektedir. Hükmün 3. cümlesinde söz konusu temsilcinin hangi ülkede atanması gerektiği açıklıkla belirtilmiştir. Buna göre temsilcinin bulunacağı yer, ilgili kişilere mal ve hizmetin sunulduğu yer veya davranışları izlenen ilgili kişilerin bulunduğu yer olarak belirlenmelidir[15].

Atanan temsilci Regülasyon'a uyulmasının sağlanması amacıyla, işlemeye bağlı her türlü konuda muhatap alınmak üzere yetkilendirilmesine rağmen, bu durum veri sorumlusunun veya veri işleyenin kendisinin Regülasyon'dan doğan yükümlülüklerini ve sorumluluklarını ortadan kaldırmayacağı gibi, kendisine karşı yasal çarelere başvurulmasını engellemeyecektir.

İki ihtimalde veri temsilcinin atanmasına gerek olmadığı Regülasyon'da aynı madde altında düzenlenmektedir. Buna göre, kamu kurumları veri sorumlusu temsilcisi atamak zorunda olmadığı gibi, sürekli olarak geniş çapta, özel nitelikli kişisel verilerin ve cezai hükümler ve suçlarla ilgili kişisel verilerin işlenmemesi, işlemenin niteliği, kapsamı ve doğası gereği kişilerin hak ve özgürlüklerinin

[14] Çevrimiçi Davranışsal Reklamcılık'ta Kişisel Verilerin Korunması konusunda ayrıntılı bilgi için bkz: Leyla Keser Berber, Çevrimiçi Davranışsal Reklamcılık, s. 31 vd..Çevrimiçi davranışsal reklamcılıkta yaşanabilecek problemlerin temeli çevrimiçi davranışsal reklamcılığın kendisi değil, bu reklamcılık sisteminin öncesinde gerçekleştirilen izleme ve bu izleme ile toplanan kişisel verilerdir. Bu nedenle, bu faaliyet kapsamında kişisel veri işleyen şirketler ilgili kişilerin rızalarını her türlü veri işleme başlamadan, yani çevrimiçi davranışsal reklamcılık faaliyetleri bakımından opt-in modeline geçmelidirler. Kullanıcıların web üzerindeki davranışlarına göre ekranlarında ilgi alanlarıyla alakalı olarak reklam gösterilmesine ilişkin Dünya'nın ilk ve alanında en bilinen şirketlerinden birisi olan Phorm, eski adıyla 121 Media, Amerika'da 2002 yılında kurulmuştur. Phorm'un kendisinin davranışsal reklamcılık uygulaması olan PeopleOnPage ile desteklediği ve geliştirdiği ContextPlus, dönemin geniş kitlelerce kabul görmüş fakat konuyla ilgili kişiler tarafından casus yazılım olarak adlandırılmıştır.

[15] IT GOVERNANCE PRIVACY TEAM, EU General Data Protection Regulation (GDPR), An Implementation and Compliance Guide, Second edition, IT Governance Publishing, İngiltere 2017, s. 242.

zedelenmesi muhtemel olmaması durumlarında da temsilci atama yükümlülüğü doğmayacaktır[16].

2.2.3. Hesap Verilebilirlik

Hesap verilebilirlik ilkesi Regülasyon'un en önemli yeniliklerinden biri olarak görülebilir. Bu ilke ile birlikte veri sorumlusu, veri koruma ilkelerine ne derece uygun olduğunu kanıtlama imkanına sahip olacaktır. Regülasyon kapsamındaki tüm bu yükümlülüklerin eksiksiz yerine getirilmesi ve bu durumun şeffaflık ilkesi ile birlikte hesap verilebilirlik ilkesi ile birlikte de gözler önüne serilmesi ilgili kişilerin, verilerinin ne şekilde işlendiği ve ne gibi risklere maruz kaldığı ortaya çıkacaktır.

Veri sorumlusu, gerçekleştirdiği veri işleme süreçlerine ve bu süreçler nedeniyle karşılaşabileceği risklere göre önlemler alma yükümlülüğü altındadır. Bu kapsamda üç yeni kontrol mekanizması vardır. Veri sorumlusu, Regülasyon'un 30. maddesi gereği işleme faaliyetlerinin kayıtlarını tutmalı, ilgili kişilerin haklarını koruma altında tutabilmek adına yüksek risk öngörülen durumlarda 35. madde gereğince veri koruma etki değerlendirmesi yapmalı ve veri işleme kamu kurumları tarafından yapılıyor, veri sorumlusunun esas faaliyeti geniş çapta ve sistematik olarak ilgili kişilerin izlenmesini kapsıyor ya da esas faaliyet özel veri kategorilerine ilişkin ise 37. Madde gereği Veri Koruma Görevlisi atamalıdır.[17]

[16] IT GOVERNANCE PRIVACY TEAM, s. 241.
[17] Sahar BHAIMIA, The General Data Protection Regulation: The Next Generation of EU Data Protection. Legal Information Management, 18(1), 21-28, s. 25.

2.2.4. Unutulma Hakkı

Yönerge'nin uygulandığı dönemde oldukça fazla gündeme gelen ve ilk olarak Avrupa Birliği Adalet Divanı'nın Google vs. Spain kararı[18] ile birlikte veri koruması alanında kendine oldukça önemli bir yer edinen unutulma hakkı da Regülasyon ile birlikte yasal bir temele oturtulmuştur.

İnternet ve sosyal ağların gelişmesi ile birlikte kişisel veriler daha önce görülmemiş bir şekilde ve hızda yayılmaya başlamıştır. İnternetin yapısal tasarımı, web üzerine kaydedilen bilgilerin web üzerinde kalması sonucunu doğurmaktadır. Bu nedenle, ilgili kişilere ait internet ortamında bulunan herhangi bir verinin yok edilmesi için hem Yönerge hem de Regülasyon, ilgili kişilere kişisel verilerin silinmesini isteme ve elde etme hakkını sağlamaktadır. Bu imkanlar, Regülasyon ile unutulma hakkı adı altında yeni bir kimlik kazanıştır. Bu hak uyarınca ilgili kişiler, Regülasyon'da tanınan haklar ile birlikte arama motorları listesinden kaldırılma ve gizlilik hakkını ihlal eden bağlantılar için arama motorlarından bilgi alma imkanlarına sahip olacaklardır[19].

Regülasyon'un 17. maddesinde metne alınan unutulma hakkı ile; ilgili kişi, veri sorumlusundan, kendisine ait kişisel verilerin gecikmeden silinmesini isteme hakkına haiz olmuştur. Veri sorumlusu ilgili maddede sayılan hallerin varlığı halinde kişisel verileri gecikmeden silme yükümlülüğü altındadır. Veri sorumlusunun, elinde bulundurduğu kişisel verileri paylaşmış olması durumunda ise söz konusu verilerin bağlantı, kopya veya nüshalarının silinmesi taleplerini,

[18] İspanyol Mario Costeja Gonzalez'in, sosyal güvenlik borçlarını ödememesinden dolayı evinin cebri satışa çıkarılmasıyla alakalı haberlerin 11 yıl sonra dahi kendi ismini girerek yaptığı Google aramalarında ilk sırada çıkması üzerine haberlerin silinmesi için Google İspanya'ya başvurmuş ve bu talebi olumsuz karşılanmıştır. İspanya Ulusal Yüksek Mahkemesi'ne kadar uzanan bu konu, görüş alınması için Avrupa Birliği Adalet Divanı'na iletilmiştir (ECJ, Decision of 13 May 2014, C-131/12). Divan konuyla alakalı olarak, kamunun üstün bir menfaatinin bulunmaması halinde özel hayatın gizliliği hakkı kapsamında ilgili kişinin kişisel verilerini içeren bağlantıların üçüncü kişilerin veritabanlarından dahi kaldırılması gerektiğini belirtmiştir.

[19] NICOLADOU/GEORGIADES, s. 7.

verilerin paylaşıldığı veri sorumlularına iletmek için gerekli adımları atması, veri sorumlusundan beklenecektir.

Regülasyon m. 17'ye göre,

"a) *kişisel verilerin elde edildikleri veya başka surette işlendikleri amaçla ilgili olarak artık gerekli olmaması*

b) kişisel verilerin işlenmesinin veri koruma hukukuna aykırılık taşıması

c) ilgili kişinin rızasını geri çekmesi ve işlemeye itiraz etmesi"

Hallerinde ilgili kişi unutulma hakkının hayata geçirilmesini veri sorumlusundan talep edebilecektir. Hükmün kaleme alınış şekli, öğretide ifade edildiği üzere, ilgili kişiye aslında bir silme hakkı tanımaktadır[20]. "Unutulma hakkı" içeresinde barındırdığı pasif eylem düşünüldüğünde, madde 17'de karşılık bulmamaktadır. Bilakis ilgili kişi aktif bir eylemde bulunarak unutulma hakkını hayata geçirmelidir. Bu ise maddenin lafzı ile "Right to Erasure (Right to be forgotten" şeklindeki kenar başlığı arasında farklılığı açıklamaktadır.

Her ne kadar Regülasyonun 17 maddesi unutulma hakkının kesin bir hak olarak algılanmasına yol açıyorsa da, Regülasyonun 19 maddesi ile birlikte okunmalıdır. Bu hüküm çerçevesinde veri sorumlusunun alacağı tedbirler teknik olarak mümkün, savunulabilir ve makul olmalıdır. Özellikle veri sorumlusunun altına gireceği külfet karşısında ilgili kişinin elde edeceği menfaat karşılaştırıldığında bu veri sorumlusu açısından orantısız bir yük oluşturmamalıdır[21]. Menfaat terazinin nasıl hakimin değerlendirmesinde dikkate alınacağı konusunda yukarıda atıf verilen Google İspanya kararı yol gösterici niteliktedir.

[20] Nicolai CULIK Christian DOPKE, About Forgetting and Being Forgotten, in: ed. Thomas Hoeren/ ed. Barbara Kolany-Raiser, Big Data in Context Legal, Social and Technological Insights, Cham 2017, Springer, s. 21 – 26, s. 22.
[21] KULHARI, s.47.

Bireylerin kişisel verilerinin işlenmesi ile oluşabilecek hak ihlalleri sonucu korunması gereken kişisel haklar; ticari çıkarlar, ifade özgürlüğü ve kamu menfaati arasında çatışmalar meydana gelebilir. Birbiriyle bağlantılı bu hakların uyumlu hale getirilebilmesi adına Avrupa Birliği Adalet Divanı kararları ışığında dört genel kategori oluşturulabilir.

İlk olarak, etkilenen kişinin kamusal hayattaki rolü dikkate alınabilir. Bu rol ne kadar küçük olursa mahremiyet hakkı da bir o kadar büyük olacaktır. Örneğin politikacılar ya da "normal" vatandaşlar gibi kamusal hayattaki rolü kalıcı olan ya da olmayan kişilerin sınıflandırılması bu kapsamda zorluk çıkarmamaktadır. Şov katılımcıları gibi belirli bir bağlamda kamusal varlık yaratmış kişilerin kategorize edilmesi daha zor bir durumdur.

İşlenen verilerin türü de bir diğer kategori olarak sayılabilir. İşlenen kişisel verilerin etkilenen kişi ya da kamu için ne şekilde bir anlam ifade ettiği değerlendirmeye alınmalıdır. Bu kapsamda da işlenen kişisel verilerin ne şekilde anlam ifade ettiğinin açıklanması için üç farklı alan belirlenmiştir; sosyal alan, özel alan ve mahrem alan. Genel olarak mahrem alana ilişkin kişisel veriler silme hakkını doğuracaktır.

Üçüncü kategori olarak bilginin kaynağının analiz edilmesi sayılabilir. Kaynak ne kadar şüpheli olursa, işlenen kişisel verilerin de silinmesi o kadar gündeme gelecektir.

Son kriter ise zamandır. Güncel bilgiler, eski bilgilere göre korunma imkanından daha fazla yararlanacaktır.[22]

[22] CULIK, DOPKE, s. 24-25.

2.2.5. Tasarımda Veri Koruması (Privacy by Design) ve Varsayılan Ayarlarda Veri Koruması (Privacy by Default)

Regülasyon, yeni teknolojilerin geliştirilmesi ile birlikte, yeni gizlilik risklerini de beraberinde getirdiği öngörüsü ile tasarımda veri koruması ilkesini benimsemektedir. Buna göre uygulamaları akıllı cihazlarına indiren kişiler genellikle uygulamaların tasarımcıların veya üçüncü şahısların kişisel verilerine erişimine izin vermekten başka seçeneğine sahip olmamaktadır. Regülasyon, veri koruma ve gizlilik dostu koruma önlemlerini hem "tasarım aşamasında" hem de "varsayılan ayarlar" olarak en başta yeni teknolojilere yerleştirmeyi zorunlu kılmaktadır. Örneğin, bir sosyal ağa ilk defa kayıt olurken, varsayılan ayarlar diğer kullanıcıların yeni hesaba erişimini engelleyecek şekilde ayarlanmış olmalıdır. Yeni kullanıcı, "arkadaşlar" listesine kimlerin ekleneceğini seçme hakkına sahip olmalıdır [23].

2.2.6. Veri Taşınabilirliği

Regülasyon'un 20. maddesi ile yine yeni bir düzenleme olan "veri taşınabilirliği hakkı" gündeme getirilmiştir. Buna göre; ilgili kişi, ilgili maddede belirtilen hallerde, veri sorumlusuna verdiği kişisel verilerini, biçimlendirilmiş, genel olarak kullanılan ve teknik olarak okunabilen bir formatta talep edebilir ve bu kişisel verilerini paylaşmış olduğu ilk veri sorumlusunun engellemesi ile karşılaşmadan başka bir veri sorumlusuna aktarabilir.

Regülasyon ile sosyal ağlar bakımından getirilen bu önemli yenilik, sosyal ağ kullanıcılarının kişisel verilerinin taşınabilmesi imkanı yaratmaktadır. Buna göre, bir kişi artık bir sosyal ağ kullanıcısı olmak istemiyorsa, başka birine geçmeye karar verirse, şimdiye kadar gönderdiği tüm verileri ikinci bir ağa taşımak isterse ve hatta diğer kullanıcıların yayınlarında yaptığı beğenileri taşımak isterse,

[23] NICOLAIDOU/ GEORGIADES, s. 8.

Regülasyon, bu gibi sorunların üstesinden gelmek adına veri taşınabilirliği hakkını düzenlemiştir. Bu hakkın, veri sorumlularının, Regülasyon'a uyum sağlaması adına teknik açıdan hayata geçirilmesi gerekmektedir.

Veri taşınabilirliği hakkının tanınmış olması, aynı zamanda kullanıcının kendi verileri üzerinde tasarruf etme özgürlüğünü ve özellikle veri sorumlusu karşısında içinde bulunduğu bilgi asimetrisi ilişkisi karşısında onu güçlendirme amacını taşımaktadır. Bu hak regülasyonun teknoloji nötr yapısı ile birlikte değerlendirildiğinde, Regülasyonu çerçevesinde teknolojilerin de kullanıcı dostu geliştirilmesine hizmet edeceği aşikardır. Zira farkındalık düzeyinin gelişmesi ile birlikte kullanıcı dostu ve veri koruması dostu teknolojiler kullanıcılar tarafından tercih edilecektir[24].

2.2.7. Veri Koruması Etki Değerlendirmesi

Veri koruması etki değerlendirmesi de Regülasyon ile birlikte getirilen yeniliklerden biridir. Yönerge, otomatik olarak işleme yapan veri sorumlularının denetim makamına yapacakları bildirim sonrasında, denetim makamı tarafından denetlenmesini öngörmüştü, ancak bu denetim veri sorumlularına oldukça fazla idari yük ve masraf oluşturmaktaydı, Regülasyon ile getirilen veri koruma etki değerlendirmesi, veri sorumlusu tarafından yapılacak etki değerlendirmesi sonrası gereken hallerde denetim makamına başvuru ile bu idari yük ve masrafı azaltmaktadır[25]. 35. maddede yer verilen bu düzenleme; özellikle yeni teknolojiler kullanan bir işleme türünün, işlemenin tabiatı, kapsamı, bağlamı ve amaçları dikkate alındığında gerçek kişilerin hak ve özgürlükleri bakımından önemli risklere yol açması halinde, veri sorumlusunun işlemeden önce, planlanan işleme faaliyetlerinin kişisel verilerin korunması üzerindeki etkisine yönelik bir

[24] KULHARI, s. 40.
[25] Hüseyin Murat DEVELİOĞLU,6698 sayılı Kişisel Verilerin Korunması Kanunu ile Karşılaştırmalı Olarak AB Genel Veri Koruma Tüzüğü uyarınca Kişisel Verilerin Korunması Hukuku,1. Baskı, İstanbul, Aralık 2017, s. 110.

değerlendirme yapması gerekliliğini belirtir. Denetim makamı veri koruması etki değerlendirmesi yapılmasını gerektiren veya gerektirmeyen işleme faaliyetlerinin bir listesini oluşturup yayınlayabilecektir. Regülasyon, bu tür bir denetim için kesin kurallar koyarak bir denetim mekanizması oluşturmak yerine, kişisel verilerin işlenmesi süreci içinde ortaya çıkabilecek muhtemel risklerin tespiti ve bu riskleri önlemek adına alınabilecek tedbirlerin belirlenmesi hususunda yükümlülüğü veri sorumlusuna yüklemiştir[26].

İlgili maddeye göre Regülasyonda belirtilen tabir ile "data privacy officer" (DPO), Türkçe ifade ile "Veri Koruma Görevlisi" (Çalışmanın bundan sonraki bölümlerinde "Veri Koruma Görevlisi" olarak anılacaktır.) atanmış bir veri sorumlusu ise, veri sorumlusu değerlendirmeyi gerçekleştirirken Veri Koruma Görevlisinin tavsiyelerine başvuracaktır. Veri koruma etki değerlendirmesi esas olarak veri sorumlusunun görevidir, Veri Koruma Görevlisi'nin veri koruma etki değerlendirmesindeki rolü ise veri sorumlusu tarafından tavsiyesine başvurulmasıdır[27]. Veri koruma etki değerlendirilmesinin yapılıp yapılmaması, yapılırken hangi metodolojinin izlenmesi gerektiği, bu hizmetin kurum içerisinde yapılması ya da kurum dışı hizmet olarak alınıp alınmamasının gerekliliği ve bu değerlendirmenin doğru bir şekilde yapılıp yapılmadığı ve sonuçların Regülasyon ile uyumunun değerlendirilmesi konusunda Veri Koruma Görevlisinin tavsiyelerine uyulması Article 29 Working Party (Art. 29 WP) (Çalışmanın bundan sonraki kısımlarında "Çalışma Grubu" olarak anılacaktır.) tarafından tavsiye edilmektedir[28]. Veri sorumlusunun Veri Koruma Görevlisi'nin tavsiyelerine uymaması halinde tavsiyelerin neden dikkate alınmadığının yazılı olarak belirtilmesi gerekmektedir. Veri sorumlusunun Veri Koruma Görevlisini yönlendirerek tavsiye alması söz konusu olamaz ve menfaatlerine göre bir tavsiye

[26] Mesut Serdar ÇEKİN, AB Hukukuyla Mukayeseli Olarak 6698 Sayılı Kişisel Verilerin Korunması Kanunu, 1. Baskı, İstanbul 2018, s. 115.
[27] IT GOVERNANCE PRIVACY TEAM, s. 81.
[28] Article 29 Data Protection Working Party, Guidelines on Data Protection Officers ("DPOs"), Adopted on 13 December 2016 As last Revised and Adopted on 5 April 2017, s. 17.

kararı çıkmaması halinde 38. maddenin 3. fıkrası gereği bu nedenle görevden alınamaz.

Veri koruma etki değerlendirmesi ile birlikte ortaya çıkan sonuçlara göre; öngörülen risklerin önlenmesi adına veri sorumlusu tarafından gerekli tedbirlerin belirlenmesi ve hayata geçirilmesi gündeme geleceğinden, veri işleme ve veri işlemede kullanılacak teknoloji ve sistemlerin belirlenmesi açısından veri sorumlularına önemli derecede fayda sağlanacaktır[29]. Veri koruma etki değerlendirmesi ile asıl amaçlanan, işleme sürecinde ortaya çıkabilecek olası risklerin en aza indirgenmesidir. Bu sebeple veri sorumluları bu değerlendirme ile işletmeleri için uzun vadede kullanabilecekleri en uygun teknolojiyi yine kendileri belirlemiş olacaklardır.

Regülasyon'un 35. ve 36. maddeleri göz önüne alındığında; denetim makamının veri koruma etki değerlendirmesindeki rolü, değerlendirmenin yapılması/yapılmaması gereken faaliyetlerin türlerinin belirlendiği listeler hazırlayarak bunları Veri Koruma Kurul'una bildirmek ve yapılan veri koruması etki değerlendirmesi sonucu önemli risklerin ortaya çıkacağı öngörülen durumlarda veri sorumlusuna görüş vermek olarak belirtilebilir. Veri sorumlusu tarafından yapılan veri koruması etki değerlendirmesinin mutlak surette denetim makamına sunulması gerekliliği yoktur, Regülasyon denetim makamının, önemli risklerin varlığı halinde veri sorumlusuna görüş vermesi gerekliliğini hüküm altına almıştır.

Veri koruma etki değerlendirilmesi tek seferlik bir uygulama olarak öngörülmemiştir. Regülasyon'un 35. maddesinin 11. fıkrası veri sorumlusunun, risklerde değişiklik meydana geldiği durumlarda, işlemenin hala veri koruma etki değerlendirmesine uygun olarak gerçekleştirilip gerçekleştirilmediği konusunda inceleme yapması gerekliliğini belirtmiştir. Veri işleme süreci devam ettiği süre

[29] Susan DOE, Practical Privacy: Report from the GDPR World. Legal Information Management, 18(2), 76-79, s. 78.

boyunca gerekli hallerde ve özellikle öngörülen risklerin farklı şekillerde ortaya çıkması durumlarında tekrarlanması ya da değişen koşulların veri koruma etki değerlendirmesine uygunluğunun denetiminin gerekliliği muhakkaktır[30].

2.3.Veri Sorumlusu

Regülasyon'un "Tanımlar" başlıklı 4. maddesinde açıklandığı üzere; veri sorumlusu, kişisel verilerin işlenmesinin amaçlarını ve vasıtalarını tek başına veya başkalarıyla birlikte belirleyen gerçek veya tüzel kişi, kamu makamı, kurumu veya diğer kamu kuruluşudur. Tanımda bahsedilen "işlenme amaçlarını ve vasıtalarını belirlemek" kişiyi veri sorumlusu yapan asıl kriterdir. Veriyi elinde bulunduran herkes veri sorumlusu olarak tanımlanamaz.

Regülasyon 26. maddede müşterek veri sorumlularına yer vermiştir. İşleme amaçlarını ve vasıtalarını iki veya daha fazla veri sorumlusunun belirlemesi halinde bu veri sorumluları müşterek veri sorumlusu olarak adlandırılacaklardır. Ancak bu durum, Regülasyon'un 82. maddesinin 4. fıkrasında da belirtildiği üzere; işlemenin sebep olduğu herhangi bir zarardan dolayı tarafların sorumluluğunu etkilemeyecektir. Her bir veri sorumlusu, hatta aşağıda anlatılacak olan veri işleyen, zararın tamamından sorumlu tutulacaklardır. Veri sorumlularının müşterek veri sorumlusu hale gelmeleri sorumlulukların paylaşımından değil, işleme amaç ve vasıtalarının birlikte belirlenmesinden kaynaklı doğan bir sonuç olarak düşünülmelidir.

[30] Felix BIEKER, Michael Friedewald, Marit Hansen, Hannah Obersteller, Martin Rost, A Process for Data Protection Impact Assessment Under the European General Data Protection Regulation, Privacy Technologies and Policy, 4th Annual Privacy Forum, APF 2016, Frankfurt/Main, Germany, September 7-8, 2016, s. 35.

2.3.1. Veri Sorumlusunun Yükümlülükleri

2.3.1.1.Temel Prensipler

Regülasyon'un 5. maddesinde kişisel verilerin işlenmesine ilişkin temel prensiplere yer verilmiştir. Veri sorumlusu belirtilen tüm prensiplere uymakla yükümlü olduğu ve bu prensiplere aykırı hareket ettiği takdirde sorumlu tutulacağı ilgili maddenin 2. fıkrasında belirtilmiştir. Belirtilen bu prensipler aşağıda Türk Hukuku'na ilişkin yapılan çalışmada, veri sorumlusunun yükümlülükleri altında daha detaylı olarak incelenecektir. Çalışmanın bu kısmında bu prensiplere ilişkin yapılacak açıklamalar KVKK ve uygulaması kısmındaki çalışmaya bir giriş niteliğinde değerlendirilebilir. 6 başlık altında sayılabilecek bu prensipler:

- **Hukuka uygunluk, hakkaniyet ve şeffaflık:**

Kişisel verilerin işlenmesine ilişkin günümüze kadar oluşturulan hemen hemen tüm yasal metinlerde işlemenin hukuka uygun olması gerekliliği belirtilmiştir. Bu prensip diğer tüm prensipleri kapsayıcı ve bağlantısı olan bir yükümlülüktür[31]. Regülasyon, 6. maddede işlemenin hukuka uygunluğunu hüküm altına almış ve hangi durumlarda yapılan işlemenin hukuka uygun sayılacağını belirtmiştir. Şeffaflık ise Yönerge'de sayılmayan ve Regülasyon ile detaylandırılan bir prensiptir. Yönerge'de yer alan prensiplere ekleme yapılmasının amacı gelişen teknoloji ile ilgili kişilerin haklarının zarara uğramamasıdır. Getirilen şeffaflık ilkesi ile birlikte ilgili kişilerin bilgilendirilmeleri konusunda veri sorumlularının yükümlülükleri daha sıkı hale getirilmiştir[32]. Regülasyon'un 3. Bölümünde de "şeffaflık ve usuller" başlığı ile ilgili kişilere bilginin ne şekilde sağlanacağı belirtilmiştir.

[31] KÜZECİ, s. 206.
[32] European Data Protection Supervisor, Opinion of the European Data Protection Supervisor on the Data Protection Reform Package, March 2012, s. 19.

- **Amaçla sınırlı olma:**

Verilerin belirli, açık ve meşru amaçlar için toplanması gerekliliğinin yanı sıra, belirlenen bu amaçlar dışında hiçbir surette işlenmemesi gerekmektedir. Ancak Regülasyon'un 89. maddesinin 1. fıkrasında belirtilen, arşivleme amacıyla, bilimsel veya tarihi araştırma amacıyla veya istatistiksel amaçla işleme, buna istisna olarak gösterilebilir. Amacın belirli ve açık olması, işlenen verilerin baştan belirlenmiş amaç doğrultusunda kullanımı ve bu amacın ilgili kişiler tarafından bilinebilir olması anlamına gelir. Verilerin işlenmesi için belirlenen amacın daha sonradan toplanma amacından farklı hale gelmesi bu ilkeye aykırılık teşkil edecektir.

- **Veri minimizasyonu:**

Bu prensip, yeterli, alakalı ve işlendikleri amaçla bağlantılı olarak gerekli şekilde sınırlı olarak veri işlenmesi gerektiğini ifade etmektedir. Veri sorumlusu belirli, açık ve meşru amacı doğrultusunda işleme yaparken, gerektiğinden fazla veriye sahip olmamalıdır. Hatta veri sorumlusu, elindeki verilerin yalnızca belli bir kısmı ile dahi amacına ulaşabilecek durumdaysa, gerekli olmayan verileri kullanmamalıdır. Söz konusu gerekli olmayan verilerin elde tutulması artık amaca aykırılık teşkil edeceğinden hukuka aykırı olarak elde tutuluyor sayılacaktır. Örneğin, youtube bir videonun 18 yaş altı kulanıcılar tarafından seyredilmesine engel olmak istiyorsa, kullanıcının doğum tarihi bilgisi yerine kullanızının 18 yaşının üstünde olup olmadığının kendisine sorulması ile elde edilecek basit bir evet ya da hayır ile bu amacı sağlayabilecektir. Görüldüğü üzere, veri minimizasyonu ile amaçla bağlılık ilkeleri dikkate alınarak hukuka uygun kişisel veri işlenmiş olacaktır[33].

[33] KULHARI, s. 45.

- **Doğruluk:**

Verilerin doğru ve gereken hallerde, güncel olmaları, yanlış olan kişisel verilerin gecikmeden silinmesi veya düzeltilmesini sağlamak adına tüm makul adımların veri sorumlusu tarafından atılması gerekmektedir. Bu kapsamda verilerin doğru ve güncel tutulması, ilgili kişilere Regülasyon'un 16. maddesi ile tanınan "düzeltme hakkı" ile de mümkün olacaktır. Düzeltme hakkı ile ilgili kişiler, verilerin doğru ve güncel olmaması sebebiyle veri sorumlusuna başvurabilirken, veri sorumluları da verilerin doğru ve güncel olmaması sebebiyle ilgili kişilere doğru ve güncel verilerin kendisine aktarılması için başvurabilir.

- **Sınırlı süre saklama:**

Veriler, işlendikleri amacın gerektirdiği süreyi aşmayacak şekilde işlenmelidir. Ancak uygun tedbirlerin alınmış olması halinde, kamu yararı için arşivleme yapılması amacıyla, bilimsel veya tarihi araştırma amacıyla veya istatistiksel amaçla verilerin daha uzun süre saklanması Regülasyon kapsamında mümkündür. Verilerin işlenmesi aynı zamanda veri güvenliğinin sağlanması gerekliliğini de doğurmaktadır. Verilerin sınırlı süre ile saklanması prensibinin olmadığı varsayımında, sonsuz bir döngüde veri güvenliğini sağlayabilmek oldukça zor bir yükümlülük olacaktır. Aynı zamanda bireysel özerklik, bireyin maddi ve manevi bütünlüğü ve özel hayatın gizliliği gibi değerler de verinin bir kere verilmesi ile birlikte yaşam boyunca kayıt altında olması ile zarar görecektir. Bu nedenler de göz önüne alınarak, verilerin sınırlı süre ile işlenmesi gerekliliği prensibi ve yukarıda detaylı olarak anlatılan unutulma hakkı[34], veri koruması hukukunda kendilerine önemli bir yer edinmişlerdir.

[34] Bkz: s.11.

- **Bütünlük ve gizlilik**

Veri sorumluları ve veri işleyenler ellerinde bulundurdukları kişisel verilerin korunmasına yönelik veri güvenliğini sağlamakla yükümlü olduklarından, bu kapsamda teknik ve organizasyonel tedbirler almakla yükümlüdürler.

2.3.1.2.Temsilci Atama Yükümlülüğü

AB'de kişisel veri işleyen veri sorumlusu veya veri işleyen AB'de merkezi bulunmasa bile bir temsilci atama zorunlulukları vardır. Temsilci atama yükümlülüğü, veri işlemenin AB dahilinde gerçekleşmesinin veri sorumluları ve veri işleyenler için Regülasyon kapsamında sorumluluklarının doğması, yani Regülasyon'un yer bakımından uygulanması ile yakından ilgisi vardır. Bu nedenle bu yükümlülüğe yukarıda "Yer Bakımından Uygulanma" başlığı[35] altında da değinilmiştir. Ancak çalışmanın ileriki bölümlerinde "Temsilci"[36] başlığı altında daha detaylı bilgiye yer verilecektir.

2.3.1.3.Gerekli Tedbirleri Alma Yükümlülüğü

Veri sorumlusu, Regülasyon'un 24. maddesi uyarınca, ilgili kişilerin haklarını korumak adına, ortaya çıkabilecek riskleri öngörerek, uygun teknik ve organizasyonel tedbirleri almakla yükümlüdür. Bu tedbirlerin, işleme süreçleriyle ve teknolojik gelişmelere bağlı olarak gerektiği hallerde güncel duruma uygun hale getirilmesi de veri sorumlusundan beklenir. Regülasyon'un 32. maddesinde, riskle orantılı bir güvenlik seviyesi temin etmek için uygun teknik ve organizasyonel tedbirleri almakla yükümlü olarak veri sorumlusu ve veri işleyeni işaret etmiştir.

[35] Bkz: s. 7.
[36] Bkz: s. 29.

İhlal, veri sorumlularının marka değerlerine zarar verdiği gibi, finansal olarak da veri sorumlularını olumsuz olarak etkilemektedir. IBM'in 2015 yılına ait araştırmasına göre, ihlal gerçekleşen bir olay ortalama 3,8 Milyon $ zarar anlamına gelmektedir. Telekomünikasyon şirketi TalkTalk da 2015 yılına ait araştırmasıyla ihlal gerçekleşen bir olayın ortalama 35 Milyon £ zarar anlamına geldiğini belirtmiştir[37].

Avusturya Veri Koruma Otoritesi, özel nitelikli kişisel verilerin korunması adına Regülasyon'un 32. maddesinde belirlenen güvenlik önlemlerinden "psödonimleştirme" yapılmadığı iddiasıyla hak ihlali yaşadığını ileri sürerek şikâyette bulunan ilgili kişinin talebini, ilgili kişilerin, verilerin korunmasına ilişkin alınacak tedbirlerin belirlenmesine ilişkin bir talep hakkı bulunmadığını belirterek reddetmiştir. Bu karar, veri sorumlularının 32. madde kapsamında yol gösterici bir karar olabilecektir[38]. Psödonimleştirme, yani takma adlı verinin açık bir şekilde tanımlanması, Regülasyon ile iletişim ve teknoloji sektörünün olumsuz etkileneceğinden çekinen kuruluşların Regülasyon için getirdikleri önerilerden biridir[39]. Veri sorumlusunun işlediği veri, bir kişiyi direkt olarak belirlemeye yetmiyor veya takma adlı veri oluşturuyorsa veri sorumlusu ilgili kişiyi belirlemek adına ek bilgi toplayamaz ve işleyemez, bu şekilde tek başına kullanıldığında başkaca ek bir bilgi olmaksızın bir kişiyi tanımlamayan veriler için de koruma gerekmektedir[40].

[37] LAMBERT, s. 7.
[38] AZ: DSB-D123.070 / 0005-DSB / 2018, https://www.jdsupra.com/legalnews/austrian-data-protection-authority-45800/, Erişim Tarihi: 18.12.2018.
[39] Leyla KESER/Mehmet Bedii KAYA/Batu KINIKOĞLU, Türkiye'de Kişisel Verilerin Korunmasının Hukuki ve Ekonomik Analizi (Raporun İkinci Bölümü), İstanbul Bilgi Üniversitesi, 2014, s. 41.
[40] KESER/ KAYA/ KINIKOĞLU, s. 63.

Veri güvenliğine ilişkin alınması gereken tedbirlerle ilgili detaylı bilgi, çalışmanın ileriki bölümünde, veri sorumlusunun yükümlülükleri başlığı[41] altında yer almaktadır.

2.3.1.4.Bildirim Yükümlülüğü

Regülasyon'un 4. maddesi'nde tanımlandığı üzere, aktarılarak, depolanarak ya da başka yollarla, işlenen verilerin kazaen veya hukuka aykırı şekilde imha edilmesi, kaybolması değiştirilmesi, ifşası ya da ele geçirilmesine yol açan güvenlik ihlalleri, kişisel veri güvenliğinin ihlalidir. 33. madde, kişisel veri güvenliğinin ihlali halinde, bu durumun denetim makamına bildirilmesi gerekliliğini düzenlemiştir. Veri sorumlusunun, denetim makamına haber verme yükümlülüğünün yanı sıra, veri işleyen de ihlali öğrenir öğrenmez veri sorumlusunu haberdar etme yükümlülüğü altındadır.

Veri ihlali sonucu veriyi elde eden yetkisiz kişilerin, veriyi anlamasını engelleyen teknik ve organizasyonel tedbirlerin alınmış olması halinde bildirimin gerekli olmadığı söylenebilir. Bildirim için orantısız bir çaba gerekmesi halinde de ilgili kişiye bildirimin yapılmaksızın kamuya açıklama yapılabilir[42].

2.3.1.5.Gizlilik Yükümlülüğü

Regülasyon, gizlilik yükümlülüğü ile ilgili olarak özel bir düzenleme yapmasa da kişisel verilerin, gerekli tedbirler ile güvenliğinin ve gizliliğinin sağlanarak işlenmesi gerektiğini belirtmiştir. Veri koruması hukukunun en temel yükümlülüğü olarak düşünülebilecek olan gizlilik yükümlülüğü çeşitli maddelerde anılarak çalışmada yer almıştır.

[41] Bkz: s. 72.
[42] DEVELİOĞLU, s. 109.

9. maddede yer alan "Özel nitelikli kişisel verilerin işlenmesi" başlığı, 28. maddede veri işleyenlere getirilen gizlilik yükümlülüğü, veri güvenliğine ilişkin 32. maddede, çalışmanın ileriki bölümlerinde "Veri Koruma Görevlisi" başlığı[43] altında detaylı olarak anlatılacak olan, 38. maddede yer alan Veri Koruma Görevlisi'nin gizlilik yükümlüğü gibi çeşitli maddeler altında gizlilik ve sır saklamaya ilişkin düzenlemeler yer almaktadır.

2.3.1.6.Ön Denetim Yükümlülüğü

Veri koruma etki değerlendirmesi başlıklı madde ile Regülasyon'a eklenen bu yükümlülük çalışmanın önceki bölümlerinde "Veri Koruma Etki Değerlendirmesi" başlığı[44] altında detaylı olarak anlatılmıştır.

2.3.1.7.Veri Koruma Görevlisi Atama Yükümlülüğü

Regülasyon'da belirtilen veri sorumlularının Veri Koruma Görevlisi atama yükümlülükleri çalışmanın ileriki bölümlerinde "Veri Koruma Görevlisi" başlığı[45] altında detaylı olarak anlatılacaktır.

2.4.Veri İşleyen

Regülasyon ile birlikte, Yönerge'de önemli bir etkisi bulunmayan "veri işleyen" veri koruma hukukunda önemli bir aktör haline gelmiştir. Regülasyon'un 28. maddesi veri işleyeni düzenleyen kapsamlı bir maddedir. Bu madde ile veri sorumlusunun yükümlülük ve sorumlulukları da belirlenmiştir. Ancak veri işleyene ilişkin tanım Regülasyon'un "Tanımlar" başlıklı 4. maddesinde yapılmıştır; veri işleyen, veri sorumlusu adına kişisel verileri işleyen gerçek veya tüzel kişi, kamu makamı, kurumu veya diğer kamu kuruluşudur. Belirlenen veri

[43] Bkz: s.. 31.
[44] Bkz: s. 15.
[45] Bkz: s. 31.

işleyen veri sorumlusunun izni ile başka bir veri işleyen görevlendirebilir, ancak ikinci bir veri işleyen görevlendirildiği takdirde veri sorumlusunun da bilgilendirilmesi gerekmektedir.

2.4.1. Veri İşleyen'in Yükümlülükleri

Veri işleyen Yönerge'de detaylı bir düzenleme edinmemiş olsa da veri sorumlusu adına işleme yapması nedeniyle, veri sorumlusunun üstlenmiş olduğu birçok yükümlülüğü üstlenmektedir. Bu kapsamda veri sorumlusundan çok ayrı tutulmamalıdır. Yukarıda "Veri Sorumlusunun Yükümlülükleri" başlıklı madde altında sayılan yükümlülüklerin hemen hepsi ve veri işlemede uyulması gereken temel prensipler, veri işleyen için de geçerlidir. Örnek olarak; verilerin işlenmesi sürecinde gerekli tedbirlerin alınması, ilgili kişilerin bilgilendirilmesi, gizlilik yükümlülüğü ve Veri Koruma Görevlisi atama yükümlülükleri veri işleyene de yüklenmiş olan yükümlülüklerdir.

Veri işleyenin, yukarıda bahsi geçen yükümlülüklerin dışında veri sorumlusuyla yapacağı sözleşme gereği yükümlülükleri de gündeme gelecektir. Veri sorumlusu ile belirlenen veri işleyen arsında var olan sözleşme; veri işleyenin veri sorumlusunun talimatlarına uygun hareket etmesi gerektiğini, gizlilik yükümlülüğüne uyulması gerekliliğini, teknik ve organizasyonel tedbirlerin alınmasını, veri sorumlusunun yükümlülüklerine uyulmasını, işleme hizmetlerinin verilmesinin ardından verilerin silinmesi veya veri sorumlusuna iadesini, veri sorumlusunun yetkilendirdiği denetçi tarafından denetim yapılmasına izin verilmesi hususlarını içermelidir. Veri sorumlusunun verdiği talimatların Regülasyona ya da üye devlet düzenlemelerine aykırı olduğunu düşünen veri işleyen bunu veri sorumlusuna bildirmelidir.

2.5.Veri Sorumlusu ve Veri İşleyen'in Sorumlulukları

Yönerge'de sorumluluk veri sorumlusunun üzerindeyken, Regülasyon ile birlikte veri sorumlusu ile veri işleyenin de hukuka uygun veri işleme kapsamında sorumluluğu gündeme gelmiştir.

Veri işleyen, veri sorumlusunun bilgisi ve onayı dahilinde başka bir veri işleyen görevlendirirse, veri işleyene yüklenen yükümlülükler diğer veri işleyene de yüklenecektir. Diğer veri işleyenin yükümlülüklerini yerine getirmemesi halinde ilk veri işleyen, diğer veri işleyenin yükümlülüklere aykırı davranışlarından dolayı veri sorumlusuna karşı sorumlu olacaktır.

Bir veri işleyenin, işlemenin amaçlarını ve vasıtalarını belirleyerek bu Regülasyon'u ihlal etmesi halinde, veri işleyen bu işleme ile ilgili olarak veri sorumlusu kabul edilecektir.

İlgili maddeden de anlaşılacağı üzere veri işleyen Regülasyon ile birlikte detaylı bir tanımlamaya dahil edilmiştir. Veri işleyenin başka veri işleyenler kullanabilmesi, bu veri işleyenlerin arasındaki ilişki, veri işleyenin işlemlerinde uyması gereken kurallar, veri sorumlusu ile aralarındaki ilişki ve sorumluluklara ilişkin uzun bir metin kaleme alınmıştır. Bununla birlikte madde 79'da da ilgili kişilerin veri sorumlusuna ve veri işleyene karşı etkin yasal çarelere başvurma hakkını düzenlenmiştir. Maddeye göre; denetim makamına şikâyette bulunma hakkı dahil olmak üzere, kişisel verilerin Regülasyona aykırı olarak işlenmesi sonucunda hakları ihlal edilen ilgili kişiler yasal yollara başvurabilecektir.

Regülasyon ile birlikte ilgili kişilere tanınan hakların yönlendirilebileceği kişiler Yönerge'de olduğu gibi veri sorumlularıyla sınırlandırılmamış veri işleyenler de dahil edilmiştir. Veri işleyenin başka bir veri işleyen ile çalışması halinde ikinci veri işleyenin de ilk veri işleyen gibi yükümlülükler altına gireceği açıktır. Bu durum şirketlerin bulut hizmet sağlayıcıları ile çalışmaları halinde bu

sağlayıcıların da sorumluluğunun gündeme geleceğini göstermektedir. Uygulamada bulut hizmet sağlayıcıların çoğunluk olarak AB dışında olması Regülasyon'un yer bakımından uygulanma politikası gereğince bu şirketlerin sorumluluğunun doğmasını engellemeyecektir. Bu duruma ek olarak "Veri işleyen" başlıklı 28. madde'nin 4. fıkrasına tekrar bakıldığında; "… Diğer veri işleyenin kişisel verilerin korunmasına yönelik yükümlülükleri yerine getirmekte başarısız olması halinde, ilk veri işleyen veri sorumlusuna karşı diğer veri işleyenin yükümlülüklerinin yerine getirilmesi için tam olarak sorumlu kalmaya devam eder." hükmü ile veri işleyenlerin, görevlendirdikleri ikinci veri işleyenlerin işlemlerinden de sorumlu kalmaya devam edecekleri belirtilmiştir.

Regülasyon'un 82. maddesi tazminat hakkı ve sorumlulukları düzenlemiştir. Eğer ki Regülasyon ihlal edilir ise, bu ihlal nedeniyle zarara uğrayan ilgili kişi, zararın giderilmesini veri sorumlusu ya da veri işleyenden talep edebilecektir. İhlalin gündeme geldiği verinin işlenmesi sürecine katılan her bir veri sorumlusu bu zarardan sorumlu tutulacaktır. Veri işleyen, Regülasyon ile üstlenmiş olduğu yükümlülüklere, veri sorumlusunun kendisine verdiği talimatlara aykırı davrandığı takdirde sorumlu hale gelecektir. Veri sorumluları ve veri işleyenlerin sorumluluktan kurtulmaları, zararın doğmasına sebep olan ihlalde herhangi bir sorumlulukları olmadığını ispatlamaları halinde mümkündür.

İdari ve cezai yaptırım konusu da oldukça etkili hükümleri içermektedir ve Regülasyon'un 83. ve 84. maddelerinde düzenlenmiştir. İdari para cezalarında ciddi ihlallerin varlığı halinde 20 Milyon Euro'ya ya da işletmenin bir önceki yılın küresel cirosunun %4'üne kadar çıkabilmektedir. Cezai yaptırımlarda ise, idari para cezalarına tabi olmayan ihlaller için, üye devletler kendi cezai yaptırımlarını belirleyebileceklerdir.

Bu yeni ve kapsamlı düzenleme ile belki de verilerin işlenmesi konusunda sürecin başından itibaren taraf konumunda olan veri işleyenlerin sorumluluk

alanına dahil edilmesi ilgili kişilerin olası ihlaller karşısında daha geniş bir sorumluluk sahasında haklarını arayabilmesi açısından olumlu olmuştur.

2.6.Temsilci

Regülasyon'un "Birlik dahilinde merkezi bulunmayan veri sorumlularının veya veri işleyenlerin temsilcileri" başlıklı 27. maddesi kapsamında anlatılan temsilci, çalışmanın önceki bölümlerinde "Yer Bakımından Uygulama"[46] ve "Temsilci Atama Yükümlülüğü"[47] başlıkları altında anlatılmıştır. AB dahilindeki kişilerin, AB içerisinde merkezi bulunmayan bir veri sorumlusu veya veri işleyen tarafından işlenmesi durumunda temsilci atama durumu gündeme gelecektir.

Çalışmanın ileriki bölümlerinde anlatılacak olan Türk Hukuku sisteminde yer alan "veri sorumlusu temsilcisi"nden[48] farklı olarak temsilci, 27. madde başlığından ve madde içeriğinden de anlaşılacağı üzere yalnızca veri sorumlusu tarafından atanmayacaktır. Veri işleyen de şartlar oluştuğu takdirde temsilci atama yükümlüğü altına girecektir[49].

Temsilci, Regülasyon'un 27. maddesinin 4. fıkrasına göre; *"veri sorumlusu veya veri işleyen tarafından, veri sorumlusu veya veri işleyenin yanında ya da onun yerine, özellikle denetim makamları ve ilgili kişiler tarafından, Regülasyon'a uyulmasının sağlanması amacıyla, işlemeye bağlı her türlü konuda muhatap alınmak üzere yetkilendirilir".*

Temsilcinin, ilgili maddenin lafzına bakıldığında veri sorumlusu ve veri işleyenle birlikte de muhatap alınacağı gibi, onların yerine de muhatap alınabileceği görülmektedir. Temsilcinin AB dahilinde merkezi bulunmayan veri

[46] Bkz: S. 7.
[47] Bkz: s. 22.
[48] Bkz: s. 109.
[49] IT GOVERNANCE PRIVACY TEAM, s. 241.

sorumlusu ve veri işleyen tarafından atanması göz önüne alındığında, Regülasyon'a uyum konusunda temsilcinin önemli pozisyonlarda bulunacağı öngörülebilir. Kimi durumlarda, denetim makamları ve ilgili kişiler ile veri sorumlusu veya veri işleyenden daha çok karşı karşıya kalacakları görevler edinebileceklerdir[50].

Temsilcinin yerine getirmesi gereken görevler Regülasyon'un birçok farklı hükmünde ya da resitallerinde kendisi göstermektedir:

- 27. maddenin 4. fıkrası ve Resital 80 gereğince Veri Koruma Otoritesi'nin ya da ilgili kşişinin sorularına cevap verme yükümlülüğü
- Resital 80 Regülasyon'a uyum sürecinin yönetilmesinde veri temsilcini yetkilendiriyor.
- 30. maddenin 1. fıkrası gereği veri işleme süreçlerinin kayıt altına alınması (*to maintain a specific record of the processing activities*) ve bu kayıtların talep halinde erişilebilir olmasını sağlamak

Temsilci Regülasyon kapsamındaki konumu dikkate alındığında, veri sorumlusunun ya da veri işleyenenin talimatı ile hareket eder ve onunla bağlıdır. Aynı zamanda temsilci yerel denetim makamları ve ilgili kişiler karşısında muhatap konumundadır[51].

Temsilcinin denetim makamı ve ilgili kişiler tarafından muhatap alınması durumu ise yasal sorumluluk konusunda veri sorumlusu ve veri işleyeni kurtardığı ise söylenemeyecektir. Regülasyon'un 27. maddesinin 5. fıkrasına göre *"veri sorumlusu veya veri işleyen tarafından temsilci atanması veri sorumlusunun veya veri işleyenin kendisine karşı yasal çarelere başvurulmasını engellemez".* Atanan temsilci ile veri sorumlusu veya veri işleyen arasındaki hukuki ilişkiye göre temsilcinin sorumluluğunun gündeme geleceği durumlar ortaya çıkabilecekse de

[50] IT GOVERNANCE PRIVACY TEAM, s. 242.
[51] IT GOVERNANCE PRIVACY TEAM, s. 242.

bu durum veri sorumlusu ve veri işleyenin yasal sorumluluğunu ortadan kaldırmayacaktır[52].

2.7.Veri Koruma Görevlisi

2.7.1. Genel Olarak

Regülasyon'un getirdiği yeniliklerden bir diğeri de Regülasyon'da 4. kısımda 37. ve 39. Maddeleri arasında düzenlenen, Veri Koruma Görevlisidir. Hükümler incelendiğinde görülecektir ki, veri koruma görevlisinin atanmasının tabi olacağı koşullar, atanacak kişinin sahip olması gereken özellikler, rolü, yükümlülükleri ve özellikle ilgili kişi, veri sorumlusu ve veri işleyen ile arasındaki ilişkiler Regülasyon kapsamında düzenlenmektedir.

Aslında Veri Koruma Görevlisi kavramı AB hukukuna çok da yabancı olmayan bir kavram olmakla birlikte ilk olarak 1977 tarihli Alman Veri Koruma Yasası ile ortaya çıkmıştır[53]. Yönerge'de Veri Koruma Görevlisi kurumu yer almasa da şirketler isteğe bağlı olarak Yönergeye uyumu sağlamakla görevli yetkililer atayabiliyordu.

Yönerge, uyum yetkililerinin atanmasını hüküm altına almasa da, Yönerge yürürlükte iken; Almanya[54], İsveç[55], Fransa, Belçika, Bulgaristan, Estonya, Macaristan, Letonya, Litvanya, Lüksemburg, Malta, Hollanda, Polonya, Slovakya, Birleşik Krallık[56] gibi bazı üye devletler kendi iç hukuk kurallarıyla kimi veri sorumlularının, verilerin korunması alanında faaliyet gösterecek bir yetkili atamaları gerekliliğini hüküm altına almış, bazı üye devletler ise böyle bir

[52] IT GOVERNANCE PRIVACY TEAM, s. 242.
[53] RECIO, Miguel. Data Protection Officer: The Key Figure to Ensure Data Protection and Accountability. Eur. Data Prot. L. Rev., 2017, s. 114.
[54]DEVELİOĞLU, s.114.
[55] Marta-Claudia; SPATARU-NEGURA, Laura-Cristiana. The General Protection Regulation: What Does the Public Authorities and Bodes Need to Know and to Do. Juridical Trib., 2018, s. 494.
[56] RECIO, s. 114.

yetkili atanmasını gerekli görmemişlerdir. ABD'de ise birçok yasal düzenleme ve FTC kararlarında; veri sorumlularının, veri korunması alanında sorumlu olacak bir yetkili ataması gerektiği belirtilmiştir[57].

2.7.2. Bir İşletmenin Veri Koruma Görevlisi'nin Olmasının Anlamı

Bir veri sorumlusunun Veri Koruma Görevlisi'ne sahip olması; bu veri sorumlusunun Regülasyon başta olmak üzere, veri koruması alanına ilişkin yasal düzenlemelerden haberdar olması, kendi veri koruma politikasını bu düzenlemelere ve gelişen yasal çerçevelere kısa sürede uygun hale getirebilmesi, yasal düzenlemeler çerçevesinde veri sorumlusunun kendisi ve veri koruma konusunda sorumluluk sahibi olan çalışanların rollerinin net bir şekilde belirlenebilmesi ve bu rollerin gereklerinin yerine getirilip getirilmediğinin denetlenebilmesi, ilgili kişilerin verilerinin işlenmesi süreçlerine ilişkin başvurularının etkin ve hızlı bir şekilde cevaplandırılması hususlarında veri sorumlularına olumlu etki sağlayacaktır.

Önemle altı çizilmelidir ki, Veri Koruma Görevlisi şirketin Regülasyon'a uygunluğundan kişisel olarak sorumlu tutulmayacaktır. Yukarıda anlatıldığı ve Regülasyonda da açıkça belirtildiği üzere tüm bu uyum sürecinde sorumluluk veri sorumluları ve veri işleyenler üzerindedir. Ancak Veri Koruma Görevlisinin uyum sürecindeki etkisi yine de azımsanmayacak derecede önemlidir. Veri Koruma Görevlisi'nin atanmış ve bu kurumun Regülasyon'a uygun şekilde işliyor olması, veri sorumlusunun Regülasyon kapsamında hesap verilebilirliğin mümkün olduğunu gösterecektir[58]. Veri Koruma Görevlileri, birçok kuruluş için bu yeni yasal çerçevenin merkezinde yer alacak konumdadır ve Regülasyon hükümlerine uyumu kolaylaştıracaktır[59]. Bu nedenle veri sorumlularının Veri Koruma Görevlisi'ne sahip olması ve Regülasyon hükümlerine uyumluluğun sağlanması, veri koruma ilkelerine uyumluluğun bir göstergesi olarak da kabul edilebilecektir.

[57] GILBERT, s. 839.
[58] RECIO, s. 118.
[59] Art. 29 WP, Guidelines on "DPOs", s. 4.

2.7.3. Veri Koruma Görevlisi Atanması Öngörülen Haller

Veri Koruma Görevlisinin Atanması başlıklı madde 37; hangi hallerde veri sorumlusunun ve veri işleyenin Veri Koruma Görevlisi ataması gerektiğini düzenlemiştir.

Maddenin lafzına bakıldığında Veri Koruma Görevlisi atama yükümlülüğünün hem veri sorumlusuna hem de veri işleyene verildiği görülmektedir. Hangi durumlarda veri sorumlusunun ya da veri işleyenin veya her ikisinin de Veri Koruma Görevlisi atamasının gerekli olduğu ise 37. maddenin 1. fıkrasında sayılan faaliyetlerin kim tarafından gerçekleştirildiği göz önünde bulundurularak belirlenebilir. Örneğin, lokal bir alanda ve tek bir hizmet veren küçük bir veri sorumlusu az sayıda müşteriye sahiptir ve bu veri sorumlusunun sınırlı sayıda müşterisi ve faaliyeti olduğu göz önüne alındığında geniş çaplı veri işlemediği görülecektir ve bu nedenle veri sorumlusu olsa da Veri Koruma Görevlisi ataması gündeme gelmeyecektir. Ancak bu gibi birçok lokal veri sorumlusuna web, pazarlama gibi konularda hizmet vererek verilerini işleyen büyük çaplı şirketler düzenli ve sistematik olarak geniş çaplı gözlem ve veri işleme yaptıklarından veri işleyen olarak Veri Koruma Görevlisi ataması gerekecektir[60].

İlgili madde uyarınca;

- İşlemenin, yargısal faaliyette bulunan mahkemeler hariç, kamu kurum ve kuruluşu tarafından gerçekleşmesi,
- Esas faaliyetin, ilgili kişilerin düzenli ve sistematik olarak geniş çaplı izlenmesi,
- Esas faaliyetin, özel nitelikli kişisel verilerin veya cezai hükümler ve suçlarla ilgili kişisel verilerin geniş çapta işlenmesi hallerinde veri

[60]Art. 29 WP, Guidelines on "DPOs", s. 9.

sorumlusu ve/veya veri işleyen Veri Koruma Görevlisi atamak durumunda kalacaktır[61].

Madde metninden anlaşılabileceği üzere (a) bendi hariç, veri sorumlusunun "esas faaliyeti" bir Veri Koruma Görevlisi atanıp atanmaması hususunda belirleyici bir rol oynar. (a) bendine göre ise işlenen verinin niteliğinde herhangi bir özellik aranmaksızın Veri Koruma Görevlisi atanması esastır. Aşağıda bu kriterler madde metnindeki sıra esas alınarak incelenecektir:

a) Regülasyon, kamu kurum ve kuruluşu kavramını tam olarak tanımlamamış, bu kavramların ulusal yasalar çerçevesinde belirleneceği düşünülmüştür. Ancak Regülasyon'da belirtilen ifade ile mahkemeler ve adli yargı merciileri Veri Koruma Görevlisi atama zorunluluğundan muaftırlar[62]. Günümüzde kamu hizmeti yalnızca kamu kurumları tarafından değil özel hukuk kişileri tarafından da yerine getirilebilmektedir. Bu durumda da ilgili kişiler, verileri kamu kurumları tarafından işleniyormuş gibi veri işleme süreçlerine dair bir seçim hakkına sahip olmamaktadırlar. Bu nedenlerden dolayı, yasal bir zorunluluk olarak öngörülmemiş olsa Çalışma Grubu kamu hizmeti veren özel hukuk kişilerinin de Veri Koruma Görevlisi atamalarını önermektedir[63].

b) Bir veri sorumlusunun esas faaliyeti o veri sorumlusunun ana, temel faaliyetlerini ifade eder. İşletmenin hedeflerini gerçekleştirmesi için kişisel verileri işleme ihtiyacı duyması temel faaliyeti gereği veri işlediğini gösterir. Devamlı olarak işlenen verilerin her zaman veri sorumlusunun esas faaliyeti nedeniyle işlenmesi söz konusu olmayacaktır, tali amaçlar doğrultusunda da devamlı olarak veri işlenmesi gündeme gelebilir. Örneğin, bordro ve İK bilgilerinin toplanması herhangi bir alanda hizmet veren veri sorumlularının genel olarak yaptığı veri işlemenin en çok karşılaşılan örneklerindendir ancak bu

[61] LAMBERT, s. 39.
[62] CLIZA, s. 493.
[63] Art. 29 WP, Guidelines on "DPOs", s. 6.

işlemeler her veri sorumlusunun temel faaliyetlerinin bir parçası olarak değerlendirilemez[64]. Bunun yanı sıra bir hastanenin temel faaliyeti sağlık bakımı sağlamaktır, bu nedenle hastane tarafından işlenen sağlık kayıtlarının hastanenin temel faaliyeti gereği işlendiği kabul edilir ve Veri Koruma Görevlisi ataması gündeme gelir[65].

Düzenli ve sistematik bir şekilde geniş çaplı gözlem tanımlamasına; çevrimiçi davranışsal reklamcılık, mobil uygulamalarla konum izleme, giyilebilir cihazlar aracılığıyla sağlık verilerinin izlenmesi, akıllı arabalar gibi örnekler verilebilir. Geniş çaplılık ise farklı kriterlerle belirlenebilecek bir konudur. İşlemenin geniş çaplı olup olmadığını belirlerken dikkat edilecek kriterler;

- İlgili veri konularının sayısı
- İşlenen kişisel verilerin hacmi
- İşlenen farklı veri ögelerinin dağılımı
- İşleme faaliyetinin süresi ve sürekliliği

Örneğin, büyük bir perakende web sitesi, kullanıcılarının aramalarını ve satın alımlarını izlemek için algoritmalar kullanır ve bu bilgilere dayanarak, onlara önerilerde bulunur. Bu, sürekli olarak ve önceden tanımlanmış kriterlere göre gerçekleştiği için, veri konularının geniş çapta düzenli ve sistematik olarak izlenmesi olarak düşünülebilir[66].

c) Özel veri kategorilerinin ve cezai hükümler ve suçlara ilişkin kişisel verilerin işlenmesi diğer verilere göre daha hassas ve risk taşıyan veriler olarak düşünülür. Bu nedenle bu nitelikteki kişisel verilerin geniş çaplı olarak işlenmesi söz konusu olduğunda da Veri Koruma Görevlisi'nin var olması gerekmektedir. Örneğin, Bir sağlık sigortası şirketi, çok sayıda kişi hakkında tıbbi koşullar ve

[64] Information Commissioner's Office, Guide to the General Data Protection, August 2018, s. 194.
[65] Art. 29 WP, Guidelines on "DPOs", s. 7.
[66] ICO, Guide to the GDPR, s. 195.

diğer sağlık bilgileri de dahil olmak üzere çok çeşitli kişisel verileri işler. Bu durum, özel veri kategorisine dahil olan kişisel verilerin geniş çapta işlemesi olarak düşünülebilir[67].

Yukarıda detaylı olarak anlatıldığı ve 37. maddenin ilk fıkrasında da belirtildiği üzere; eğer adli sıfatla hareket etmekte olan mahkemeler hariç, kamu kurum veya kuruluşları tarafından işleme yapılıyorsa, bir Veri Koruma Görevlisi tayin edilmelidir. Aynı şekilde veri sorumlusu veya veri işleyenin esas faaliyetleri; tabiatı, kapsamı ve/veya amaçları gereği ilgili kişilerin verilerinin düzenli ve sistematik şekilde geniş çaplı olarak işlenmesi ile ilgiliyse ya da özel nitelikli kişisel veri kategorilerinin geniş çapta işlenmesine ilişkinse, bir Veri Koruma Görevlisi atanmalıdır[68].

37. maddenin 1. fıkrasında belirtilen veri sorumlularından olmadıkları için yasal zorunluluğu olmayan veri sorumluları da gönüllü olarak Veri Koruma Görevlisi atayabilme imkanına sahiptirler. Regülasyon bu imkânı ilgili maddenin 4. fıkrasında kaleme almıştır. Gönüllü olarak bir Veri Koruma Görevlisi atandığı takdirde 4. kısımda belirlenen yükümlülükler zorunlu olarak bir Veri Koruma Görevlisi atanmış gibi Regülasyon'un 4. kısmında sayılan tüm hükümlere uygunluğun sağlanması gerekecektir.

Yasal olarak Veri Koruma Görevlisi atama zorunluluğu olmayan bir veri sorumlusu gönüllü olarak da bir Veri Koruma Görevlisi atamayıp, kişisel verilerin korunmasına ilişkin ayrı bir personel tayin edebilir ya da şirket dışı danışmanlık alabilir, bunun önünde herhangi bir engel yoktur. Ancak böyle bir durumda bu personelin ya da danışmanın görev ve iş tanımı, pozisyonu ve görevleri, yükümlülükleri net bir şekilde belirlenmeli ve bu kişilerin unvanlarının Veri Koruma Görevlisi olmadığı açıkça belirtilmelidir[69].

[67] ICO, Guide to the GDPR, s. 195.
[68] DEVELİOĞLU, s.114.
[69] Art. 29 WP, Guidelines on "DPOs", s. 6.

Tek bir Veri Koruma Görevlisi'nin, organizasyonel yapıları ve büyüklükleri dikkate alınarak birden fazla kamu kurum veya kuruluşuna ya da her bir işletme tarafından erişimin kolaylığı göz önüne alınarak teşebbüsler birliğine atanması da söz konusu olabilecektir. İlgili maddenin 2. ve 3. fıkrasında düzenlenen bu hususla amaçlanan, örneğin grup şirketler gibi yapılanmalarda her bir şirket için ya da organizasyonel olarak bir arada bulunan kamu kurum ve kuruluşlarda her bir kurum ayrı birer Veri Koruma Görevlisi'nin belirlenmesinin ortaya çıkaracağı bürokrasi ve maliyet yükü olarak değerlendirilebilir.

IAPP, Regülasyon kapsamında belirlenmiş koşulların sağlanabilmesi adına, 75.000'den fazla Veri Koruma Görevlisi'nin atanması gerekeceğini ve bu sayının veri sorumlularına Regülasyon'a uyum konusunda önemli derecede maliyet yükleyeceğini belirtmiştir[70].

2.7.4. Veri Koruma Görevlisi Kimdir?

Veri Koruma Görevlisi, aşağıda görevleri detaylı olarak anlatılacağı üzere; veri sorumlusunun ve veri işleyenin ve çalışanların veri koruması kapsamındaki yasal ve teknik düzenlemeler arasındaki bir köprü olarak değerlendirilebilir. Veri Koruma Görevlisi bağlı olduğu veri sorumlusu kapsamında veri korumasına ilişkin bilgi, eğitim verme ve denetleme yapma yetkilerine haiz olduğundan, özellikle kişisel verilerin korunması hukuku ve uygulaması hakkında uzmanlık bilgisi başta olmak üzere mesleki yetileri dikkate alınarak tayin edilmelidir.

Uzmanlık bilgisi net bir şekilde tanımlanmamıştır. Ancak, Veri Koruma Görevlisi'nden beklenen uzmanlık bilgisi, organizasyon süreçlerinin hassasiyeti, karmaşıklığı ve işlenen verilerin büyüklüğü ile orantılı olmalıdır. Örneğin, veri işleme faaliyetinin karmaşık olduğu ya da büyük miktarda hassas verinin

[70] KARADUMAN, s. 227.

işlenmesinin söz konusu olduğu durumlarda, Veri Koruma Görevlisi'nden standart bir uzmanlık bilgisinin üzerinde bir uzmanlık beklenebilir. Regülasyon "mesleki yetiler"den ne anlaşılması gerektiğini de tanımlamamıştır. Veri Koruma Görevlisi'nin kişisel verilerin korunması hukuku ve uygulaması hakkında uzmanlık bilgisi olması ihtiyacının yanı sıra, sektörel bilgisi ve veri sorumlusunun organizasyonel yapısına ilişkin hakimiyetinin olması, bilgi sistemleri, veri güvenliği ve veri koruma ihtiyaçlarını da karşılayabilecek düzeyde bilgi sahibi olması beklenir[71]. Aksi takdirde; ilgili kişilerin haklarının korunması ve yasal zorunluluklara uyulması konusunda olumlu etki yaratması beklenirken, veri sorumlusunun faaliyetleri ve yükümlülükleri konusunda yeterli bilgiye sahip olmaması sonucu, yasal düzenlemelere uyumluluk konusunda veri sorumlusunun problemlerle karşılaşması gündeme gelebilir[72]. Veri Koruma Görevlisi'nin bir veri sorumlusuna sağlayacağı fayda, o işletmenin ihtiyaçlarının belirlenmesiyle mümkündür.

Konuyla alakalı olarak, 5 Eylül 2018 tarihinde İtalya İdare Mahkemesi'nin bir kararı mevcuttur. Bu karara göre, bilgi güvenliği yönetim sistemi standardı olan ISO 27001 denetçisi ya da baş denetçisi olmayan bir kişinin Veri Koruma Görevlisi olma talebinin reddine karar verilmemelidir. Karar; Regülasyon'un, Veri Koruma Görevlisi olarak atanacak kişiler için ISO 27001 denetçisi ya da baş denetçisi olma gibi bir şartı kapsamadığını ve kişinin bu belgeye sahip olmaması durumunun, Veri Koruma Görevlisi olarak kendine yüklenen sorumlulukları yerine getiremeyeceği anlamına gelmediğini belirtmiştir[73]. Bir veri sorumlusunun, Veri Koruma Görevlisi olarak belirleyeceği kişinin sahip olması gereken özellikler, Regülasyon'da belirtilen özelliklerin, işletmenin ihtiyaçlarını karşılayabilecek düzeyde olması dikkate alınarak belirlenmelidir. Bir veri sorumlusunun veri işleme faaliyetleri ve süreçleri karmaşık ve risk taşıyan faaliyetler kapsamında değerlendirildiği takdirde, atanacak Veri Koruma

[71] Art. 29 WP, Guidelines on "DPOs", s. 11.
[72] RECIO, s. 118.
[73] https://www.insideprivacy.com/eu-data-protection/italian-court-decides-that-a-data-protection-officer-does-not-have-to-be-a-certified-iso-27001-auditor/, Erişim Tarihi: 18.12.2018.

Görevlisi'nde aranan uzmanlık bilgisi de daha fazla olacaktır[74]. Bu görevi yerine getirmesi için herhangi bir belge, sertifika sahibi olması zorunlu tutulmamalıdır.

Veri Koruma Görevlisi, veri sorumlusunun veya veri işleyenin çalışanı olabilir veya görevlerini hizmet sözleşmesi kapsamında yerine getirebilir. Bu konuya ilişkin Regülasyon'da detaylı bir düzenleme yer almadığından, veri sorumlusu ve/veya veri işleyen Veri Koruma Görevlisi olarak uygun gördüğü ve Regülasyon'da belirtilen özelliklere haiz herhangi bir kimseyi atayabilecektir. Veri sorumlusunun, kendisine bağlı bir çalışanı Veri Koruma Görevlisi olarak ataması, dışarıdan birini atayarak bu hizmeti almasına oranla maliyet olarak daha avantajlıdır. Aynı zamanda maliyet avantajının yanı sıra, şirket içi gizlilik konularında da veri sorumlusuna bağlı bir çalışanın Veri Koruma Görevlisi olarak atanması yararlı görülebilir. Ancak, hizmet sözleşmesi kapsamında çalışan birinin Veri Koruma Görevlisi olarak atanmasının avantajların bulunmasına rağmen dışarıdan bu hizmetin alınması uzun vadede veri sorumlusuna daha fazla avantaj sağlayabilir. Dışarıdan atanan bir Veri Koruma Görevlisi, bu görevi yerine getirebilmek adına, veri sorumlusu tarafından atanmadan, güncel uygulamalar, teknolojik gelişmeler konusunda daha fazla bilgi ve tecrübeye sahip olabileceği gibi, bu görev için gerekli sertifikasyon ve eğitimlere de sahip olabilecektir. Dışarıdan atanan bir Veri Koruma Görevlisi, sektör içinde farklı veri sorumluları tarafından da aynı görevlerde bulunmuş olabileceğinden, veri koruma hukuku kapsamında yaşanan ve yaşanabilecek sektörel problemlerin daha geniş bir çerçevede değerlendirilmesi gibi yeteneklere de sahip olabilecektir. Veri Korum Görevlisi, veri sorumlusu tarafından gerekli durumlarda görevini ifa etmek üzere göreve başlatılabilir, bu durumda da işin görülmesi üzerinden bir ücretlendirme sağlanabilir. Tüm bu bilgiler kapsamında, veri sorumlusu çalışanı birinin Veri Koruma Görevlisi olarak atanması yerine, dışarıdan bu hizmetin alınması daha makul bir seçenek olarak görülebilmektedir[75].

[74] CLIZA, s. 495.
[75] IT GOVERNANCE PRIVACY TEAM, s. 81-82.

Veri sorumlusu veya veri işleyen, atamış olduğu Veri Koruma Görevlisinin iletişim bilgilerini yayınlar ve denetim makamına bildirir. Veri sorumlusu ve/veya veri işleyene yüklenen bu yükümlülük aleniyet gereği konulmuş bir hüküm olarak karşımıza çıkmaktadır. İlgili kişilerin kendilerine tanınan hakları kullanabilmek için Veri Koruma Görevlisi'yle iletişime geçmesi Regülasyon kapsamında öngörülmüş ve düzenlenmiş olduğundan, iletişim bilgilerinin aleni hale getirilmesi de bu amaca hizmet eder nitelikte görülecektir. İlgili kişilerin ulaşmasında kolaylık sağlamak adına, Veri Koruma Görevlisi'ne ulaşım konusunda özel bir altyapı sistemi ya da direkt olarak Veri Koruma Görevlisi'ne ulaşacak bir form oluşturulabilir, aynı zamanda Veri Koruma Görevlisi'nin isminin de bildirilmesi gündeme gelebilir ancak bununla ilgili olarak Regülasyon'da herhangi bir düzenleme yer almadığından, Veri Koruma Görevlisi'nin isminin açıklanması hususu veri sorumlusu ve veri işleyenin kararına bırakılmış bir konu olarak belirtilebilir[76].

Regülasyon kapsamında, veri sorumluları tarafından atanması zorunlu olan Veri Koruma Görevli'si öncesinde veri güvenliğine ilişkin konular IT departmanları kapsamında değerlendirilmekteyken Regülasyon ile birlikte veri korumasına ilişkin konularda artık daha bağımsız, teknik ve hukuki açıdan "mesleki yeterliliğe" sahip Veri Koruma Görevlileri bu görevi üstlenmeye başlamıştır. Veri Koruma Görevlisi, veri sorumlusuna bağlı olarak çalışan bir IT yetkilisine oranla veri koruması için gerekli çalışmalara, alınması ya da alınmaması gereken kararlara daha bağımsız ve uyumlu kararlar alabilecektir[77]. Veri Koruma Görevlisi, IT görevlisinden farklı olarak verilerin toplanması, saklanması, imhası ve tüm bu süreçler için oluşturulacak politikalar gibi konularda da görevi gereği aktif rol oynayacaktır[78].

[76] CLIZA, s. 498.
[77] LAMBERT, s. 83-84.
[78] LAMBERT, s. 86.

Veri Koruma Görevlisi'nden beklenen uzmanlık bilgisi ve tecrübe; Avrupa ve yerel veri koruma uygulamaları ve veri sorumlusu tarafından uygulanan veri işleme süreci hakkında bilgi sahibi olmayı, bilgi teknolojisi ve veri güvenliğine, ticari hayat ve iş hayatına ilişkin tecrübelere sahip olmayı kapsar. Veri Koruma Görevlisi'nden bunlara ek olarak, veri sorumlusu dahilinde veri korumasına ilişkin konularda çalışanları bilinçlendirme görevlerini üstlenebilmesi de beklenir[79].

2.7.5. Veri Koruma Görevlisi'nin Görevleri

Veri Koruma Görevlisi Kimdir başlığı[80] altında Veri Koruma Görevlisi'nin, Regülasyon tarafından belirlenen görevleri yerine getirebilecek niteliklere haiz olması gerektiğinden bahsedilmiştir. Regülasyon 39. maddede Veri Koruma Görevlisi olarak atanan kişinin görevlerini asgari olarak saymıştır. Asgari olarak sayılmış olması, Veri Koruma Görevlisi'ne Regülasyon'da öngörülen görevler dışında da görevler yüklenebileceği anlamını taşır. Veri sorumluları ve/veya veri işleyenler Regülasyon'a ek olarak görevler tayin edebilirler. İlgili maddeye göre ise Veri Koruma Görevlisi'nin görevleri;

- Veri sorumlusu ve/veya veri işleyeni ve veri işlemekle görevlendirilmiş çalışanları, Regülasyon ve üye devlet veri koruma hükümleri hakkında bilgilendirmek, tüm bu yasal düzenlemeler kapsamında tavsiyelerde bulunarak hukuka uygunluk şartının yerine getirilmesini sağlamak,
- Regülasyon ve üye devlet yasal düzenlemeleri uyarınca sorumluluk dağılımını gerçekleştirerek, sorumluluklara ilişkin eğitimler vermek ve bu eğitimler sonrası oluşturulan veri koruma politikalarına uyum konusunda gerekli denetimleri yapmak,

[79] CHIRICA, Simona. The Main Novelties and Implications of the New General Data Protection Regulation. " Perspectives of Business Law" Journal, 2017, s. 164.
[80] Bkz: s. 36.

- Regülasyon'un 35. maddesinde bahsi geçen ve yukarıda detaylı olarak anlatılan "Veri Koruma Etki Değerlendirmesi"[81] hakkında tavsiyeler vererek uygulamasını takip etmek,
- Denetim makamı ile iş birliği halinde olmak ve denetim makamının veri sorumlusu ile arasındaki iletişim noktası olmak,
- İşleme faaliyetlerine bağlı riskleri dikkate almak olarak sayılabilir.

Veri Koruma Görevlisi'nin görevleri göz önüne alındığında, Regülasyon'un amaçları ve yüklediği yükümlülüklerin veri sorumluları ve veri işleyenler tarafından doğru bir şekilde hayata geçirilmesinin Veri Koruma Görevlisi aracılığıyla olacağı görülmektedir. Veri sorumluları ve veri işleyenler, bireylerin haklarını korumak adına, Regülayon'a uyumluluğun sağlanması için veri sorumlusunun görev ve ihtiyaçları doğrultusunda bir veri koruma politikası geliştirmelidirler[82], oluşturulacak bu veri koruma politikasının en önemli aktörü de belirlenen görev ve sorumluluklar doğrultusunda Veri Koruma Görevlisi olacaktır. Veri Koruma Görevlisi yasal düzenlemelerin veri sorumluları ve veri işleyenlerden ne beklediğini bu kişilere aktarmak ve bu kişileri yasal düzenlemelere uygunluk konusunda eğitmekle kalmayıp, bu yasal düzenlemelere uygunluk konusunda işletme içi bir denetim mekanizması da oluşturacaktır. Veri Koruma Görevlisi'nin, kendisinden beklenen görevleri yerine getirirken veri sorumlusu veya veri işleyen tarafından kendisine gerekli bağımsız alanın, zamanın ve kaynağın sağlanması gerekmektedir[83]. Yukarıda detaylı olarak anlatılan veri koruma etki değerlendirmesi, veri sorumlusunun veri işlemesini hukuka uygunluk prensibi çerçevesinde yapabilmesi adına oldukça önemli bir yükümlülüktür ve Regülasyon bu yükümlülük içinde de Veri Koruma Görevlisi'ne önemli bir görev vermiştir. Veri sorumlusu, işletme dahilinde veri koruması adına yeterli, belki de en üst düzeyde bilgi sahibi olduğuna karar kıldığı Veri Koruma Görevlisi'nin tavsiyeleri ile değerlendirmesini yapacak ve bu tavsiyelere göre hareket edecektir.

[81] Bkz: s. 15.
[82] GILBERT, s. 837.
[83] CLIZA, s. 497.

Kısaca, Veri Koruma Görevlisi Regülasyon'un işletmeler üzerinde doğru bir şekilde yansıması için aracı bir mekanizma olarak adlandırılabilir.

Veri sorumlusu ve/veya veri işleyenin, Veri Koruma Görevlisi'ni denetim makamına bildirmesiyle birlikte, Veri Koruma Görevlisi, denetim makamı ile veri sorumlusu ve/veya veri işleyen arasında adeta bir köprü görevi üstlenmeye başlamış olacaktır. Denetim makamı ilgili veri sorumlusuyla alakalı artık iletişim noktası olarak Veri Koruma Görevlisi'ni görecek ve talep ve bilgiler Veri Koruma Görevlisi aracılığıyla veri sorumlusuna ulaşacaktır. Yine bu köprü görevi ile birlikte karşılıklı bir iş birliği yoluna gidilerek iki kurum da birbiri ile iletişim halinde olacaktır. Denetim makamı ve Veri Koruma Görevlisi arasında, uyumlu ve çözüm odaklı bir ilişki olması amaçlanmış ve bu ilişkinin sağlam kurulabilmesi, ileride oluşabilecek problemleri önceden çözüme kavuşturması için bir yol olarak görülmüştür[84].

Veri Koruma Görevlisi kendisine yöneltilen talepleri bir ay içinde cevaplamakla yükümlü olmakla birlikte, veri sorumlularına yöneltilen taleplerin de aynı zaman dilimi içinde sonuçlandırılmasını sağlamakla yükümlüdürler. Bu zaman dilimi içinde anılan taleplerin sonuçlandırılması mümkün değilse, denetim makamına Veri Koruma Görevlisi bilgi vermekle yükümlü olacaktır[85].

Veri Koruma Görevlisi atanmasının veri sorumlularına sağlayacağı faydalar aşağıda sayılanlarla sınırlı olmamak üzere şu şekilde sıralanabilir[86]:

- Veri korumasına ilişkin yasal yükümlülüklerin yerine getirilmesi
- Veri korumasına ilişkin prosedürlerin oluşturulması ve var olan veri koruma prosedürlerinin iyileştirilmesi
- İşletmelere en uygun veri koruma politikalarının oluşturulması
- Veri korumasına ilişkin veri sorumlusu tarafından alınan kararların kontrolü ve iyileştirilmesi

[84] LAMBERT, s. 131; IT GOVERNANCE PRIVACY TEAM, s. 79/80.
[85] IT GOVERNANCE PRIVACY TEAM, s. 80.
[86] LAMBERT, s. 209-210.

- İşletme içerisinde veri korumasına ilişkin, çalışanlara eğitimin sağlanması
- Veri korumasına ilişkin işletme içi denetimin sağlanması
- Denetim makamları ile iletişim

2.7.6. Veri Koruma Görevlisi'nin Regülasyon Kapsamındaki Konumu

2.7.6.1. Genel Olarak

Yukarıda anlatıldığı üzere Veri Koruma Görevlisi Regülasyon kapsamında önemli görevlerle yükümlendirilmiş bir aktör olarak karşımıza çıkmaktadır. Regülasyon, Veri Koruma Görevlisinin konumunu 38. maddede 6 fıkra altında kaleme almıştır. Bu fıkralarda veri sorumlusu ve/veya veri işleyenin Veri Koruma Görevlisi ile olan ilişkisi, Veri Koruma Görevlisi'nin görevlerini ifa ederken bağımsızlığı, yetkileri, yükümlülükleri belirtilmiştir. Madde metnine göre;

Veri sorumlusu veya veri işleyen, Veri Koruma Görevlisi'nin, kişisel verilerin işlenmesine ilişkin tüm meselelere uygun şekilde ve zamanında dahil olmasını temin edecektir. Veri Koruma Görevlisi'nin kişisel verilerin işlenmesine ilişkin tüm meselelere uygun şekilde ve zamanında dahil olabilmesi adına, üst ve orta kademe yönetim toplantılarına düzenli olarak katılmalı, veri koruma ile ilgili alınacak tüm kararlarda tavsiyeleri alınmalı, veri işleme konusunda ihlal gündeme geldiğinde derhal Veri Koruma Görevlisine danışılmalıdır[87].

Veri sorumlusu ve veri işleyen, Veri Koruma Görevlisi'nin, görevlerini yerine getirmesi ve kişisel verilere ve işleme faaliyetlerine erişebilmesi ve uzmanlığını sürdürebilmesi için gerekli kaynakları sağlayarak 39. maddede sayılan görevleri ifa etmesi için destekleyecektir. Veri sorumlusu ve veri işleyen tarafından gerekli kaynakların sağlanması geniş olarak yorumlanabilecek bir yükümlülüktür. Bu yükümlülük, şirket içerisindeki İK, IT, güvenlik gibi hizmetlere Veri Koruma Görevlisi'ne direkt erişim yetkisi verilmesi, veri koruma ve diğer ilgili mesleki

[87] IT GOVERNANCE PRIVACY TEAM, s. 78/79.

konularda güncel kalınabilmesi adına eğitimlere dahil edilmesi, şirketin yapısı dikkate alındığında tek bir Veri Koruma Görevlisinin yetersiz kalacağı öngörülüyorsa bir ekip kurulması ve bu ekip içerisinde her bir sorumlunun görevlerin net bir şekilde belirlenmesi gibi çalışmalarla yerine getirilebilir[88].

Veri sorumlusu veya veri işleyen, Veri Koruma Görevlisi'nin, söz konusu görevlerin ifasına ilişkin olarak hiçbir talimat almamasını temin edecek, Veri Koruma Görevlisi, görevlerini ifa ettiği için veri sorumlusu veya veri işleyen tarafından görevden alınamayacak veya cezalandırılamayacak, Veri Koruma Görevlisi, doğrudan veri sorumlusunun veya veri işleyenin en üst yönetim seviyesine rapor verecektir[89]. Veri Koruma Görevlisinin bağımsızlığı, 39. maddede sayılan görevlerinin dışında bir karar verme yetkisine sahip olduğu anlamına gelmemelidir. Altı çizilen konu, görevlerini yerine getirirken herhangi bir baskı altında olmamasının temin edilmesi ile ilgilidir. Veri Koruma Görevlisi, kendisinin veri sorumlusu veya veri işleyen tarafından baskı altına alınmasına müsaade etmemeli, yükümlülüklerin ihlal edilmesini görmesi halinde veri sorumlusu veya veri işleyenin herhangi bir şekilde müdahalesine izin vermeden gerekli işlemleri yapmalı ve ihlalin karşısında durmalıdır[90]. Regülasyon, Veri Koruma Görevlisi'nin hangi durumlarda görevden alınabileceği konusunda bir değerlendirme yapmamıştır. Veri Koruma Görevlisinin yasal olarak garanti altına alınmış bir bağımsızlığı olsa da örneğin ceza kanunu kapsamında bir suç işlemesi halinde normal bir çalışan sözleşmesi hükümleri uyarınca sözleşmesi feshedilebilecektir.

İlgili kişiler, kişisel verilerinin işlenmesine ve Regülasyon'dan kaynaklanan haklarını kullanmalarına ilişkin tüm konularda Veri Koruma Görevlisiyle iletişime geçebilecektir[91]. 37. maddenin 7. fıkrası gereği Veri Koruma Görevlisi'nin iletişim bilgileri yayınlanır ve denetim makamına bildirilir. Veri Koruma

[88] IT GOVERNANCE PRIVACY TEAM, s. 77/78.
[89] LAMBERT, s. 40.
[90] LAMBERT, s. 71-72.
[91] LAMBERT,s. 49.

Görevlisinin erişilebilir olması önemli bir husustur. İletişim bilgilerinin yayınlanması, ilgili kişilerin ya da denetim makamlarının veri sorumlusu ya da veri işleyen içerisinde başkaca hiçbir departmanın aracılığına gerek duymadan Veri Koruma Görevlisi'ne doğrudan ulaşmasını sağlamak açısından yararlı bir uygulamadır. Çalışma Grubu, veri sorumlusu ya da veri işleyenin AB içerisinde kurulmuş olup olmadığına bakılmaksızın, Veri Koruma Görevlisi'nin AB içinde yer almasını önermektedir[92].

Veri Koruma Görevlisi, AB ve üye devlet hukukuna uygun olarak görevlerinin ifasında sır saklama veya gizlilik yükümlülüğü altında olmalıdır.

Veri Koruma Görevlisi, başka görev ve yükümlülükler de ifa edebilir. Veri sorumlusu veya veri işleyen, söz konusu görev ve yükümlülüklerin bir menfaat çatışmasına neden olmadığını temin etmelidir[93]. Veri Koruma Görevlisi'nin, organizasyon içinde kişisel verilerin işlenmesinin amaçlarını ve araçlarını belirleyen bir pozisyonda bulunmaması gerekir. Bir işletme içerisinde, pazarlama sorumlusu, finans, operasyon, İK, IT müdürlüğü gibi üst düzey pozisyonlarda bulunan bir kişinin Veri Koruma Görevlisi olarak atanması halinde, menfaat çatışması gündeme gelmesi olasıdır[94]. Menfaat çatışmasına şu şekilde bir örnek verilebilir; bir şirketin pazarlama sorumlusu, hangi müşterilerin hedefleneceğinin, kullanılacak iletişim yönteminin ve kişisel özelliklerin planlanacağı bir reklam kampanyası hazırlarsa aynı zamanda o şirketin Veri Koruma Görevlisi görevini üstlenemez. Çünkü tüm bu reklam kampanyası, yürütülen politika ve veri koruma yükümlülükleri arasında bir menfaat çatışması ortaya çıkacaktır[95]. Bir başka deyişle, bir IT Müdürü'nün Veri Koruma Görevlisi olarak atanması mümkün olmayacaktır. Şirket dışı atanmış bir Veri Koruma Görevlisi'nin varlığı halinde de olası bir veri koruma ihlali durumunda adli merciler karşısında veri sorumlusunu ya da veri işleyeni temsil etmesi de yine menfaat çatışması halini yaratacaktır.

[92] Art. 29 WP, Guidelines on "DPOs", s. 11.
[93] LAMBERT, s. 49; [93] IT GOVERNANCE PRIVACY TEAM, s. 69.
[94] CLIZA, s. 496; IT GOVERNANCE PRIVACY TEAM, s. 69.
[95] ICO, Guide to the GDPR, s. 197.

Regülasyon kapsamında üye devletlere Veri Koruma Görevlisi'nin veri sorumlusunun ya da işleyenin organizasyonu içindeki konumu bakımından ek yükümlülükler yükleme imkanı bahşedilmiştir. Bu kapsamda, üye devletler belirli sektörlerde faaliyet gösteren veri sorumlulukları bakımından birer Veri Koruma Görevlisi'nin atanmasını zorunlu tutabilirler[96].

2.7.6.2. Regülasyon kapsamında Veri Koruma Görevlisi, İrtibat Kişisi ve Veri Sorumlusu Temsilcisi Kavramları

Veri koruma görevlisi, Regülasyon kapsamında yukarıda görüleceği üzere birçok görevle görevlendirilmiştir ancak çalışmanın önceki bölümlerinde yer alan "Temsilci"[97] ve ileriki bölümlerinde yer alan "Veri Sorumlusu Temsilcisi"[98] ve "İrtibat Kişisi"[99] konularında da işaret edildiği üzere, bu kişilerin veri sorumluları veya veri işleyen ile arasındaki hukuki ilişkinin nitelendirmesine göre sorumlulukları farklılık gösterecektir.

Regülasyon'da Veri Koruma Görevlisi'ni açıklayan 37. maddede Veri Koruma Görevlisi'nin atanması gereken haller sayılmıştır. Veri Koruma Görevlisi ataması gereken haller yukarıda incelenmişti. Ancak özetle hatırlatmak gerekirse, veri işlemenin yargısal faaliyette bulunan mahkemeler hariç, kamu kurum ve kuruluşu tarafından gerçekleştirilmesi halinde; ya da veri sorumlusunun esas faaliyetin, ilgili kişilerin düzenli ve sistematik olarak geniş çaplı izlenmesini gerektirmesi ya da veri sorumlusunun esas faaliyetin, özel nitelikli kişisel verilerin veya cezai hükümler ve suçlarla ilgili kişisel verilerin geniş çapta işlenmesini gerektirmesi hallerinde veri sorumlusu ve/veya veri işleyen Veri Koruma Görevlisi atamak durumunda kalacaktır.

[96] IT GOVERNANCE PRIVACY TEAM, s. 70.
[97] Bkz: s. 29.
[98] Bkz: s. 109.
[99] Bkz: s. 119.

AB içerisinde merkezi bulunmayan bir veri sorumlusunun "Temsilci" mi yoksa "Veri Koruma Görevlisi" mi ataması gerektiği sorusu ise yukarıda sayılan son iki kritere göre cevaplanmalıdır. Eğer ilgili veri sorumlusu, düzenli ve sistematik olarak geniş çaplı izleme ile veri işlemiyor ya da esas faaliyeti özel nitelikli kişisel verilerin veya cezai hükümler ve suçlarla ilgili geniş çapta veri işlemesini gerektirmiyorsa, Regülasyon kapsamında, veri sorumlusundan Veri Koruma Görevlisi ataması beklenmeyecektir. Temsilci atama yükümlülüğü ise ancak Regülasyon 3. madde 2. fıkrada belirtilen hallerde söz konusu olacaktır:[100].Buna göre de kamu kurumları temsilci atama yükümlülüğünden muaf olmakla birlikte, AB dahilinde merkezi bulunmamasına rağmen, AB dahilindeki kişilere mal ve hizmet sunan ve AB dahilindeki kişilerin davranışlarını izleyen, ancak; özel nitelikli kişisel verilerin veya cezai hükümlere ve suçlara ilişkin verileri işlemeyen veri sorumluları ve işlemenin doğası, kapsamı ve amaçları gereği kişilerin hak ve özgürlükleri açısından risk teşkil etmeyen veri işleme süreçlerine sahip veri sorumluları temsilci atama yükümlülüğünden muaftır.

Temsilci başlığı altında ifade edildiği gibi, temsilci atama yükümlülüğü bulunan bir veri sorumlusu tarafından atanan bir temsilci, kendi görevleri yanı sıra, yerel denetim makamları ve ilgili kişiler karşısında muhatap konumunda da görev alacaktır. Regülasyon irtibat kişisi kavramına yer vermemektedir, temsilcinin bir şekilde yüklendiği görevlerden biri de muhatap olarak adlandırılabilir.

Regülasyon'da düzenlenmiş olan temsilci kurumu, Regülasyon'a uyum, veri işleme süreçlerini kayıt altına alma ve denetim makamları ve ilgili kişilerle iletişimi sağlama görevleriyle görevlendirilmişken, Türk Hukukunda yer alan ve çalışmanın ileriki bölümlerinde detaylı olarak incelenecek olan "veri sorumlusu

[100] https://ico.org.uk/for-organisations/data-protection-and-brexit/data-protection-if-there-s-no-brexit-deal/the-gdpr/european-representatives/ Erişim Tarihi: 20.03.2019.

temsilcisi" kurumu görev olarak "temsilci"den ayrılmaktadır. Temsilci, AB içerisinde merkezi bulunmayan veri sorumluları tarafından atanması gereken bir kişi, veri sorumlusu temsilcisi de Türkiye'de merkezi bulunmayan veri sorumluları tarafından atanması gereken bir kişi olarak karşımıza çıkmakta. Veri sorumlusu temsilcisi ve temsilci, atanma sebepleri olarak birbirine yakın anlamlar taşımaktalarsa da görev olarak farklılıklar mevcuttur. Veri sorumlusu temsilcisi, çalışmanın ileriki bölümlerinde detaylı anlatılacağı üzere, temsilcinin aksine yasal düzenlemelere uyum ve veri işleme süreçlerini kayıt altına alma gibi bir yükümlülük altına sokulmamıştır[101]. Veri sorumlusu temsilcisinin temsilciye göre görevleri daha sınırlı olarak karşımıza çıkmaktadır.

2.7.7. Veri Koruma Görevlisi'nin Atanmamasının Tabi Olacağı Yaptırım

Regülasyon'un 83. Maddesinin 4. fıkrası gereğince; zorunlu olarak Veri Koruma Görevlisi atanması öngörülen veri sorumlularında, Veri Koruma Görevlisi atanmamış olması durumunda; 10.000.000 Euro'ya veya bu rakamdan yüksekse, işletmenin bir önceki mali yılda dünya çapında toplam yıllık cirosunun %2'sine kadar idari para cezası öngörülmüştür. AB hukuku, üye devletlerin iç hukuk düzenlemelerinde aksi düzenlenmedikçe, kamu kurum ve kuruluşlarına idari para cezalarının uygulanmasını öngörmüştür, bu nedenle aynı maddenin 7. fıkrası, üye devletlerin, ilgili üye devlette bulunan kamu kurum ve kuruluşlarına idari para cezası verilmesi konusunda düzenleme yapabileceğini hüküm altına almıştır[102].

[101] Bkz: s. 109.
[102] CLIZA, s. 499.

3. TÜRKİYE'DE VERİ SORUMLUSUNUN 6698 SAYILI KİŞİSEL VERİLERİN KORUNMASI KANUNU KAPSAMINDAKİ KONUMU

3.1.Ulusal Düzenlemeler

Çalışmanın ilk bölümünde de açıklandığı üzere, gelişen ve küreselleşen dünyada kişisel verinin işlenmediği hemen hemen tek bir sektör bile kalmamıştır. Ulusal ticaret dikkate alındığında ülkemizde de kişisel verilerin işlenmesinin oldukça yaygın olduğu, ilgili kişilerin ve veri sorumlularının hak ve yükümlülüklerinin belirlenmesi, uluslararası ticaret dikkate alındığında ise ilgili kişilerin verilerinin, yurtdışına aktarımı gibi konuların yasal düzenlemeye ihtiyaç duyması gibi nedenlerle ülkemizde de yasal bir düzenlemeye gidilmesi ihtiyacı gün geçtikçe artmıştır. Ticari ilişkilerin dışında, özellikle belirli sektörlerde veri işlemenin oldukça sık olduğu ve bu sektörlerde ilgili kişilerin haklarının ne derecede korunduğuna ilişkin soru işaretleri mevcuttur. Temel insan haklarından biri olan veri koruması hakkı ile birlikte, orantılılık ilkesi de göz önünde tutularak gerek özel sektör gerek devlet karşısında bireyin hukuki bir koruma altına alınması ve bu korumayla birlikte ilgili kişilerin hayatlarına teknolojinin dahil olması sağlanmalıdır[103]. Örneğin, veri işlemenin oldukça yoğun olarak yapıldığı sağlık sektörüne bakılacak olursa, Türk Tabipler Birliği'ne yapılan başvurulardan anlaşılmaktadır ki, hastaların verilerine ilişkin yeterli koruma sağlanamamakta, hastaların onamı alınmadan verilerin açıklanmaktadır[104]. Keza 01.12.2013 tarihinden itibaren, "Biyometrik Kimlik Doğrulama Sistemi" ile hastaların avuç içi, damar izinin alınması gibi veri korumasına aykırı uygulamalar özel hastalenerde uygulanmaya başlanmıştır[105]. 6698 sayılı Kişisel Verileri Koruma Kanunu'nun (KVKK) (Çalışmanın bundan sonraki bölümlerinde "Kanun" olarak anılacaktır.) Genel Gerekçesinde de belirtildiği üzere; günümüzde kişisel verilerin özel sektör ve kamu sektöründe, bilişim sistemleri üzerinden kullanılması her iki

[103] KESER/ KAYA/ KINIKOĞLU, s. 73.
[104] Sabire Sanem YILMAZ, Tıp Alanında Kişisel Verilerin Açıklanması Suçu, Terazi Aylık Hukuk Dergisi 11 (119), Temmuz 2016, s. 273.
[105] YILMAZ, s. 274.

sektöre ve ilgili kişilere kolaylıklar sağlasa da yetkisiz kişilerin ele geçirmesi halinde problemlerin ortaya çıkacağı da öngörülmelidir. Bu iki menfaat arasında makul bir dengenin oluşturulması gerekmektedir[106]. Kanun'un 3. maddesinde tanımlandığı üzere; *"Kişisel veri: kimliği belirli veya belirlenebilir gerçek kişiye ilişkin her türlü bilgi"*yi ifade ederken, *"Kişisel verilerin işlenmesi ise: kişisel verilerin tamamen veya kısmen otomatik olan ya da herhangi bir veri kayıt sisteminin bir parçası olmak kaydıyla otomatik olmayan yollarla elde edilmesi, kaydedilmesi, depolanması, muhafaza edilmesi, değiştirilmesi, yeniden düzenlenmesi, açıklanması, aktarılması, devralınması, elde edilebilir hale getirilmesi, sınıflandırılması ya da kullanılmasının engellenmesi gibi veriler üzerinde gerçekleştirilen her türlü işlemi"* ifade etmektedir. Hazırlanan yasal düzenlemelerin temelinde bu iki kavram yer almakla birlikte tüm bu verilerin ve işleme süreçlerinin ne şekilde ilerlemesi gerektiği, dikkat edilmesi gereken hususlar, yasal yükümlülükler, sorumluluk altına giren süjelerin belirlenebilmesi için yasal çalışmaların gerekliliği ortaya çıkmıştır.

Ülkemizde kişisel verilere ilişkin bütüncül bir yasal düzenleme geçmiş yıllara kadar bulunmamaktayken, çeşitli kanun ve yönetmelikler ile bazı düzenlemeler yapılmıştır.

Kanun yürürlüğe girene dek ülkemizde kişisel verilerin korunmasına ilişkin yeknesak bir düzenleme yer almamaktaydı. 4721 Sayılı Türk Medeni Kanunu'nun (TMK) 23., 24. ve 25. maddeleri kişiliğin korunmasına ilişkindir. TMK 23. maddesi ile kişinin herhangi bir hukuki işlem ile hak ve fiil ehliyetlerinden, temel hak ve özgürlüklerinden vazgeçemeyeceği, bunları hiçbir şekilde sınırlayamayacağı, TMK 24. maddesi ile kişilik hakkına saldırı teşkil eden üçüncü kişilerin hukuka aykırı fiilleri karşısında kişinin hakimden koruma talep edebileceği, TMK 25. maddesi ile ise hakimden koruma talep edilmesi halinde kişilik hakkına saldırı halinde, saldırının durdurulması, önlenmesi veya tespiti

[106]Kişisel Verilerin Korunması Kanunu Genel Gerekçesi, https://www.tbmm.gov.tr/sirasayi/donem26/yil01/ss117.pdf, s. 4, Erişim Tarihi: 18.12.2018.

şeklinde üç farklı dava açılabileceği hüküm altına alınmıştır[107]. 6098 Sayılı Türk Borçlar Kanunu'nun (TBK) 27. maddesine göre, kişilik hakkını sınırlayıcı nitelikte, karşı tarafa aşırı ve hakkaniyete aykırı güvenceler sağlayan, sözleşmeye kendi rızasıyla taraf olsa dahi ölçüsüz ve sınırlayıcı hükümlerle kişilik haklarını ihlal eden sözleşmeler kesin hükümsüzdür. TBK'nın 58. maddesi ise, *"Kişilik hakkının zedelenmesinden zarar gören, uğradığı manevi zarara karşılık manevi tazminat adı altında bir miktar para ödenmesini isteyebilir."* Demektedir. 2005 yılında yürürlüğe giren 5237 sayılı Türk Ceza Kanunu'nun (TCK) 135, 136, 138. maddeleri de kişisel verilerin hukuka aykırı şekilde kaydedilmesi, verilmesi ya da elde edilmesi, sürelerin geçmesine rağmen yok edilmemesi konularını düzenlemiştir. Bu üç suç için de korunan hukuki değerin kişinin özel hayatı olduğu söylenebilir[108]. 2010 yılında gerçekleştirilen Anayasa değişikliği ile "Özel Hayatın Gizliliği" başlıklı 20. maddeye eklenen bir hükümle birlikte, kişisel verilerin korunmasını isteme hakkı düzenlenmiştir.

TCK 135. maddesi: "Hukuka aykırı olarak kişisel verileri kaydeden kimseye bir yıldan üç yıla kadar hapis cezası verilir."

"Kişisel verinin, kişilerin siyasi, felsefi veya dini görüşlerine, ırki kökenlerine; hukuka aykırı olarak ahlaki eğilimlerine, cinsel yaşamlarına, sağlık durumlarına veya sendikal bağlantılarına ilişkin olması durumunda birinci fıkra uyarınca verilecek ceza yarı oranında artırılır." Demektedir. Maddenin gerekçesi[109] ise şu şekildedir:

---

[107] Kemal ATASOY, Kişilik Hakkı Kapsamında Sosyal Medyada Kişisel Verilerin Korunması ve Veri Sahibinin Rızası, T.C. Marmara Üniversitesi Hukuk Fakültesi Hukuk Araştırmaları Dergisi Prof. Dr. Cevdet Yavuz'a Armağan I. Cilt 22 (3), İstanbul, 2016, s. 274.

[108] Veli Özer ÖZBEK/ Mehmet Nihat KANBUR/ Koray DOĞAN/ Pınar BACAKSIZ/ İlker TEPE, Türk Ceza Hukuku Özel Hükümler, Güncellenmiş ve Genişletilmiş 6. Baskı, Seçkin Yayınevi, Ankara, Mart 2014, 526, 537, 540.

[109] Gazi Üniversitesi, Türk Ceza Hukuku Uygulama ve Araştırma Merkezi, Türk Ceza Hukuku Mevzuatı Cilt 1, Güncellenmiş 20. Baskı, Seçkin Yayınevi, Ankara, Ekim 2017, s. 345.
TBMM, Dönem: 22, Yasama Yılı:2, Sıra Sayısı: 664, s. 544.

“Çağımızda kişilerle ilgili kayıtların bilgisayar ortamlarına geçirilip muhafaza edilmesi uygulamasına bazı kamu kurum ve kuruluşlar tarafından başvurulmaktadır; hastanelerde hastalara, sigorta şirketlerinde sigortalılara, bankaların ve kredili alışveriş yapan mağazaların müşterilerine ilişkin kayıtlar, böylece tutulmaktadır. Bu bilgilerin amaçları dışında kullanılmasından veya herhangi bir şekilde üçüncü şahısların eline geçerek hukuka aykırı olarak yararlanılmasından dolayı hakkında bilgi toplanan kişiler büyük zararlara uğrayabilmektedirler. Bu bakımdan, kişilerle ilgili bilgilerin hukuka aykırı olarak kayda alınması suç olarak tanımlanmıştır.”

“Suçun konusu kişisel verilerdir. Gerçek kişiyle ilgili her türlü bilgi, kişisel veri olarak kabul edilmelidir.”

“Söz konusu suç tanımında kişisel verilerin bilgisayar ortamında veya kâğıt üzerinde kayda alınması arasında bir ayrım gözetilmemiştir. Bu bakımdan, söz konusu suç tanımı ile, Avrupa Konseyi bünyesinde hazırlanan Türkiye’nin 28 Ocak 1981 tarihinde imzalamakla taraf olduğu ‘Kişisel Nitelikteki Verilerin Otomatik İşleme Tabi Tutulması Karşısında Şahısların Korunmasına Dair Sözleşme’nin ilgili hükümlerine geçerlilik tanınmıştır.”

“Bu suçun oluşabilmesi için, kişisel verilerin hukuka aykırı bir şekilde kayda alınması gerekir. Kişinin rızası ile, kendisiyle ilgili bilgilerin kayda alınmasının suç oluşturmayacağı muhakkaktır. Belirli nitelikteki kişisel verilerin kayda alınması kanun hükmü gereği olarak yapılmaktadır. Bu bakımdan, çeşitli kamu kurumlarında verilen kamu hizmetinin gereği olarak kişilerle ilgili bazı bilgiler ilgili kanun hükümlerine istinaden kayda alınmaktadırlar. Bu durumlarda, söz konusu suç oluşmayacaktır.”

“Maddenin ikinci fıkrasında, kişilerin siyasi, felsefi veya dini görüşlerine, ırki kökenlerine, ahlaki eğilimlerine, cinsel yaşamlarına, sağlık durumlarına veya sendikal bağlantılarına ilişkin bilgileri kayda almak, suç olarak tanımlanmıştır.

Ancak, bunlardan kişilerin ahlaki eğilimlerine, cinsel yaşamlarına, sağlık durumlarına veya sendikal bağlantılarına ilişkin bilgilerin kayda alınmasına kanunlarda özellikle suçlulukla mücadele bağlamında, suç ve suçluların ortaya çıkarılmasını sağlamak amacıyla belli ölçüde izin verilebilir. Bu durumlarda söz konusu suç oluşmayacaktır."

TCK 136. maddesi: "Kişisel verileri, hukuka aykırı olarak bir başkasına veren, yayan veya ele geçiren kişi, iki yıldan dört yıla kadar hapis cezası ile cezalandırılır." Demektedir. Maddenin gerekçesi[110] ise şu şekildedir:

"Bu madde hükmü ile, hukuka uygun olarak kaydedilmiş olsun veya olmasın, kişisel verileri hukuka aykırı olarak başkalarına vermek, yaymak veya ele geçirmek, bağımsız bir suç olarak tanımlanmıştır."

Madde gerekçesinden de anlaşılacağı üzere, hukuka uygun olarak elde edilmiş bir verinin, daha sonrasında hukuka aykırı olarak ele geçirilmesi halinde de TCK 136. madde uygulama alanı bulacaktır[111]. Seçimlik hareketli bir suç olarak düzenlenen madde, belirtilen verme, yayma, ele geçirme eylemlerinden biriyle gerçekleşeceğinden bağlı hareketli suç olarak değerlendirilecektir.

TCK 135. ve 136. maddeler için nitelikli haller 137. maddede sayılmıştır. Buna göre söz konusu suçun "Kamu görevlisi tarafından ve görevin verdiği yetki kötüye kullanılmak suretiyle, Belli bir meslek ve sanatın sağladığı kolaylıktan yararlanmak suretiyle işlenmesi halinde verilecek ceza yarı oranında artırılır."

[110] Gazi Üniversitesi, Türk Ceza Hukuku Uygulama ve Araştırma Merkezi, Türk Ceza Hukuku Mevzuatı Cilt 1, Güncellenmiş 20. Baskı, Seçkin Yayınevi, Ankara, Ekim 2017, s. 346.
TBMM, Dönem: 22, Yasama Yılı:2, Sıra Sayısı: 664, s. 546.
[111] Doğan SOYASLAN, Ceza Hukuku Özel Hükümler, Gözden Geçirilmiş 8. Baskı, Yetkim Yatınları, Ankara, 2010, s. 345, 346.

TCK 138. maddesi: “Kanunların belirlediği sürelerin geçmiş olmasına karşın verileri sistem içinde yok etmekle yükümlü olanlara görevlerini yerine getirmediklerinde bir yıldan iki yıla kadar hapis cezası verilir”

“Suçun konusunun Ceza Muhakemesi Kanunu hükümlerine göre ortadan kaldırılması veya yok edilmesi gereken veri olması halinde verilecek ceza bir kat artırılır.” Demektedir. Maddenin gerekçesi[112] ise şu şekildedir:

“Bu madde hükmü ile, hukuka uygun olarak kaydedilmiş olan kişisel verilerin kanunların belirlediği sürelerin geçmiş olmasına rağmen yok edilmemesi, bağımsız bir suç olarak tanımlanmıştır.”

Madde, verilerin yok edilmemesi üzerine oluşturulduğundan, suçun ihmali bir suç olduğu değerlendirilebilir. Kanunların belirlediği süreler geçmiş olmasına karşın veriler yok edilmemişse ya da kanunlarda bir süre öngörülmeyen hallerin varlığında, işin niteliği gereği belirlenen makul süre içerisinde verilerin yok edilmemesi ile suç oluşacaktır[113]. Mevzuatta bazen, verilerin belli kararların verilmesi halinde yok edileceğine ilişkin düzenlemeler de yer almaktadır, örneğin fizik kimliğin tespiti sonucu elde edilen veriler bakımından CMK 81. Maddenin 2. Fıkrası “Kovuşturmaya yer olmadığı veya beraat kararı verilmesi hallerinde söz konusu kayıtlar Cumhuriyet savcısının huzurunda derhal yok edilir ve bu husus tutanağa geçilir.” Demektedir[114].

Kanun ile birlikte, TCK kapsamında düzenlenmiş bulunan ilgili maddeler daha anlaşılır hale gelerek, pasif durumda kalmayacak, TCK’da düzenlenen ilgili maddelerin ne zaman hukuka aykırı ne zaman hukuka uygun olduğu, hangi

[112] Gazi Üniversitesi, Türk Ceza Hukuku Uygulama ve Araştırma Merkezi, Türk Ceza Hukuku Mevzuatı Cilt 1, Güncellenmiş 20. Baskı, Seçkin Yayınevi, Ankara, Ekim 2017, s. 347.
TBMM, Dönem: 22, Yasama Yılı:2, Sıra Sayısı: 664, s. 546.
[113] SOYASLAN, s. 351.
[114] ÖZBEK/ KANBUR/ DOĞAN/ BACAKSIZ/ TEPE, s. 541.

verilerin kişisel veri olarak kabul edileceği gibi konularda yaşanacak tereddütler ortadan kalkacaktır[115].

Farklı yönetmelikler altında düzenlenmeler oluşturulmuştur, ancak bu düzenlemeler etkin bir koruma sağlayacak derecede geniş tutulmamıştır. 2004 yılında "Telekomünikasyon Sektöründe Kişisel Bilgilerin İşlenmesi ve Gizliliğin Korunması Hakkında Yönetmelik" ile bir düzenleme oluşturulmuş, sonrasında bu düzenleme, 5.11.2008 tarihli ve 5809 sayılı Elektronik Haberleşme Kanununun 4, 6, 12 ve 51. maddelerine dayanılarak hazırlanan; 24.07.2012 tarih ve 28363 sayılı Resmî Gazete'de yayınlanan "Elektronik Haberleşme Sektöründe Kişisel Verilerin İşlenmesi ve Gizliliğin Korunması Hakkında Yönetmelik" ile yürürlükten kaldırılmıştır.

Kişisel verilerin korunmasına ilişkin yasal düzenlemeler, Ülkemizde AB'ye nazaran daha geç oluşturulmaya başlanmıştır. Türkiye'de kişisel verilerin korunmasına yönelik kanun çalışmalarının 1989 yılında başladığı belirtilmektedir. Kişisel verilerin korunmasına ilişkin yasa tasarısı hazırlamak üzere ilk komisyon 13 Eylül 1995'te kurulmuştur. Ancak bu komisyon çalışmalarını tamamlayamamıştır. Daha sonra 2000 yılında oluşturulan ikinci komisyon üç yıllık bir çalışmanın ardından Kişisel Verilerin Korunması Kanun Tasarısını hazırlamıştır. Adalet Bakanlığı tarafından 7 Eylül 2003 tarihinde açıklanan bu tasarı, AB raporlarında ve e-Dönüşüm Türkiye Projesi Kısa Dönem Eylem Planlarında konuya ilişkin ifadelerin yer almasına karşın yasalaşmamıştır. Adalet Bakanlığınca 2003 yılında hazırlanan bu ilk tasarı, ilk kez 22 Nisan 2008 tarihinde TBMM'ye sevk edilmiştir. Adalet Alt Komisyonunda iki toplantı gerçekleşse de Tasarı, Genel Kurul'a sevk edilemeden, seçimlerin yenilenmesi nedeniyle hükümsüz kalmıştır. 2011 yılında yeni bir tasarı taslağı gündeme gelmiştir. Adalet Bakanlığında oluşturulan Komisyon'da tasarı taslağı yenilenmiş ve 2012 yılında Başbakanlığa gönderilmiştir. 2014 yılının son haftasında ise yeni bir tasarı bir kez

[115] KESER/ KAYA/ KINIKOĞLU, s. 45.

daha TBMM'ye sevk edilmiştir. Seçimler dolayısıyla bu tasarı TBMM'de görüşülmemiş ve önceki metnin akıbetine benzer şekilde hükümsüz kalmıştır. Belirtilen metni temel alan, ancak üzerinde önemli değişiklikler yapılan yeni tasarı ise Bakanlar Kurulunda kabul edilmesinin ardından 18 Ocak 2016'da TBMM'ye sevk edilmiştir[116].

3.2.6698 Sayılı Kişisel Verileri Koruma Kanunu

Anayasa'nın 20. maddesi'nde kişisel verilerin korunmasına ilişkin esas ve usullerin kanunla düzenleneceği belirtilmiş, 26 Aralık 2014'te "Kişisel Verilerin Korunması Kanunu Tasarısı" TBMM Başkanlığı'na sunulmuş, 24 Mart 2016 tarihinde kanunlaşmış, 7 Nisan 2016 tarihinde de 29677 sayılı Resmî Gazete'de yayınlanmıştır.

Kanunun Genel Gerekçesi'nde yasanın yürürlüğe girmesini gerektiren değişik sebeplerin olduğu belirtilmiştir. Bu kapsamda özellikle dikkat çeken gerekçeler şöyle sıralanabilir[117]:

- TCK'da konuya ilişkin suç ve cezaların belirlenmesi, ancak konuya ilişkin özel bir düzenleme bulunmaması nedeniyle, bir fiilin ne zaman hukuka aykırı olduğunun belirlenmesinin güçlüğü,
- Anayasanın 20. maddesi gereği kişisel verilerin korunmasına ilişkin yasa ile düzenleme yapılması gerekliliği,
- AB üyelik sürecinin ilerleyebilmesi,
- EUROPOL ve EUROJUST ile iş birliği yapılamaması ve elektronik bilgi paylaşımının gerçekleştirilememesi,
- Sağlık verilerinin tutulmasına ilişkin yasal düzenleme eksikliği ve AİHM'nin bu konuyla alakalı ihlal kararları,

[116] KÜZECİ, s. 311-312.
[117] KÜZECİ, s. 312-313.

- Türkiye'de yaşayan yabancılar ile yurtdışında yaşayan T.C. yurttaşları açısından veri paylaşımında sorunların yaşanması,
- Kişisel Verilerin Korunması Kanunu'nun Türkiye'nin Katılım Ortaklığı Belgesine yanıt olarak hazırladığı 2003 Ulusal Programında taahhüt ettiği yükümlülükler arasında yer alması,
- 64. Hükümet 2016 yılı Eylem Planında üç ay içerisinde gerçekleştirilecek reformlar arasında kişisel verilerin korunmasına yönelik bir kanunun çıkarılmasının yer alması,
- Ekonomik kayıplar.

Kanun'un 1. maddesinde, Kanun'un amacının, kişisel verilerin işlenmesinde, başta özel hayatın gizliliği olmak üzere, kişilerin temel hak ve özgürlüklerini korumak ve kişisel verileri işleyen gerçek ve tüzel kişilerin yükümlülükleri ile uyacakları usul ve esasları düzenlemek olduğu belirtilmiştir. Görüleceği üzere Kanun, verinin kendisinin korunmasını direkt olarak hedeflemeden, temelde hak ve özgürlükleri korumayı amaç edinmiştir. Kanun'la birlikte kişisel verilerin korunması, aslında temel hak ve özgürlüklerin korunmasına hizmet etmektedir. Kanun'un uygulama alanı içerisine ise, verileri işlenen gerçek kişiler ve veri işleme işlemini gerçekleştiren gerçek ve tüzel kişiler girmektedir[118].

Kanun, kişisel verilerin işlenme şartlarını 5. maddede saymıştır. Kural olarak; kişisel veriler, ilgili kişinin açık rızası olmaksızın işlenemez, ilgili kişinin açık rızasının aranmaksızın kişisel verilerin işlenmesinin mümkün olduğu haller de ilgili maddenin 2. fıkrasında sayılmıştır. Buna göre;

- Kanunlarda açıkça öngörülmesi

[118] Afra Ece KAYA, Kişilik Hakkı Olarak Kişisel Veriler ve Yeni Kişisel Verilerin Korunması Kanunu, Terazi Aylık Hukuk Dergisi 12 (125), Ocak 2017, s. 76.

- Fiili imkânsızlık nedeniyle rızasını açıklayamayacak durumda bulunan veya rızasına hukuki geçerlilik tanınmayan kişnin kendisinin ya da bir başkasının hayatı veya beden bütünlüğünün korunması için zorunlu olması
- Bir sözleşmenin kurulması veya ifasıyla doğrudan doğruya ilgili olması kaydıyla, sözleşmenin taraflarına ait kişisel verilerin işlenmesinin gerekli olması
- Veri sorumlusunun hukuki yükümlülüğünü yerine getirebilmesi için zorunlu olması
- İlgili kişinin kendisi tarafından alenileştirilmiş olması
- Bir hakkın tesisi, kullanılması veya korunması için veri işlemenin zorunlu olması
- İlgili kişinin temel hak ve özgürlüklerine zarar vermemek kaydıyla, veri sorumlusunun meşru menfaatleri için veri işlenmesinin zorunlu olması
- Hallerinin varlığı halinde ilgili kişinin açık rızası aranmaksızın kişisel verilerinin işlenmesi mümkün olacaktır.

Kurul'un 16.10.2018 Tarihli ve 2018/119 Sayılı ilke kararı ile, *"ilgili kişilerin rızalarını almadan veya Kanun'un 5. maddesinin 2. fıkrasında hüküm altına alınan işleme şartlarını sağlamadan, telefon numaralarına SMS göndermek, arama yapmak veya e-posta adreslerine posta göndermek suretiyle reklam içerikli ileti yönlendiren veri sorumluları ile veri sorumluları adına reklam içerikli mesaj ve/veya e-posta göndermek veya arama yapmak amacıyla ilgili kişilerin açık rızaları bulunmaksızın bu verileri kullanan veri işleyenlerin söz konusu veri işleme faaliyetlerini Kanun'un 15. maddesinin 7. fıkrası uyarınca derhal durdurulması gerektiği"* belirtilmiştir[119]. İlgili kişilerin reklam bildirimleri ile sıkça rahatsız edilmesi ve bu durum üzerine Kurul'a gelen çok sayıda başvuru ile Kurul izinsiz reklam iletileri konusunda ilke karar alma yoluna gitmiştir. Kurul, Kanun'da belirtilen "açık rıza aranmaksızın veri işlemenin mümkün olduğu haller" içerisine girmeyen ve ilgili kişilerden açık rıza alınmadan ilgili kişilere

[119]Kişisel Verileri Koruma Kurulu, https://kvkk.gov.tr/Icerik/5299/2018-119, Erişim Tarihi: 16.02.2019.

gönderilen reklam iletilerinin Kanun'a aykırı olduğu sonucuna vararak, söz konusu faaliyetlerde bulunan veri sorumlularına Kanun'un 18. Maddesi gereği yaptırımlar uygulanacağını ve aynı zamanda TCK kapsamında da "Verileri Hukuka Aykırı Olarak Verme veya Ele Geçirme" başlıklı 136. madde gereğince ilgili Cumhuriyet Başsavcılığına bildirimde bulunacağını bildirmiştir.

Kişisel veriler içerisinde yer alan bazı alanlara ilişkin veriler ise Kanun'da ve ulusal ve uluslararası diğer yasal metinlerde ayrı bir adlandırmayla ayrı tutulmuştur. Kanun'da; *"Kişilerin ırkı, etnik kökeni, siyasi düşüncesi, felsefi inancı, dizi, mezhebi veya diğer inançları, kılık kıyafeti, dernek, vakıf veya sendika üyeliği, sağlığı, cinsel hayatı, ceza mahkumiyeti ve güvenlik tedbirleriyle ilgili verileri ile biyometrik ve genetik veriler"* özel nitelikli kişisel veri olarak adlandırılmıştır ve sınırlı sayı prensibi ile belirlenen bu özel nitelikli kişisel verilerin, ilgilinin açık rızası olmaksızın işlenmesi de yasaktır.

Kanun, özel nitelikli kişisel veriler arasında bir ayrıma gitmiştir. Sağlık ve cinsel hayata ilişkin veriler ile bunlar dışındaki özel nitelikli kişisel verilerin, açık rıza olmaksızın işlenebileceği haller farklı şekilde düzenlenmiştir, sağlık ve cinsel hayat dışındaki özel nitelikli kişisel veriler, kanunlarda öngörülen hallerde, sağlık ve cinsel hayata ilişkin kişisel veriler ise ancak, kamu sağlığının korunması, koruyucu hekimlik, tıbbi teşhis, tedavi ve bakım hizmetlerinin yürütülmesi, sağlık hizmetleri ile finansmanının planlanması ve yönetimi amacıyla, sır saklama yükümlülüğü altında bulunan kişiler veya yetkili kurum ve kuruluşlar tarafından işlenebilecektir[120].

Bu tür kişisel verilerin, diğer kişisel verilerden ayrı olarak koruma altına alınmasının nedeni, özellikle İkinci Dünya Savası sonrası yaşanan ayrımcılığın bir yansıması olarak; ilgili kişilerin bu tür verilerin kullanılması ile birlikte

[120] Kişisel Verileri Koruma Kurumu, Özel Nitelikli Kişisel Verilerin İşlenme Şartları, s. 3.

ayrımcılığa uğrama tehdidini ortadan kaldırma amacıdır[121]. AİHM de kişisel verilerin işlenmesi nedeniyle ortaya çıkabilecek olası zararların derecesine göre bir ayrım yapılmasını uygun görmektedir.

Şekil 1: Özel Nitelikli Kişisel Verilerin İşleme Şartları

İşleme Şartları	Kapsam	Örnek
İlgili Kişinin Açık Rızası	İlgili kişinin açık rızasının alınmış olması	Klinik araştırmalar kapsamında gönüllülerin rızasının alınması.
Kanun Hükmü	Sağlık ve cinsel hayat dışındaki kişisel veriler ilgili kişinin açık rızası aranmaksızın işlenebilir. Vergi Kanunları, İş Kanunu, Türk Ticaret Kanunu vb. daha sıkı hassas veri işleme şartları.	Çalışana ait sendikalılık bilgisinin özlük dosyasında mevzuat gereği tutulması gerekir.
Kamu sağlığının korunması, koruyucu hekimlik, tıbbî teşhis, tedavi ve bakım hizmetlerinin yürütülmesi ile sağlık hizmetlerinin planlanması, yönetimi ve finansmanı	Kamu sağlığının korunması, koruyucu hekimlik, tıbbî teşhis, tedavi ve bakım hizmetlerinin yürütülmesi ile sağlık hizmetlerinin planlanması, yönetimi ve finansmanı amacıyla, sır saklama yükümlülüğü altında bulunan kişiler veya yetkili kurum ve kuruluşlar tarafından işlenmesi	Doktorun hastası hakkında işlediği sağlık verileri.

Kaynak: Kişisel Verileri Koruma Kurumu, Özel Nitelikli Kişisel Verilerin İşlenme Şartları, s. 5., Erişim Tarihi: 12.02.2018

[121] Murat Volkan DÜLGER, Kişisel Verilerin Korunması Kanunu ve Türk Ceza Kanunu Bağlamında Kişisel Verilerin Ceza Normlarıyla Korunması, İstanbul Medipol Üniversitesi Hukuk Fakültesi Dergisi 3 (2) Güz 2016; 101-167, s. 109.

Kanun'un 6. maddesinin 4. fıkrasında da belirtildiği üzere; *"özel nitelikli kişisel verilerin işlenmesinde, ayrıca Kurul tarafından belirlenen yeterli önlemlerin alınması şarttır."* Bu kapsamda da Kurul, özel nitelikli kişisel verilerin işlenme şartlarını bir rehber ile belirlemiş ve özel nitelikli kişisel verilerin işlenmesinde veri sorumlularınca alınması gereken yeterli önlemlere ilişkin 31.01.2018 Tarih 2018/10 Sayılı Kararı[122] ile veri sorumlularının özel nitelikli kişisel verileri işlerken alması gereken önlemleri de belirlemiştir. Buna göre;

"1- Özel nitelikli kişisel verilerin güvenliğine yönelik sistemli, kuralları net bir şekilde belli, yönetilebilir ve sürdürülebilir ayrı bir politika ve prosedürün belirlenmesi,

2- Özel nitelikli kişisel verilerin işlenmesi süreçlerinde yer alan çalışanlara yönelik,

a) Kanun ve buna bağlı yönetmelikler ile özel nitelikli kişisel veri güvenliği konularında düzenli olarak eğitimler verilmesi,

b) Gizlilik sözleşmelerinin yapılması,

c) Verilere erişim yetkisine sahip kullanıcıların, yetki kapsamlarının ve sürelerinin net olarak tanımlanması,

ç) Periyodik olarak yetki kontrollerinin gerçekleştirilmesi,

d) Görev değişikliği olan ya da işten ayrılan çalışanların bu alandaki yetkilerinin derhal kaldırılması. Bu kapsamda, veri sorumlusu tarafından kendisine tahsis edilen envanterin iade alınması,

3- Özel nitelikli kişisel verilerin işlendiği, muhafaza edildiği ve/veya erişildiği ortamlar, elektronik ortam ise

a) Verilerin kriptografik yöntemler kullanılarak muhafaza edilmesi,

b) Kriptografik anahtarların güvenli ve farklı ortamlarda tutulması,

c) Veriler üzerinde gerçekleştirilen tüm hareketlerin işlem kayıtlarının güvenli olarak loglanması,

[122] http://www.resmigazete.gov.tr/eskiler/2018/03/20180307-7.pdf, Erişim Tarihi: 12.02.2018.

ç) Verilerin bulunduğu ortamlara ait güvenlik güncellemelerinin sürekli takip edilmesi, gerekli güvenlik testlerinin düzenli olarak yapılması/yaptırılması, test sonuçlarının kayıt altına alınması,

d) Verilere bir yazılım aracılığı ile erişiliyorsa bu yazılıma ait kullanıcı yetkilendirmelerinin yapılması, bu yazılımların güvenlik testlerinin düzenli olarak yapılması/yaptırılması, test sonuçlarının kayıt altına alınması,

e) Verilere uzaktan erişim gerekiyorsa en az iki kademeli kimlik doğrulama sisteminin sağlanması,

4- Özel nitelikli kişisel verilerin işlendiği, muhafaza edildiği ve/veya erişildiği ortamlar, fiziksel ortam ise

a) Özel nitelikli kişisel verilerin bulunduğu ortamın niteliğine göre yeterli güvenlik önlemlerinin (elektrik kaçağı, yangın, su baskını, hırsızlık vb. durumlara karşı) alındığından emin olunması,

b) Bu ortamların fiziksel güvenliğinin sağlanarak yetkisiz giriş çıkışların engellenmesi,

5- Özel nitelikli kişisel veriler aktarılacaksa

a) Verilerin e-posta yoluyla aktarılması gerekiyorsa şifreli olarak kurumsal e-posta adresiyle veya Kayıtlı Elektronik Posta (KEP) hesabı kullanılarak aktarılması,

b) Taşınabilir Bellek, CD, DVD gibi ortamlar yoluyla aktarılması gerekiyorsa kriptografik yöntemlerle şifrelenmesi ve kriptografik anahtarın farklı ortamda tutulması,

c) Farklı fiziksel ortamlardaki sunucular arasında aktarma gerçekleştiriliyorsa, sunucular arasında VPN kurularak veya sFTP yöntemiyle veri aktarımının gerçekleştirilmesi,

ç) Verilerin kağıt ortamı yoluyla aktarımı gerekiyorsa evrakın çalınması, kaybolması ya da yetkisiz kişiler tarafından görülmesi gibi risklere karşı gerekli önlemlerin alınması ve evrakın "gizlilik dereceli belgeler" formatında gönderilmesi gerekir.

6- Yukarıda belirtilen önlemlerin yanı sıra Kişisel Verileri Koruma Kurumunun internet sitesinde yayımlanan Kişisel Veri Güvenliği Rehberinde

belirtilen uygun güvenlik düzeyini temin etmeye yönelik teknik ve idari tedbirler de dikkate alınmalıdır."

Amacın, temel hak ve özgürlüklerin korunması olduğu dikkate alındığında, bir başka kavram olan "ilgili kişi" de tanımlanabilir hale gelmektedir. Tüzel kişilerin, Kanun kapsamında hakkı korunan kişi olarak adlandırılabilmesi, Kanun'un amacıyla bağdaşmayacak, tüzel kişiler Kanun kapsamında hakkı korunan bir konuma geldiğinde, gerçek kişilerin Kanun kapsamında korunması etkinliği de azalacaktır. Tüzel kişilere ait verinin elde edilmesi birden çok gerçek kişiye ait kişisel verinin işlenmesi ile gündeme geliyorsa, bu takdirde tüzel kişinin Kanun'dan yararlanma durumu söz konusu olacaktır.

3.3.Kişisel Verileri Koruma Kurumu

Kanun'un 19. Maddesinde belirtildiği üzere; Kişisel Verileri Koruma Kurumu, Kanunla verilen görevlerin yerine getirilmesini sağlamak adına, idari ve mali özerkliğe sahip, kamu tüzel kişiliğine haiz bir kurumdur. Kurum, Türkiye'nin taraf olduğu uluslararası anlaşmalar, AB üyelik süreci gibi uluslararası sebeplerin yanı sıra, oluşturduğu ulusal yasal metinler, teknolojik gelişmeler idari uygulamalar sonucu ilgili kişilerin haklarına zarar gelmesini önlemek gibi amaçlarla oluşturulmuş bir kurum olarak karşımıza çıkmaktadır.

Anayasa'da belirtilen "insan haklarına saygılı" devlet prensibi gereği, idarenin, güvenlik soruşturması, sağlık verilerini toplaması gibi uygulamalar sonucu, kişisel verilerin işlenmesi ile ilgili süreçlerde kanuni dayanak oluşturulması ve ilgili kişilerin hukuki koruma altına alınabilmesi adına Kanun, Kanun'un uygulanmasının denetimi ve süreçlerin sorunsuz yürütülebilmesi için Kurum oluşturulması gerekliliği ortaya çıkmıştır[123].

[123] Mutlu KAĞITÇIOĞLU, Kişisel Verileri Koruma Kurumuna İdare Hukuku Çerçevesinden Bir Bakış, Aurum Sosyal Bilimler Dergisi 1 (2) 77-99, 2016, s. 80.

"Paris Prensipleri[124]" olarak bilinen ilkelerin yer almış olduğu BM Genel Kurul Kararı, Kurum'un sahip olması gereken özellikleri belirleyen uluslararası bir belge niteliğindedir. 2001 tarihli "Uluslararası Veri Koruma ve Mahremiyet Komiserleri Konferansı"'nda alınan "Veri Koruma Otoritelerinin Akreditasyon İlkelerine İlişkin Karar" da kişisel verilerin korunması adına oluşturulacak denetim kurumunu öngören bir başka uluslararası metin olarak karşımıza çıkmaktadır. İlgili karara göre; denetim kurumları özerk ve bağımsız, yasal bir çerçevede oluşturulmuş, yürütme organına doğrudan raporlama yapabilecek, veri korumasına ilişkin uluslararası düzenlemelere uygun kurumlar olmalıdır[125]. Belirtilen uluslararası düzenlemelerin yanı sıra, Türkiye'nin taraf olduğu 181 Sayılı Kişisel Verilerin Otomatik İşleme Tabi Tutulması Karşısında Bireylerin Korunması Sözleşmesine Ek Denetlyici Makamlar ve Sınırı Aşan Veri Akışına İlişkin Protokol, Direktif ve Regülasyon da belirlenen görevlerin yerine getirilmesini sağlamak adına bağımsız bir kurumun oluşturulması gerekliliğini ortaya koymuştur[126]. Görüleceği üzere bu kurumların yapılandırılmasına ilişkin tek bir ölçüt yoktur, veri koruma kurumlarına ihtiyaç duyulması ve bu kurumlarda bulunması gereken özellikle hukuki metinler ve farklı düzenlemelerle belirlenebilmekte ve gereken özelliklerin standart olarak sağlanmasının ardından, oluşturulan kurumların isimlendirme gibi hususları ülkelerin kendi takdirine bırakılmaktadır[127].

Kişisel Verileri Koruma Kurumu Teşkilat Yönetmeliği'nin 4. maddesi Kurum'un Kurul ve Başkanlık teşkilatından oluştuğunu belirtmiştir. Kişisel

[124] https://www.ohchr.org/EN/ProfessionalInterest/Pages/StatusOfNationalInstitutions.aspx, Erişim Tarihi: 16.02.2019.
[125] Esin GÜRSEL, Fatih DÜĞMECİ, Yapısal Anlamda Türkiye Kişisel Verileri Koruma Kurumu'na İlişkin Bir Değerlendirme, R&S- Research Studies Anatolia Journal 1(2), 318-329, 30.07.2018, s. 319.
[126] https://www2.tbmm.gov.tr/d26/1/1-0692.pdf, Erişim Tarihi: 16.02.2019.
[127] Dilek Yüksek CİVELEK, Kişisel Verilerin Korunması ve Bir Kurumsal Yapılanma Önerisi, Ankara, 2011, s. 94.

Verileri Koruma Kurumu Teşkilat Yönetmeliği madde 5 ve Kanun'un 20. maddesi ise Kurum'un görevlerini sıralamıştır. Buna göre Kurum;

"Görev alanı itibarıyla, uygulamaları ve mevzuattaki gelişmeleri takip etmek, değerlendirme ve önerilerde bulunmak, araştırma ve incelemeler yapmak veya yaptırmak,

İhtiyaç duyulması halinde, görev alanına giren konularda kamu kurum ve kuruluşları, sivil toplum kuruluşları, meslek örgütleri veya üniversitelerle işbirliği yapmak,

Kişisel verilerle ilgili uluslararası gelişmeleri izlemek ve değerlendirmek, görev alanına giren konularda uluslararası kuruluşlarla işbirliği yapmak, toplantılara katılmak,

Yıllık faaliyet raporunu Cumhurbaşkanlığına, TBMM İnsan Haklarını İnceleme Komisyonuna sunmak,

Kanunlarla verilen diğer görevleri yerine getirmek." İle görevlendirilmiştir.

Kurum, sektör içinde belirli konulara ilişkin düzenlemeler yapma, şikayet üzerine ya da resen denetim yapma, şikayet üzerine ya da resen yapılan denetimler sonucu ihlalin varlığına kanaat getirdiği takdirde bu hususlarla ilgili olarak hukuka aykırılıkların veri sorumlusu tarafından giderilmesine karar vererek uyuşmazlığı çözmeye çalışma, denetimler sonucu ihlallerin varlığı halinde yaptırım uygulama, veri koruma alanında yer alan özel hukuk ya da kamu hukuku tüzel kişilerine ve mevzuat taslakları hakkında görüş bildirme gibi görevlerle donatılmıştır[128].

3.3.1 Kişisel Verileri Koruma Kurulu

Kişisel Verileri Koruma Kurulu Çalışma Usul ve Esaslarına Dair Yönetmelik'in 4. maddesinde belirtildiği üzere; *"Kurul, Kurum'un karar*

[128] GÜRSEL/ DÜĞMECİ, s. 323, 324.

organıdır. Kurul; biri Başkan, biri İkinci Başkan olmak üzere dokuz üyeden oluşur."

Kanun'un 22. maddesi ve Kişisel Verileri Koruma Kurulu Çalışma Usul ve Esaslarına Dair Yönetmelik'in 7. maddesi Kurul'un görev ve yetkilerini belirlemiştir. Buna göre Kurul;

"Kişisel verilerin temel hak ve özgürlüklere uygun şekilde işlenmesini sağlamak,

Kişisel verilerle ilgili hakların ihlal edildiğini ileri sürenlerin şikayetlerini karar bağlamak,

Şikâyet üzerine veya ihlal iddiasını öğrenmesi durumunda resen görev alanına giren konularda kişisel verilerin kanunlara uygun olarak işlenip işlenmediğini incelemek ve gerektiğinde bu konuda geçici önlemler almak,

Veri güvenliğine ilişkin yükümlülükleri belirlemek amacıyla düzenleyici işlem yapmak,

Özel nitelikli kişisel verilerin işlenmesini için alınması gereken yeterli önlemleri belirlemek,

Veri sorumluları sicilinin tutulmasını sağlamak,

Kişisel verilerin silinmesine, yok edilmesine veya anonimleştirilmesine ilişkin usul ve esasları belirlemek,

Kurul'un görev alanı ile Kurum'un işleyişine ilişkin konularda gerekli düzenleyici işlemleri yapmak,

Veri sorumlusunun ve temsilcisinin görev, yetki ve sorumluluklarına ilişkin düzenleyici işlem yapmak,

Yurtdışına veri aktarılabilmesi için yeterli korumaya sahip olan ve olmayan ülkeleri belirleyip ilan etmek,

Kişisel verilerin korunması, işlenmesi ve güvenliği ile ilgili sektörel uygulama esaslarını belirlemek ve akreditasyon, sertifikasyon, eğitim ile rehberlik konularında usul ve esasları belirlemek,

Kişisel verilerin korunması ile ilgili yurt içi ve yurt dışı projeler yapmak ve yaptırmak,

Kişisel verilerin korunması konusunda kurum ve kuruluşları bilgilendirmek, kamuoyuna yönelik farkındalık faaliyetleri gerçekleştirmek,

Ücret tarifeleri ile ilgili çalışmalar yapmak,

Üniversiteler ve ilgili diğer yurt içi ve yurt dışı kurum ve kuruluşlarla işbirliği ve koordinasyon çalışmaları yürütmek,

Kanun'da öngörülen idari yaptırımlara karar vermek,

Diğer kurum ve kuruluşlarca hazırlanan ve kişisel verilere ilişkin hüküm içeren mevzuat taslakları hakkında görüş bildirmek,

Kurum'un; stratejik planını karara bağlamak, amaç ve hedeflerini, hizmet kalite standartlarını ve performans kriterlerini belirlemek,

Kurum'un stratejik planı ile amaç ve hedeflerine uygun olarak hazırlanan bütçe teklifini görüşmek ve karara bağlamak,

Kurum'un performansı, mali durumu, yıllık faaliyetleri ve ihtiyaç duyulan konular hakkında hazırlanan rapor taslaklarını onaylamak ve yayımlamak,

Taşınmaz alımı, satımı ve kiralanması konularındaki önerileri görüşüp karara bağlamak " ile görevlendirilmiştir.

3.3.2 Başkanlık Teşkilatı

Kanun'un 25. maddesi Başkanlığın oluşum ve görevlerini düzenlemiştir. Buna göre; "Başkanlık; Başkan Yardımcısı ve hizmet birimlerinden oluşur. Başkanlık, belirlenen görevleri daire başkanlıkları şeklinde teşkilatlanan hizmet birimleri aracılığıyla yerine getirir."

Başkanlığın görevleri 25. maddenin 4. fıkrasında sayılmıştır. Buna göre Başkanlık;

- *"Veri Sorumluları Sicilini tutmak,*
- *Kurum'un ve Kurul'un büro ve sekreterya işlemlerini yürütmek,*
- *Kurum'un taraf olduğu davalar ile icra takiplerinde avukatlar vasıtasıyla Kurum'u temsil etmek, davaları takip etmek veya ettirmek, hukuk hizmetlerini yürütmek,*

- *Kurul üyeleri ile Kurum'da görev yapanların özlük işlemlerini yürütmek,*
- *Kanunlarda mali hizmet ve strateji geliştirme birimlerine verilen görevleri yapmak,*
- *Kurum'un iş ve işlemlerinin yürütülmesi amacıyla bilişim sistemlerinin kurulmasını ve kullanılmasını sağlamak,*
- *Kurul'un yıllık faaliyetleri hakkında veya ihtiyaç duyulan konularda rapor taslaklarını hazırlamak ve Kurul'a sunmak,*
- *Kurum'un stratejik plan taslağını hazırlamak,*
- *Kurum'un personel politikasını belirlemek, personelin karişyer ve eğitim planlarını hazırlamak ve Kurul'a sunmak,*
- *Kurum'un stratejik plan taslağını hazırlamak,*
- *Kurum'un personel politikasını belirlemek, personelin kariyer ve eğitim planlarını hazırlamak ve uygulamak,*
- *Personelin atama, nakil, disiplin, performans, terfi, emeklilik ve benzeri işlemlerini yürütmek,*
- *Personelin uyacağı etik kuralları belirlemek ve gerekli eğitimi vermek*
- *Kurum'un ihtiyacı olan her türlü satın alma, kiralama, bakım, onarım, yapım, arşiv, sağlık, sosyal ve benzeri hizmetleri yürütmek,*
- *Kurum'a ait taşınır ve taşınmazların kaydını tutmak,*
- *Kurul veya Başkan tarafından verilen diğer görevleri yapmak."* İle görevlendirilmiştir.

Kurumun'un hizmet birimleri Kişisel Verileri Koruma Kurumu Teşkilat Yönetmeliği 13. maddesinde sayılmıştır.

Veri Yönetimi Dairesi Başkanlığı: Kişisel verilerin işlenmesine ilişkin usul ve esasların belirlenmesi, veri sorumlusu, temsilcisi ve irtibat kişisinin görev, yetki ve sorumluluklarına ilişkin iş ve işlemleri yürütme, Sicil ile ilgili iş ve işlemleri yürütme, aydınlatma yükümlülüğünü yerine getirmeyenler hakkındaki iş ve işlemleri yürütme, veri silme, yok etme ve anonimleştirme usulleri ile ilgili çalışmaları yürütme gibi görevleri yerine getirir.

İnceleme Dairesi Başkanlığı: Veri sorumlusuna başvuru ve Kurul'a yapılan şikâyete ilişkin iş ve işlemler, Kurul'a yapılan şikayetlerle ilgili ön inceleme ve esas incelemeleri, şikayet üzerine veya resen incelemeyle ilgili işlemler, Kurul tarafından verilen kararları yerine getirmeyenler hakkındaki iş ve işlemler, Kurul'a ait yazışmaları yapmak, karar ve yazışmalara ilişkin arşiv oluşturmak ve bunları muhafaza etmek gibi görevleri yerine getirir.

Hukuk İşleri Dairesi Başkanlığı: Kurum'un taraf olduğu dava ve icra takiplerinde Kurum'u temsil etme, Başkan ve Kurul tarafından intikal ettirilen konularda hukuki görüş bildirme, Kişisel verilerin yurtdışına aktarılmasında yeterli korumanın bulunduğu ülkelerin belirlenmesinde ilişkin işlemleri yürütme gibi görevleri yerine getirir.

Veri Güvenliği ve Bilgi Sistemleri Dairesi Başkanlığı: Veri güvenliği ile ilgili iş ve işlemleri yürütme, veri koruması amacıyla uygun güvenlik düzeyini temin etmeye yönelik gerekli her türlü tedbirin alınması hususundaki işlemleri yürütme, özel nitelikli kişisel verilerin işlenmesi için alınması gereken önlemleri belirlemekle ilgili çalışmaları yürütme, veri aktarımına ilişkin alınması gereken güvenlik önlemlerini belirleme gibi görevleri yerine getirir.

Rehberlik, Araştırma ve Kurumsal İletişim Dairesi Başkanlığı: Kişisel verilerin korunması ile ilgili standartların belirlenmesi, yetkilendirme ve sertifika işlemleri, kamu kurum ve kuruluşları, gerçek ve tüzel kişiler ile gönüllü kuruluşlara faaliyetlerinde yol gösterecek plan ve programlar oluşturma ve rehberlik etme, Kurujm'un yurtiçi ve yurtdışı faaliyetlerini raporlama ve arşivleme gibi görevleri yerine getirir.

İnsan Kaynakları ve Destek Hizmetleri Dairesi Başkanlığı: Kurum'un insan kaynakları politikasını belirleme, personelin kariyer ve eğitim planlarını hazırlama

ve uygulama, Kurum'un hizmet içi eğitim planını hazırlama ve eğitim programları düzenleme gibi görevleri yerine getirir.

Strateji Geliştirme Dairesi Başkanlığı: Kurum'un stratejik planını hazırlama, amaç ve hedeflerini, hizmet kalite standartlarını ve performans kriterlerini belirleme, Kurum'un hesap planları ve muhasebe kayıtlarıyla ilgili işlemleri yürütme gibi görevleri yerine getirir.

3.4.Veri Sorumlusu

Veri sorumlusu Kanunun 3. maddesinin 1. fıkrasının (ı) bendinde de tanımlandığı üzere; kişisel verilerin işleme amaçlarını ve vasıtalarını belirleyen, veri kayıt sisteminin kurulmasından ve yönetilmesinden sorumlu olan gerçek veya tüzel kişiyi ifade eder. Bu kişiler gerçek kişiler olabileceği gibi, kamu kurumları, şirketler, dernekler veya vakıflar gibi tüzel kişiler de olabilir[129]. Kişisel Verileri Koruma Kurumu'na göre (Çalışmanın bundan sonraki bölümlerinde "Kurum" olarak anılacaktır.), tüzel kişiler, veri işleme konusunda direkt olarak veri sorumlusu olduklarından, hukuki sorumluluk da tüzel kişinin şahsında doğacaktır[130]. Bu tanımlamadan yola çıkarak, özel bir şirketin, faaliyetleri kapsamında işlemiş olduğu kişisel veriler dolayısıyla şirket içerisinde herhangi bir çalışanı sorumlu olarak göstermesi halinde, söz konusu şirketin hukuka aykırı şekilde kişisel veri işlemesi sonucu, sorumlu olarak belirlenen çalışan sorumlu kabul edilmeyecek, aksine sorumluluğunun doğmasını engellemeye çalışmasına karşın şirketin tüzel kişiliği üzerinde sorumluluk gündeme gelecektir.

Veri sorumlusunun Kanun'da önemli bir konumu vardır. Kanun'da belirtilmiş sorumluluklar veri sorumlusunun üzerinde doğmaktadır. Bu sorumluluklara aykırı davranılması halinde de yaptırımlarla karşı karşıya kalacak olan kişi veri

[129] https://www.tbmm.gov.tr/sirasayi/donem26/yil01/ss117.pdf , s.7, Erişim Tarihi: 18.12.2018.
[130]Kişisel Verileri Koruma Kurumu, https://www.kvkk.gov.tr/Icerik/2032/Veri-Sorumlusu-Kimdir, Erişim Tarihi: 18.2.2018.

sorumlusudur. Bu nedenle veri sorumlusunun belirlenmesi, tüm sorumluluk ve yaptırımların belirlenmesi ve uygulanması açısından önem arz etmektedir. Yukarıda verilen Kanun tanımından da görüleceği üzere, veri sorumlusu, kişisel verilerin işleme amaçlarını ve vasıtalarını belirleyen konumunda da olabilir. Kanunun 3. maddesinin 1. fıkrasının (ğ) bendinde belirtilen ve daha sonra detaylı olarak anlatılacak olan "veri işleyen"[131], veri sorumlusunun verdiği yetkiye dayanarak onun adına kişisel verileri işleyen gerçek veya tüzel kişidir. Bu tanımdan da anlaşılacağı üzere, Kanun veri sorumlusuna, kişisel verileri bizzat işlemese dahi üçüncü kişiler aracılığıyla işleme imkânı vermiş, buna dayanarak da 12. maddenin 2. fıkrasında; veri sorumlusunu, kişisel verilerin kendi adına başka bir gerçek veya tüzel kişi tarafından işlenmesi halinde, birinci fıkrada belirtilen tedbirlerin alınması hususunda, bu kişilerle birlikte müştereken sorumlu tutmuştur.

Uygulamada, belirli bir veri işleme sürecinde, kimin ya da neyin veri sorumlusu olduğunu belirlemekte çeşitli sıkıntılar ile karşılaşılabilir. Bu sıkıntı kendini özellikle geniş ve karmaşık yapılanmalarda ve elektronik iletişim ağlarında gösterir[132]. Veri sorumlusu ve veri işleyen rolleri dikkatli bir biçimde belirlenmelidir, veri sorumluları veri işleyenlerle çalışabileceği gibi, alt veri işleyenlerle de çalışma durumu gündeme gelebilecektir, bu ihtimal dahilinde rollerin çatışmaması adına veri sorumlusu tarafından roller ve sorumluluk haritası çıkartılması bu konuda sorumlulukların belirlenmesinde taraflara yardımcı olabilecektir[133].

3.4.1. Veri Sorumlusu'nun Yükümlülükleri

Kanun'un "Genel İlkeler" başlıklı 4. maddesi, kişisel verilerin, Kanun'da ve diğer kanunlarda öngörülen usul ve esaslara uygun olarak işlenmesi gerektiğini

[131] Bkz: s. 107.
[132] KÜZECİ, s. 17.
[133] KESER/ KAYA/ KINIKOĞLU, s. 64.

belirtir ve 2. fıkrasında da veri işlemede uyulması gereken ilkeleri belirler. Belirtilen bu ilkelere uyulmaması halinde veri sorumlusunun sorumluluğunun doğacağı, her ne kadar hüküm altına alınmasa da Kanunun 4. maddesinde belirtilen ilkelere aykırı olarak yapılan işlemeler kanuna aykırı şekilde yapılmış sayılacağından, Kanun'un 11. maddesinin (ğ) bendinde belirtildiği üzere; herkes, kişisel verilerin kanuna aykırı olarak işlenmesi sebebiyle zarara uğraması halinde, zararın giderilmesini talep etme hakkına sahip olacaktır. Bu nedenle veri sorumlusunun bu madde kapsamında sorumluluğu doğacağı söylenebilir.

3.4.1.1.Hukuka ve Dürüstlük Kuralına Uygunluk

Bu yükümlülük belirtilen diğer yükümlülükler ve ilkeleri de kapsayan genel bir yükümlülük olarak düşünülebilir. Veri işleme gerçekleştirilecek ise, bu işleme sürecinin öncesinden başlayan ve devam eden süreçte, hukuka ve dürüstlük kuralına uyulması gerekliliği tek başına önemli bir yükümlülük olmasının yanı sıra, diğer yükümlülük ve ilkelerin de uygulanması açısından onlara kaynaklık edecektir.

Hukuka uygunluk, yalnızca Kanun'a uyularak işleme sürecinin devam etmesi gerekliliğinden çok, belirlenen tüm yasal düzenlemelere uygunluğun sağlanması olarak değerlendirilmelidir.

TMK'nın "Dürüst davranma" başlıklı 2. maddesi: "Herkes, haklarını kullanırken ve borçlarını yerine getirirken dürüstlük kurallarına uymak zorundadır." şeklinde ifade edilmiştir. Kanun'da bahsedilen dürüstlük kurallarına uygun olma, her ne kadar Türk Medeni Kanunu'nda belirtilen dürüstlük kuralını kapsasa da dar anlamda düşünüldüğünde; ilgili kişilerin, ilgili kişinin veri

işlenmesine ilişkin, belirli bir amaç için verdiği rızanın, amacın değişmesi halinde geçerli olup olmayacağıyla da ilgilidir[134].

TBK 25. maddesine göre, genel işlem şartlarına, dürüstlük kurallarına aykırı olarak karşı tarafın aleyhine veya onun durumunu ağırlaştırıcı nitelikte hükümler konulamaz. TBK kapsamında düzenlenen genel işlem şartları, sosyal adaleti sağlamaya yönelik olarak oluşturulmuş emredici hükümlerdir ve zayıf durumda olan karşı tarafın korunması amacını gütmektedir[135]. Yapılacak içerik denetimi ile sözleşmenin diğer tarafının menfaatlerini dürüstlük kuralı ile korunur ancak aleyhe olan tüm hükümler değil, dürüstlük kuralına aykırılık teşkil eden hükümler geçersiz hale gelir. Bu denetim kuralı kişisel verilerin işlenmesine ilişkin hükümler açısından da geçerlidir. Dolayısıyla dürüstlük kuralı ve hakkın kötüye kullanılması hükümlerine aykırı şekilde kişisel verilerin işlenmesi mümkün değildir. Genel işlem şartları, diğer denetim aşamalarını geçmiş olsa dahi, dürüstlük kuralına aykırı hükümler içeriyorsa içerik denetimine takılır ve kesin hükümsüzlük yaptırımına tabi olur[136]. Açıklanan nedenler de göz önüne alındığında, açık rızanın genel işlem şartı şeklinde alınması söz konusu olduğunda, Kanun ve TBK hükümleri de göz önüne alınarak, kişinin yeterince bilgilendirildiği, yeterli seviyede açık ve anlaşılır olan bir dille hazırlanmış bir metin açık rıza olarak kabul edilebilir. Bu aşamada karşı tarafın uyarılması yeterli sayılmayacak, metni hazırlayan taraf tarafından, sözleşme kurulmadan önce açıkça bilgi verilmesi gerekmektedir[137].

Bu yükümlülükle birlikte "adil kullanım" kavramı da gündeme gelmektedir. Adil kullanım kavramı, tarafların çatışan menfaatlerini dengelemeyi amaçlayan hükümler çerçevesinde önem kazanacak, ayrıca rızanın özgür iradeye ile alınıp

[134] Furkan Güven TAŞTAN, Türk Sözleşme Hukukunda Kişisel Verilerin Korunması 2. Baskı, On İki Levha Yayınları, İstanbul, 2017, s. 49.
[135] Gökhan ANTALYA, 6098 Sayılı Türk Borçlar Kanunu'na Göre Borçlar Hukuku Genel Hükümler, Cilt 1, 1. Baskı, Beta Yayınları, İstanbul, İstanbul, Ocak 2012, s. 288.
[136] TAŞTAN s. 99-100.
[137] ANTALYA, s. 304.

alınmadığı, gerekli tedbirlerin uygulanıp uygulanmadığı dikkate alınacaktır[138]. Veri işleme sürecine dahil olan kişiler, özellikle veri sorumluları, Kanun'dan doğan haklarını kullanırken ilgili kişilere karşı adil davranmakla yükümlü olacaklardır.

Yukarıdaki açıklamalar ışığında dürüstlük kuralı, Regülasyon'da yer verilmiş olan "şeffaflık" ilkesinin bir yansıması olarak kabul edilebilir. Dürüstlük kuralı ile elde edilen verilerin şeffaf kurallar ile işlenmesi gerektiği anlaşılabilir[139]. Çalışmanın ilk bölümünde daha detaylı şekilde anlatıldığı üzere; şeffaflık ilkesi[140], ilgili kişinin, veri işleme süreci boyunca alınacak aksiyonlara dair bilgi sahibi olması, verdiği rızanın kapsamı ve veri sorumlusunun amacına ilişkin bilgi sahibi olması ve bu sürece müdahil olarak kontrol mekanizmalarını etkin bir şekilde kullanmasını sağlayacaktır. İlgili kişinin verdiği açık rızanın, kabul edilebilir olması için açık olarak belirlenmiş bir amaç doğrultusunda, bilgilendirmeye dayalı ve özgür irade ile alınmış olması gerekmektedir. Rıza kavramı, kullanıcılara fayda sağlama amacıyla, ilgili kişinin yalnızca olumlu ya da olumsuz beyanıyla pasif bir süje olarak kalması yerine, verilerinin işlenmesi ile ilgili olarak şeffaf süreçlere aktif katılımının sağlanabileceği uygulamalar ile hayata geçirilmelidir[141]. Bu kapsamda rızanın tereddüte yer vermeyecek şekilde açık olması ve sadece o işlemle alakalı olarak verilmiş olması gerekecektir. Rızanın kişinin özgür iradesiyle ortaya çıkması gerekliliği de yine rızanın geçerliliğini etkileyecek bir başka konudur. İlgili kişinin, verilerinin işlenmesi konusunda rıza verirken tercih hakkının bulunması ve bu hakkı kullanarak verilerinin işlenmesine onay vermesi gerekecektir. Örneğin iş sözleşmelerinin feshedileceği ve işini kaybedeceği korkusuyla kişisel verilerinin işlenmesi için açık rıza beyanında bulunan bir işçinin beyanının geçerliliği tartışmalıdır[142].

[138] ÇEKİN, s. 45.
[139] Erbil BEYTAR, İşçinin Kişiliğinin ve Kişisel Verilerinin Korunması, 2. Baskı, On İki Levha Yayınevi, İstanbul, Ekim 2018, s. 150.
[140] Bkz: s. 19.
[141] KESER, KAYA, KINIKOĞLU, s. 61.
[142] BEYTAR, s. 156-157.

3.4.1.2.Belirli ve Meşru Amaçlarla Toplama, Amaçla Bağlantılı, Sınırlı ve Ölçülü İşleme

Verilerin belirli ve meşru amaçlar doğrultusunda işlenmesi, ilgili kişilerin korunması adına önemli yükümlülüklerden biridir. Kanun, amacın belirli olması gerekliliği ile ilgili kişiyi koruyucu bir politika benimsemiştir. Buna göre veri sorumlusunun, veri işlemenin gerekliliği olan amaç dışında, ileride de lazım olabilir düşüncesi ile veri depolamasının önüne geçilmektedir. Amaca bağlılık ilkesine uyumluluk inle, verinin işleme amaçlarını baştan belirlenmesi, ilgili kişinin neye rıza gösterdiğini bilmesi ve veri sorumlusunun da belirttiği amaç doğrultusunda gerekli ve ölçülü miktarda veri işlemesi sağlanır[143].

Kanun'un gerekçesinde de belirtildiği üzere; Veri sorumluları, başta belirlediğinden farklı amaçlarla veri işlemeleri halinde, bu fiillerinden sorumlu tutulacaklardır. Amacın meşruluğundan bahsedilebilmesi için, veri sorumlusunun yaptığı iş için işlemesi gereken verilerin işlenmesi gerekir. Örneğin, bir hazır giyim mağazasının, müşterilerinin kimlik ve iletişim bilgilerini işlemesi meşru amaç, kapsamındayken, kan gruplarını işlemesi meşru amaç, kapsamında değerlendirilemeyecektir.

Verilerin işlenmesinde amacın belirli olmasının yanı sıra meşru, hukuka uygun amaçlar doğrultusunda işlenmesi gerekliliği de yine hukuki sorumluluklar çerçevesinde değerlendirilebilecek yükümlülüklerdendir. İlgili kişinden alınmış olan rızanın, amacın hukuka uygun, meşru ve belirli olduğu varsayımını destekleyecektir. Rızanın, amaç belirlendikten sonra alınması gerekmektedir ki ilgili kişi rıza verdiği ve işlemenin gerçekleşmesini gerektirecek amaç hakkında bilgi sahibi ve sonradan ortaya çıkarılabilecek yeni amaçlar karşısında da söz sahibi olabilecek durumda olsun. Veri sorumlusunun daha sonradan amacının değişmesi, makul beklenti kapsamında değerlendirilebilecek seviyede ise yeniden ilgili kişiden rıza alınmasına gerek kalmayacak, ancak makul beklentiyi aşıyor ise

[143] ÇEKİN, s. 46.

değişen amaca uygun olarak yeni bir rıza beyanı alınması gerekliliği doğacaktır. Makul beklenti; önceden alınmış olan amaca uygun rızanın kapsamı dışında kalan amaçlar ortaya çıkması ile veri işleme amacının önceki amacın devamı niteliğinde sayılıp sayılamayacağı hususunda ortaya çıkan bir kavramdır.

Kişisel verilerin, işlendikleri amaçla bağlantılı, sınırlı ve ölçülü olması ilkesi ile, işlenen verilerin, belirlenen amaçların gerçekleşmesine elverişli olması, amaçla ilgili olmayan veya ihtiyaç duyulmayan verilerin işlenmesinden kaçınılması amaçlanır. Sonradan ortaya çıkması muhtemel ihtiyaç ve amaçlar doğrultusunda veri işlenebilmesi için, işlemeye ilk kez başlıyor gibi, kişisel verilerin işlenme şartlarından birinin gerçekleşmesi ve yalnızca amacın gerçekleşmesi için gerekli şekilde veri işlenmesi gerekecektir.

Amaçla bağlantılı, sınırlı ve ölçülü işleme yükümlülüğü yukarıda anlatılmış olan "Kişisel Verileri Belirli ve Meşru Amaçlarla Toplamak"[144] yükümlülüğü ile oldukça yakından bağlantısı bulunan bir yükümlülük olarak değerlendirilebilir. İşlenen veriler başta belirtilen meşru ve belirli amaçlar adına toplanmalı, bu amaçlar dışına çıkılması halinde, işleme kanuna aykırılık teşkil edecektir. Veri sorumluları belirlenen amacın gerçekleşmesine hizmet etmeyen kişisel verilerin işlenmesinden kaçınmalıdırlar.

3.4.1.3.Veri Sorumluları Siciline Kaydolma

Kanunun "Veri Sorumluları Sicili" başlıklı 16. maddesinin 1. fıkrası, Kişisel Verileri Koruma Kurulu'nun (Çalışmanın bundan sonraki bölümlerinde "Kurul" olarak anılacaktır.) gözetiminde, Başkanlık tarafından kamuya açık olarak Veri Sorumluları Sicili[145] (Çalışmanın bundan sonraki bölümlerinde "Sicil" olarak anılacaktır.) tutulacağını hükmetmiştir. Aynı maddenin 2. fıkrası da: Kişisel

[144] Bkz: s. 76.
[145] Kişisel Verileri Koruma Kurumu, https://verbis.kvkk.gov.tr, Erişim Tarihi: 18.12.2018.

verileri işleyen gerçek ve tüzel kişiler, veri işlemeye başlamadan önce Veri Sorumluları Siciline kaydolmak zorundadır. Sicil, şeffaflık ilkesinin en önemli sonuçlarından biridir. Sicil ile amaçlanan, veri işleme süreçleri hakkında ilgili kişilerin bilgi sahibi olabilmeleridir, ki 16. maddenin 1. fıkrasında belirtilen "kamuya açıklık" da bu amacın en önemli göstergelerinden biridir.

16. maddenin 3. fıkrası, veri sorumluları siciline başvuruda bulunması gereken hususları saymıştır. Buna göre;

- Veri sorumlusu ve varsa temsilcisinin kimlik ve adres bilgileri
- Kişisel verilerin hangi amaçla işleneceği
- Veri konusu kişi grubu ve grupları ile bu kişilere ait veri kategorileri hakkındaki açıklamalar
- Kişisel verilerin aktarılabileceği alıcı veya alıcı grupları
- Yabancı ülkelere aktarımı öngörülen kişisel veriler
- Kişisel verilerin güvenliğine ilişkin alınan tedbirler
- Kişisel verilerin işlendikleri amaç için gerekli olan azami süre
- Üçüncü fıkra uyarınca verilen bilgilerde meydana gelen değişiklikler derhal Başkanlığa bildirilir.

Yönetmelik 5. maddesinin 1. fıkrasının (a) bendine göre, veri sorumluları, kişisel veri işlemeye başlamadan önce Sicil'e kaydolmak zorundadırlar. Aynı Yönetmeliğin "Kayıt yükümlülüğünün başlangıcı" başlıklı 8. maddesinin 2. fıkrasına göre, kayıt yükümlülüğü altında bulunmayan, sonradan kayıt yükümlüsü haline gelen veri sorumluları, yükümlülük altına girmelerini müteakip otuz gün içerisinde Sicile kaydolurlar.

Kurul, 19.07.2018 Tarih 2018/88 Sayılı Kararı ile;

"Yıllık çalışan sayısı 50'den çok veya yıllık mali bilanço toplamı 25 milyon TL'den çok olan gerçek ve tüzel kişi veri sorumluları için Sicil'e kayıt

yükümlülüğü başlangıç tarihinin 01.10.2018 olması ve Sicil'e kayıt yaptırmaları için bu veri sorumlularına 30.09.2019 tarihine kadar,

Yurtdışında yerleşik gerçek ve tüzel kişi veri sorumluları için Sicil'e kayıt yükümlülüğü başlangıç tarihinin 01.10.2018 olması ve Sicil'e kayıt yaptırmaları için bu veri sorumlularına 30.09.2019 tarihine kadar,

Yıllık çalışan sayısı 50'den az ve yıllık mali bilanço toplamı 25 milyon TL'den az olmakla birlikte ana faaliyet konusu özel nitelikli kişisel veri işleme olan gerçek ve tüzel kişi veri sorumluları içi Sicil'e kayıt yükümlülüğü başlangıç tarihinin 01.01.2019 olması ve Sicil'e kayıt yaptırmaları için bu veri sorumlularına 31.03.2020 tarihine kadar,

Kamu kurum ve kuruluşu veri sorumluları için Sicil'e kayıt yükümlülüğü başlangıç tarihinin 01.04.2019 olması ve Sicil'e kayıt yaptırmaları için bu veri sorumlularına 30.06.2020 tarihine kadar süre verilmesinin kabulüne karar vermiştir[146]*."*

İşlenen kişisel verinin niteliği, sayısı, veri işlemenin kanundan kaynaklanması veya üçüncü kişilere aktarılma durumu gibi Kurulca belirlenecek objektif kriterler göz önüne alınmak suretiyle, Kurul tarafından, Veri Sorumluları Siciline kayıt zorunluluğuna istisna getirilebilir, demiştir. Veri Sorumluları Sicili Hakkında Yönetmelik (Çalışmanın bundan sonraki bölümlerinde "Yönetmelik" olarak anılacaktır.) 5. maddesinin 1. fıkrasının (c) bendine göre; Kurul, kamuya açıklık ilkesinin sağlanması şartıyla, bu ilkenin kapsamı ve istisnalarını belirleme yetkisini haizdir.

Kanunun 16. maddesinde ve Veri Sorumluları Sicili Hakkında Yönetmeliğin 5. maddesinin 1. fıkrasının (c) bendinde belirtilen istisnalar, yalnızca Sicile kayıt zorunluluğunun istisnalarına ilişkindir. İstisna kapsamında olan kişilerin maddi

[146] Kişisel Verileri Koruma Kurulu, https://kvkk.gov.tr/Icerik/5272/2018-88, Erişim Tarihi: 22.02.2019.

hukuka uygunluk sebeplerinden de muaf tutulacağını söylemek imkansızdır. Bu sebeple Sicile kayıt zorunluluğunun, maddi hukuka uygunluk sebeplerine ek olarak getirilen şekli bir hukuka uygunluk sebebi olarak görülebilir[147].

Yönetmelik'in Dördüncü Bölüm'ünde istisna uygulanacak haller ve istisna kriterleri belirtilmiştir. Buna göre;

- Kişisel veri işlemenin suç işlenmesinin önlenmesi veya suç soruşturması için gerekli olması
- İlgili kişinin kendisi tarafından alenileştirilmiş kişisel verilerin işlenmesi
- Kişisel veri işlemenin Kanunun verdiği yetkiye dayanılarak görevli ve yetkili kamu kurum ve kuruluşları ile kamu kurumu niteliğindeki meslek kuruluşlarınca, denetleme veya düzenleme görevlerinin yürütülmesi ile disiplin soruşturma veya kovuşturması için gerekli olması
- Kişisel veri işlemenin bütçe, vergi ve mali konulara ilişkin olarak Devletin ekonomik ve mali çıkarlarının korunması için gerekli olması, faaliyetlerini işleyen veri sorumlularının Sicile kayıt olma yükümlülükleri yoktur.

Kurul, aynı zamanda, kişisel verinin niteliği, sayısı, işlenme amacı, işlendiği faaliyet alanı, üçüncü kişilere aktarılma durumu, işleme faaliyetinin kanunlardan kaynaklanması, muhafaza edilme süresi, veri konusu kişi grubu veya veri kategorilerini göz önüne alarak da kayıt yükümlülüğüne istisnalar getirme yetkisine sahiptir.

Kurul, "Veri Sorumluları Sicil'ine Kayıt Yükümlülüğünden İstisna Tutulacak Veri Sorumluları" ile ilgili, 02.04.2018 Tarih 2018/32 Sayılı Kararı ile;

- *"Herhangi bir veri kayıt sisteminin parçası olmak kaydıyla yalnızca otomatik olmayan yollarla kişisel veri işleyenler,*

[147] ÇEKİN, s. 121.

- *18.01.1972 tarihli ve 1512 sayılı Noterlik Kanunu uyarınca faaliyet gösteren noterler,*
- *04.11.2004 tarihli ve 5253 sayılı Dernekler Kanunu'na göre kurulmuş derneklerden, 20.02.2008 tarihli ve 5737 sayılı Vakıflar Kanununa göre kurulmuş vakıflardan ve 18.10.2012 tarihli 6356 sayılı Sendikalar ve Toplu İş Sözleşmesi Kanununa göre kurulmuş sendikalardan yalnızca ilgili mevzuat ve amaçlarına uygun, faaliyet alanlarıyla sınırlı ve sadece kendi çalışanlarına, üyelerine, mensuplarına ve bağışçılarına yönelik kişisel veri işleyenler,*
- *22.04.1983 tarihli ve 2820 sayılı Siyasi Partiler Kanununa göre kurulmuş siyasi partiler,*
- *19.03.1969 tarihli ve 1136 sayılı Avukatlık Kanunu uyarınca faaliyet gösteren avukatlar,*
- *01.06.1989 tarihli ve 3569 sayılı Serbest Muhasebeci Mali Müşavirlik ve Yeminli Mali Müşavirlik Kanunu uyarınca faaliyet gösteren serbest muhasebeci mali müşavirlik ve yeminli mali müşavirler, Sicil'e kayıt yükümlülüğünden istisna tutulmuştur*[148]*."*

Kurul, daha sonrasında 28.06.2018 Tarih ve 2018/68 Sayılı Kararı[149] ile, 4458 sayılı Gümrük Kanunu uyarınca faaliyet gösteren gümrük müşavirleri ve yetkilendirilmiş gümrük müşavirleri bakımından, 05.07.2018 Tarih 2018/75 Sayılı Kararı[150] ile, Arabulucular bakımından, 19.07.2018 Tarih 2018/87 Sayılı Kararı[151] ile, yıllık çalışan sayısı 50'den az ve yıllık mali bilanço toplamı 25 milyon TL'den az olan gerçek ve tüzel kişi veri sorumlularından ana faaliyet konusu özel nitelikli kişisel veri işleme olmayanların Sicil'e kayıt yükümlülüğüne istisna getirilmesine karar vermiştir.

[148] Kişisel Verileri Koruma Kurulu, https://kvkk.gov.tr/Icerik/4233/2018-32, Erişim Tarihi: 22.02.2019.
[149] Kişisel Verileri Koruma Kurulu, https://kvkk.gov.tr/Icerik/5269/2018-68, Erişim Tarihi: 22.09.2019.
[150] Kişisel Verileri Koruma Kurulu, https://kvkk.gov.tr/Icerik/5270/2018-75, Erişim Tarihi: 22.02.2019.
[151] Kişisel Verileri Koruma Kurulu, https://kvkk.gov.tr/Icerik/5271/2018-87, Erişim Tarihi: 22.02.2019.

Kurul tarafından, Kanun'un 16. maddesine göre Sicil'e kayıt yükümlülüğüne getirilen tüm veri sorumlularının listesi ise şu şekildedir:

Şekil 2: Kişisel Verileri Koruma Kurulunca 6698 Sayılı Kanun'un 16. Maddesine Göre Veri Sorumluları Siciline Kayıt Yükümlülüğüne İstisna Getirilen Veri Sorumluları.

KİŞİSEL VERİLERİ KORUMA KURULUNCA 6698 SAYILI KANUNUN 16 NCI MADDESİNE GÖRE VERİ SORUMLULARI SİCİLİNE KAYIT YÜKÜMLÜLÜĞÜNE İSTİSNA GETİRİLEN VERİ SORUMLULARI

	Veri Sorumluları	Kurul Kararı		Resmi Gazetede Yayım Tarihi
		Tarihi	Sayısı	
1	Herhangi bir veri kayıt sisteminin parçası olmak kaydıyla yalnızca otomatik olmayan yollarla kişisel veri işleyenler	02.04.2018	2018/32	15.05.2018
2	1512 sayılı Noterlik Kanunu uyarınca faaliyet gösteren noterler	02.04.2018	2018/32	15.05.2018
3	5253 sayılı Dernekler Kanununa göre kurulmuş derneklerden, 5737 sayılı Vakıflar Kanununa göre kurulmuş vakıflardan ve 6356 sayılı Sendikalar ve Toplu İş Sözleşmesi Kanununa göre kurulmuş sendikalardan yalnızca ilgili mevzuat ve amaçlarına uygun, faaliyet alanlarıyla sınırlı ve sadece kendi çalışanlarına, üyelerine, mensuplarına ve bağışçılarına yönelik kişisel veri işleyenler	02.04.2018	2018/32	15.05.2018
4	2820 sayılı Siyasi Partiler Kanununa göre kurulmuş siyasi partiler	02.04.2018	2018/32	15.05.2018
5	1136 sayılı Avukatlık Kanunu uyarınca faaliyet gösteren avukatlar	02.04.2018	2018/32	15.05.2018
6	3568 sayılı Serbest Muhasebeci Mali Müşavirlik ve Yeminli Mali Müşavirlik Kanunu uyarınca faaliyet gösteren Serbest Muhasebeci Mali Müşavirler ve Yeminli Mali Müşavirler	02.04.2018	2018/32	15.05.2018
7	4458 sayılı Gümrük Kanunu uyarınca faaliyet gösteren Gümrük Müşavirleri ve Yetkilendirilmiş Gümrük Müşavirleri	28.06.2018	2018/68	18.08.2018
8	Arabulucular	05.07.2018	2018/75	18.08.2018
9	Yıllık çalışan sayısı 50'den az ve yıllık mali bilanço toplamı 25 milyon TL'den az olan gerçek veya tüzel kişi veri sorumlularından ana faaliyet konusu özel nitelikli kişisel veri işleme olmayanlar	19.07.2018	2018/87	18.08.2018

ÖNEMLİ NOT - Veri Sorumluları Siciline kayıt yükümlülüğünden istisna olmak, 6698 sayılı Kişisel Verilerin Korunması Kanunundan da istisna olmak anlamına gelmemektedir. Kayıt yükümlülüğünden istisna olan veri sorumluları da diğer veri sorumluları gibi 6698 sayılı Kanun hükümlerine uymak zorundadır.

Kaynak: Kişisel Verileri Koruma Kurumu, https://www.kvkk.gov.tr/Icerik/5273/Istisna, Erişim Tarihi: 18.12.2018.

Yönetmelik'in 5. maddesinin 1. fıkrasının (ç) bendine göre, Sicil başvurularında Sicil'e açıklanacak bilgiler Kişisel veri işleme envanterine dayalı olarak hazırlanır. Kişisel veri işleme envanteri; veri sorumlularının iş süreçlerine

bağlı olarak gerçekleştirmekte oldukları kişisel veri işleme faaliyetleri, kişisel veri işleme amaçları, veri kategorisi, aktarılan alıcı grubu, kişisel verilerin işlendikleri amaçlar için gerekli olan azami süreyi, yabancı ülkelere aktarımı öngörülen kişisel verileri ve veri güvenliğine ilişkin alınan tedbirleri açıklayarak detaylandırdıkları envanteri tanımlamaktadır. Veri sorumlularının hazırlayacakları bu envanter kamuya açıklık ilkesi ile birlikte düşünüldüğünde ilgili kişilerin bilgi edinebilmeleri açısından önemli bir uygulamadır.

Kişisel veri işleme envanteri tanımında belirtilen, "kişisel verilerin işlendikleri amaçlar için gerekli olan azami süre"nin belirlenmesine ilişkin hükümler, Yönetmelik'in 9. maddesinin 4. fıkrasında detaylı olarak açıklanmıştır. Buna göre:

Veri sorumluları tarafından Sicil'e açıklanacak kişisel verilerin mevzuatta öngörülen veya işlendikleri amaç için gerekli olan azami muhafaza edilme süresine ilişkin bilgiler, veri kategorileri ile eşleştirilerek Sicil'e bildirilir. Veri sorumlusu tarafından Sicil'e bildirilen veri kategorilerinin işleme amaçları ve bu amaçlara dayalı olarak işlenmeleri için gerekli olan azami muhafaza edilme süreleri ile mevzuatta öngörülen süreler farklı olabilir. Bu durumda mevzuatta azami muhafaza edilme süresi öngörülmüşse öngörülen bu süre, yoksa bunlardan en uzun süre esas alınarak bu veri kategorisi için Sicil'e bildirim yapılır. Kişisel verilerin işlendikleri amaç için gerekli olan azami muhafaza edilme süresi belirlenirken;

- İlgili veri kategorisinin işlenme amacı kapsamında veri sorumlusunun faaliyet gösterdiği sektörde genel teamül gereği kabul edilen süre,
- İlgili veri kategorisinde yer alan kişisel verinin işlenmesini gerekli kılan ve ilgili kişiyle tesis edilen hukuki ilişkinin devam edeceği süre,
- İlgili veri kategorisinin işlenme amacına bağlı olarak veri sorumlusunun elde edeceği meşru menfaatin hukuka ve dürüstlük kurallarına uygun olarak geçerli olacağı süre,

- İlgili veri kategorisinin işlenme amacına bağlı olarak saklanmasının yaratacağı risk, maliyet ve sorumlulukların hukuken devam edeceği süre,
- Belirlenecek azami sürenin ilgili veri kategorisinin doğru ve gerektiğinde güncel tutulmasına elverişli olup olmadığı,
- Veri sorumlusunun hukuki yükümlülüğü gereği ilgili veri kategorisinde yer alan kişisel verileri saklamak zorunda olduğu süre,
- Veri sorumlusu tarafından, ilgili veri kategorisinde yer alan kişisel veriye bağlı bir hakkın ileri sürülmesi için belirlenen zamanaşımı süresi, dikkate alınır.

Kanun'dan farklı olarak, Yönetmelik'te bahsi geçen iki yeni kişi vardır, bunlar; Veri sorumlusu temsilcisi ve irtibat kişisidir. Veri sorumlusu temsilcisi[152] ve irtibat kişisi[153] çalışmanın ileriki bölümlerinde detaylı olarak anlatılacaktır.

Veri sorumlusunun Sicil'e kayıt olmasını gerektiren veri işleme faaliyetlerine son vermesi ya da veri işleme faaliyetlerinin ortadan kalkması halinde; veri sorumlusu, Kurum'a başvurarak Sicil'den kaydının silinmesini talep edebilir. Bu kayıtlar istendiğinde erişilebilir olmakla birlikte üzerinde herhangi bir değişiklik yapılamayacak şekilde tutulacak ve veri sorumlusunun Sicil'e kayıtlı olduğu dönemdeki yükümlülükleri ortadan kalkmış sayılmayacaktır.

Veri sorumlularının bu yükümlülüğe aykırı hareket etmeleri halinde, Kanun'un 18. maddesinin 1. fıkrasının (ç) bendinde yer alan idari para cezası uygulanacaktır.

[152] Bkz: s. 109.
[153] Bkz: s. 119.

3.4.1.4.Aydınlatma Yükümlülüğü

Kanun'un 10. maddesinde düzenleme alanı bulan aydınlatma yükümlülüğü veri sorumlularına yüklenmiş en önemli ve kapsamlı yükümlülüklerden biridir. Bu yükümlülükle birlikte hedeflenen; ilgili kişinin, yasal olarak düzenlenmiş tüm haklarını etkin kullanabilmesini sağlamak ve bu kullanımın şeffaf bir biçimde gerçekleştirilebilmesidir. Bu kapsamda; veri sorumluları, kişisel verilerini işlediği ilgili kişilere, işlenen verilerin kim tarafından, hangi amaçlarla, hangi yöntemlerle ve hangi hukuki gerekçelere dayanarak işlenebileceği, kimlere hangi amaçlarla aktarılabileceği hususunda bilgi vermekle yükümlülerdir. Veri sorumlusunun, ilgili kişilerin verilerinin sözleşmesel bir ilişki ile bir başkası tarafından işlenmesini sağladığı durumlarda karşımıza "veri işleyen" kavramı çıkacaktır. Aşağıda detaylı olarak açıklanacak olduğu üzere; veri işleyen, veri sorumlusunun verdiği yetkiye dayanarak onun adına kişisel verileri işleyen gerçek veya tüzel kişi olarak tanımlanmıştır. Bu kapsamda veri işleyen de Kanun'un 10. maddesi uyarınca veri sorumlusu gibi aydınlatma yükümlülüğü ile sorumlu olacaktır, ilgili maddeye göre bu yükümlülük "veri sorumlusu veya yetkilendirdiği kişi"ye yüklenmiştir. Veri sorumlularının temsilcilerinin olması halinde temsilcinin de kimliği aydınlatma yükümlülüğü kapsamında ilgili kişiye verilmelidir.

Aydınlatma yükümlülüğü, veri sorumlusunun Kanun kapsamında belirtilen diğer yükümlülüklerinden biri olan "hukuka ve dürüstlük kuralına uygunluk" şartıyla da bağlantılı bir yükümlülüktür. Bu sayede, ilgili kişi, kendine ait verilerin işlendiğini bilerek hakları doğrultusunda hareket edebilecek özgürlüğe sahip olmalıdır. Özel hukukun temel ilkelerinden biri olan eşitlik ilkesine aykırı olmayacak şekilde taraflar dengeli bir konumda bulunacaklardır.

Aydınlatma yükümlülüğünün yerine getirilmesi konusunda bir şekil şartı bulunmamaktadır. Aydınlatma yükümlülüğünün yerine getirilmesi, ilgi kişinin onayına tabi değildir. Tek taraflı bir beyanla aydınlatma yükümlülüğü yerine

getirilebilir. Aydınlatma yükümlülüğünün yerine getirildiğinin ispatı da veri sorumlusuna aittir.

Aydınlatma Yükümlülüğünün Yerine Getirilmesinde Uyulacak Usul ve Esaslar Hakkında Tebliğ'in (Çalışmanın bundan sonraki bölümlerinde "Tebliğ" olarak anılacaktır.) 5. maddesinin 1. fıkrasının (g) bendine göre; aydınlatma yükümlülüğü kapsamında açıklanacak kişisel veri işleme amacının belirli, açık ve meşru olması gerekir. Aydınlatma yükümlülüğü yerine getirilirken, genel nitelikte ve muğlak ifadelere yer verilmemelidir. Gündeme gelmesi muhtemel başka amaçlar için kişisel verilerin işlenebileceği kanaatini uyandıran ifadeler kullanılmamalıdır. Bu madde veri sorumlusunun bilgilendirme yaparken ilgili kişinin haklarına riayet etmesi gerekliliğinin önemini vurgulamaktadır. Yeterli açıklıkta olmayan aydınlatma, yükümlülüğün yerine getirilmesini engeller niteliktedir, bu nedenle ilgili kişiye yapılacak olan bilgilendirmenin Tebliğ'de de belirtilen şartları taşıması gerekmektedir. Bununla bağlantılı olarak aynı maddenin (ğ) bendinde de bildirimi anlaşılır, açık ve sade bir dil kullanılarak gerçekleştirilmesi gerekliliğinden bahsedilmiştir.

Aydınlatma yükümlülüğü kapsamında ilgili kişinin bilgi sahibi olması gereken en önemli hususlardan biri de "hukuki sebep"tir. İlgili kişi, kendine ait hangi verilerinin veri sorumlusunda bulunduğunu öğrenmenin yanı sıra, bu verilerin ne sebeple tutulduğuna ilişkin de bilgilendirilmelidir. Tebliğ'in 5. maddesinin 1. fıkrasının (h) bendine göre; Kanun'un 10. maddesinin birinci fıkrasının (ç) bendinde yer alan "hukuki sebep"ten kasıt, aydınlatma yükümlülüğü kapsamında kişisel verilerin, Kanun'un 5. ve 6. maddelerinde belirtilen işleme şartlarından hangisine dayanılarak işlendiğidir. Aydınlatma yükümlülüğünün yerine getirilmesi esnasında hukuki sebebin açıkça belirtilmesi gerekmektedir.

Kişisel verilerin ilgili kişilerden elde edilmemesi halinde aydınlatma yükümlülüğünün yerine getirilmesi; Tebliğ'in 6. maddesinin 1. fıkrasına göre; kişisel verilerin elde edilmesinden itibaren makul bir süre içerisinde, kişisel

verilerin ilgili kişi ile iletişim amacıyla kullanılacak olması durumunda, ilk iletişim kurulması esnasında, aktarılacak olması halinde ise en geç kişisel verilerin ilk kez aktarımının yapılacağı esnada ilgili kişiyi aydınlatarak yerine getirilmelidir. Madde yeteri kadar açık ve yol gösterici olmasa da veri sorumlusuna aydınlatma yükümlülüğünün yerine getirilmesinin zamanıyla ilgili yol göstermektedir. Makul süre ifadesinin, ilgili kişinin hakkını yeterli derecede koruma sağlanmasına engel olabileceği ve verilerin üçüncü kişilerden elde edilmesiyle alakalı olarak bir bilgilendirme şekline yer verilmediği açıktır.

Kurum'un çeşitli alanlarda veri işleyene ve veri sorumlularına ilişkin aydınlatma yükümlülüğüne dair yol gösterici yöntemleri de yer almaktadır. Örnek olarak; kamera kaydı gerçekleştirilen bir işletmede, kamera kayıtlarının tutulmasına ve kayıtların ne amaçlarla kullanılacağına ilişkin bilgilendirme yapılırken, ziyaretçi ve çalışanların görebileceği yerlere, kamera kaydı yapıldığına ilişkin işaret ve yazılar yerleştirilmesi ve veri işleme ve saklama amaçlarının detaylı olarak yer verilmesi bir yöntem olarak sunulmuştur[154]. İşverenin, işletme dahilinde kamera kaydı tutmasıyla ulaşmak istediği amaca ulaşabileceği alternatif yolların olması halinde, o yollardan birinin kullanılması daha isabetli olacaktır. Eğer ulaşılmak istenen amaca ancak kamera kaydı ile ulaşılabiliyor ise bu durumda da ölçülülük ilkesine ve gereklilik ilkesi doğrultusunda hareket ediliyor olması gerekmektedir[155]. Bu nedenle, işletme dahilinde yapılacak olan kamera kaydının yeterli düzeyde açık olarak bilgilendirme içermesi gerekmektedir.

Aydınlatma yükümlülüğüne ilişkin, Kanun'un 28. maddesinin 2. fıkrasında belirli istisnalar yer almaktadır;

- Kişisel veri işlemenin suç işlenmesinin önlenmesi veya suç soruşturması için gerekli olması

[154] Kişisel Verileri Koruma Kurumu, Kişisel Verilerin Korunması Kanunu Hakkında Sıkça Sorulan Sorular, s. 91.
[155] BEYTAR, s. 189.

Kurum, bu istisna için; bir polisin ciddi bir suçla ilgili şüphelinin kişisel verilerini işlemesi bu kapsamda değerlendirilebileceğini, çünkü polisin hangi kişisel verilerini işlediği veya hangi amaçlarla işlediğini şüpheliye anlatması halinde, şüphelinin ilgili verileri yok etmesi veya silmesi riski doğacağı riskini örnek olarak vermiştir[156].

- İlgili kişinin kendisi tarafından alenileştirilmiş kişisel verilerin işlenmesi

Kurum, bu istisna için; kişinin herkesin erişimine açık bir şekilde sosyal medya hesabında kişisel verisini paylaşması halinde verinin işlenmesi örneğini vermiştir[157]. Sosyal medya, bireylerin, aile bireyleriyle ve diledikleri kişilerle bir ağ yaratıp o ağa katıldıkları, hayatlarıdnan kesitler paylaştıkları iletişim platformları olarak değerlendirilebilir[158]. İlgili kişilerin sosyal medya kullanımıyla yayılan kişisel verilerin durumu tartışmaya açıktır. İlgili kişilerin kendisi tarafından alenileştirilmiş verileri, açık rıza aranmaksızın işlenebilmesinin yanı sıra aydınlatma yükümlülüğünün de istisnası kabul edilmiştir. Bir verinin aleni hale gelmesi, verinin başkaları tarafından bilinir duruma gelmesiyle de mümkün olabilecektir ve bu durum her zaman verinin ilgili kişi tarafından alenileştirilmiş olduğu anlamına gelmemekte ve aleni hale gelmiş olan veri kişisel veri olma özelliğini kaybetmemektedir[159]. Ancak, çalışmanın önceki bölümlerinde detaylı olarak anlatılan unutulma hakkı[160] gibi önemli problemler yaratabilecek bir düzenleme olarak kabul edilebilir. Özellikle sosyal medyada, verilerin yayılma hızı oldukça yüksek ve takibi de oldukça güçtür. İlgili kişinin kendisine ait veriyi alenileştirirken güttüğü amaç dikkate alınmalıdır. Aynı zamanda internet sitelerinde verilerin işlenmesi amacıyla, ziyaretçi ilgili kişilerin rızasını elde etme

[156] Kişisel Verileri Koruma Kurumu, Kişisel Verileri Koruma Kurumu, Kişisel Verilerin Korunması Kanunu ve Uygulaması, s. 26.
[157] Kişisel Verileri Koruma Kurumu, Kişisel Verilerin Korunması Kanunu ve Uygulaması, s. 26.
[158] ATASOY, s. 282.
[159] Şehriban İpek AŞIKOĞLU, Avrupa Birliği ve Türk Hukukunda Kişisel Verilerin Korunması ve Büyük Veri, 1. Baskı, On İki Levha Yayınları, İstanbul, Kasım 2018, s. 131-132.
[160] Bkz: s. 11.

yöntemleri tartışmalı bir konudur[161]. Veri her ne kadar alenileştirilmiş olsa da veri sorumlusu verilerin işlenmesinde aranan temel prensiplere ve yükümlülüklere uygun davranmalıdır. Keza, Çalışma Grubu, veri sorumlularının, sosyal medya sitelerinde, ilgililer tarafından yüklenen verilerin karşılaşabileceği güvenlik risklerine dair ilgili kişilere yeterli derecede bilgi verilmesi gerekliliğini belirtmiştir[162]. Meşru bir amaç olmadan alenileştirilmiş bir veriyi işleyen veri sorumlusunun Kanun'a aykırı hareket ettiğini söyleyebilecekken, aydınlatma yükümlülüğünde istisna kapsamına girdiğini belirtmek çelişkili bir durum meydana getirecektir.

- Kişisel veri işlemenin kanunun verdiği yetkiye dayanılarak görevli ve yetkili kamu kurum ve kuruluşları ile kamu kurumu niteliğindeki meslek kuruluşlarınca, denetleme veya düzenleme görevlerinin yürütülmesi ile disiplin soruşturma veya kovuşturması için gerekli olması.
- Kişisel veri işlemenin bütçe, vergi ve mali konulara ilişkin olarak Devletin ekonomik ve mali çıkarlarının korunması için gerekli olması.

Bu istisnaların gerçekleşmesi halinde, aydınlatma yükümlülüğünün düzenlendiği Kanun'un 10. maddesi ve zararın giderilmesi hariç Kanunun 11. maddesi uygulanmaz.

Kanun'un 3. maddesinde, "Açık Rıza" kavramı; *"belirli bir konuya ilişkin, bilgilendirilmeye dayanan ve özgür iradeyle açıklanan rızayı ifade eder."* şeklinde tanımlanmıştır. Buna göre ilgili kişinin açık rızasının alınması da aydınlatma yükümlülüğü kapsamında değerlendirilebilir. Kanunun lafzından anlaşılacağı üzere, açık rızanın bilgilendirilmeye dayanması gerekmektedir. Kanunun 5. maddesinde ilgili kişinin açık rızası aranmaksızın kişisel verilerin işlenmesinin mümkün olduğu haller sayılmıştır.

[161] ATASOY, s. 270.
[162] Art. 29 WP, Opinion 5/2009 on Online Social Networking, Adopted on 12 June 2009, s. 7.

Tebliğ'in 5. maddesinin 1. fıkrasının (f) bendinde *"kişisel veri işleme faaliyetinin açık rıza şartına dayalı olarak gerçekleştirilmesi halinde, aydınlatma yükümlülüğü ve açık rızanın alınması işlemlerinin ayrı ayrı yerine getirilmesi gerekmektedir."* denilmiştir. Bu hüküm ile, açık rıza alınması gerekliliğinin, aydınlatma yükümlülüğünü yerine getirme hususunda herhangi bir istisna oluşturmadığı belirtilmek istenmiştir. İlgili kişinin, Kanun'a uygun açık rızasının varlığı halinde de veri sorumlusunun aydınlatma yükümlülüğü devam edecektir. Veri sorumlusuna yüklenen açık rıza alınması ve bilgilendirme yapılması yükümlülüklerini birbirinden ayrı iki farklı yükümlülük olarak yerine getirilmeye devam edilmelidir[163].

Açık rızanın işlevi dikkate alındığında, genel işlem şartları çerçevesinde yer verilen bir hükümle ilgili kişinin açık rızasının alınabilmesi kural olarak mümkün olmamaktadır. TBK'nın 20. maddesinde genel işlem koşulları, bir sözleşme yapılırken düzenleyenin, ileride çok sayıdaki benzer sözleşmede kullanmak amacıyla, önceden, tek başına hazırlayarak karşı tarafa sunduğu sözleşme hükümleri olarak tanımlanmıştır. Bir hukuka uygunluk sebebi olarak açık rıza; ilgili kişinin önceden bilgilendirilmiş olması üzerine bilinçli olarak verilen bir beyanla mümkündür. Önceden, tek taraflı olarak hazırlanan bir sözleşmenin herhangi bir bölümünde yer verilen bir hükmün, Kanun'a göre verilmesi gereken "açık rıza"nın niteliklerini taşımayacağı açıktır[164].

Yönetmelik de "kişisel veri işleme envanteri" kavramıyla birlikte aydınlatma yükümlülüğü kapsamında veri sorumlularına ışık tutmaktadır. Çalışmanın önceki bölümlerinde anlatılmış olan kişisel veri işleme envanteri[165], ilgili kişilere bilgi edinme hakkı kapsamında şeffaflık sağlamaktadır. Veri sorumluları tarafından kişisel veri işleme envanterinde açıklanan bilgiler, veri

[163] Murat Volkan DÜLGER, Kişisel Verileri Koruma Kurulu'nun 2018/10 Sayılı Kararı İle Aydınlatma Yükümlülüğünün Yerine Getirilmesi Ve Veri Sorumlusuna Başvuru Konulu Tebliğlere İlişkin Değerlendirme, 2018, s. 15.
[164] ÇEKİN, s. 61.
[165] Bkz: s. 83.

sorumlusunun aydınlatma yükümlülüğü ve ilgili kişinin başvurusunun yanıtlanması ve açık rızanın kapsamının belirlenmesinde önem taşıyacaktır[166].

Tebliğ, veri sorumlularının aydınlatma yükümlülüğü kapsamında daha detaylı bilgilere yer vermiştir. Tebliğ, aydınlatma yükümlülüğünün kapsamı, uyulacak usul ve esaslar ve kişisel verilerin ilgili kişiden elde edilmemesi halinde aydınlatma yükümlülüğünün nasıl olacağı hakkında da bilgi vermektedir.

Tebliğ'in "Aydınlatma yükümlülüğünün kapsamı" başlıklı 4. maddesi Kanun'da yer alan bilgilerden farklı olmamakla birlikte, usul ve esas kısmıyla ilgili detaylı bilgilere yer vermektedir. Buna göre; *"Kişisel verilerin elde edilmesi sırasında veri sorumluları veya yetkilendirdiği kişilerce, ilgili kişilerin bilgilendirilmesi gerekmektedir. Bu yükümlülük yerine getirilirken veri sorumluları veya yetkilendirdiği kişilerce yapılacak bilgilendirmenin asgari olarak; veri sorumlusunun ve varsa temsilcisinin kimliği, kişisel verilerin hangi amaçla işleneceği, kişisel verilerin kimlere ve hangi amaçla aktarılabileceği, kişisel veri toplamanın yöntemi ve hukuki sebebi, ilgili kişinin Kanun'un 11. Maddesinde sayılan diğer hakları konularını içermesi gerekmektedir."*

Tebliğ'in "Usul ve esaslar" başlıklı 5. maddesine göre, veri sorumlusu ya da yetkilendirdiği kişi sözlü, yazılı, ses kaydı, çağrı merkezi gibi fiziksel veya elektronik ortam kullanmak suretiyle aydınlatma yükümlülüğünü yerine getirebilecektir. İlgili maddeye göre; kişisel veri işlendiği her durumda, kişisel veri işleme amacı değiştiğinde aydınlatma yükümlülüğü ayrıca yerine getirilmelidir. Veri sorumlusunun farklı birimlerinde farklı amaçlarla işlenen kişisel veriler de her bir birim nezdinde ayrıca aydınlatma yükümlülüğüne uymalıdır. Görüleceği üzere veri sorumlusunun en önemli yükümlülüklerinden biri olarak nitelendirilen aydınlatma yükümlülüğünün, Tebliğ ile hangi durumlarda ayrıca alınması gerektiği belirtilmiştir. Uygulamada, özellikle internet

[166] ÇEKİN, s. 123.

sitelerinde veri işlenmesinin öncesinde ilgili kişilerin aydınlatılması ve alınan izinlerin bu kapsamda geçerlilikleri her bir işleme durumunda ve her yeni amaçta tekrarlanması gerekliliği ortaya çıkacaktır.

"Örneğin internet ortamındaki aktif davranış, önceden işaretlenmiş olan kutucukların (checkbox) ilgili kişi tarafından işaretlenmesi (opt-in) ya da boş bir metin alanının (textarea) doldurulması veya benzeri bir yöntemle sağlanabilir. Buna karşılık daha önceden internet sitesi tarafından varsayılan olarak işaretlenmiş olan kutucuklar aracılığıyla (opt-out) kişinin rıza göstermesi, Kanun kapsamında geçerli bir irade beyanı teşkil etmez"[167]. Örneğin, davranışsal pazarlama kullanılan internet sitelerinde, ilgili kişilerin ilgi alanlarının kaydedilmesi ve ilgi alanlarına göre ürün ve sitelerin reklamlarıyla karşılaşılması sağlanırken, *"ilgilenebileceğiniz fırsatlar sunan X markası ile bilgilerinizi paylaşmamıza izin veriyorsanız, bu kutucuğa tıklayınız"* şeklinde bir açıklama ilgili kişiye sunuluyorsa bu durumda ilgili kişinin opt-in olarak rızasının alındığı kabul edilebilir, ancak e-posta hizmeti veren internet sitelerinde "bu iletileri görmek istemiyorsanız buraya tıklayınız" şeklinde bir açıklama ilgili kişiye sunuluyorsa ve ilgili kişi o kutucuğu tıklayarak verilerinin işlenmesini engellemesi, diğer bir ifade ile işleme faaliyetini durdurmak için aktif bir faaliyette bulunması halinde opt-out rızasını karşı tarafa ilettiği anlamına gelecektir, opt-out rıza söz konusu olduğunda ilgili kullanıcıdan aktif bir hareket beklenmektedir, aksi takdirde pasif kaldığı durumda verilerinin işlenmesine göz yumacağı varsayımıyla hareket edilmektedir[168]. Buna göre yalnızca internet ortamında değil tüm veri sorumlularının önceden alındığı varsayılan rıza ve bilgilendirmeye dayanarak yeni amaç ve durumlarda bu bilgilendirmeye dayanamayacağı açıktır.

İlgili kişilere, Kanun'un 11. maddesinde tanınan bilgi edinme hakkı, aydınlatma yükümlülüğüyle yakın ilişki içerisinde olmasına rağmen ayrı bir

[167] TAŞTAN, s. 161.
[168] ATASOY, s. 288.

kavram olarak değerlendirilmelidir. İlgili kişiler, veri sorumlularından bilgi edinme talebinde bulundukları takdirde, veri sorumluları tarafından gerekli bilgilerin sağlanması gerekir. Aydınlatma yükümlülüğü her ne kadar veri işlemeden önceki süreçte öngörülmüş bir yükümlülük olsa da veri sorumlusunun aydınlatma yükümlülüğünün devamlılık arz etmesi, veri güvenliğinin sağlanması açısından önemlidir. Aydınlatma yükümlülüğünün devamlılık arz eden bir şekilde yerine getirilmesi gerekliliği düşünüldüğünde, veri sorumlularının, ilgili kişilerin bilgi edinme taleplerine karşı vereceği yanıtlar aydınlatma yükümlülüğünün yerine getirilmesinin bir gereği olarak düşünülebilir. Bu kapsamda, veri sorumlusu, aydınlatma yükümlülüğü kapsamında, ilgili kişilerin, ilgili maddelerde sayılan haklara sahip olduğu konusunda bilgilendirme yapmakla yükümlü olmakla birlikte, ilgili kişilerin Kanun'un 11. maddesi kapsamındaki talepleri sonrasında yapılan işlemlere ilişkin ilgili kişileri aydınlatmakla da yükümlüdür.

Veri sorumlularının tek taraflı irade beyanıyla ilgili kişilere karşı yaptıkları bilgilendirme ile yerine getirdikleri aydınlatma yükümlülüğüne ek olarak; ilgili kişilerin, işlenen verilerine ilişkin daha detaylı bilgi edinme taleplerinin varlığı halinde, veri sorumluları yeterli açıklıkta ve anlaşılırlıkta bilgilendirme yaparak aydınlatma yükümlülüğüne uygun davranmakla yükümlüdürler. Veri sorumlularının, veri öznelerinin talepler doğrultusunda yaptıkları bu bilgilendirme Kurum'a göre "katmanlı bilgilendirme" olarak adlandırılmaktadır[169].

Kurum'un yaptığı tanıma göre; katmanlı bilgilendirme, amaca ilişkin bilgilendirilme yapılırken, önce kısa ve kolay anlaşılır bir metin sunup, metin vasıtasıyla, daha ayrıntılı açıklama talep edenlere yönelik detaylı açıklamalara işaret edilmesi durumudur.

İlgili kişi, veri sorumlusundan sadece olumlu değil, olumsuz bilgi edinme hakkına da sahiptir. Bu sebeple ilgili kişiye ait kişisel veri işlenmediği takdirde

[169] Kişisel Verileri Koruma Kurumu, Kişisel Verileri Koruma Kurumu 6698 Sayılı Kişisel Verilerin Korunması Kanunu'nun Uygulanmasına Yönelik Soru Cevaplar, s. 68.

veri sorumlusunun bunu da açıkça belirtmesi gerekecektir. Veri sorumlusu sessiz kalmakla aydınlatma yükümlülüğünü yerine getirmiş sayılmayacaktır[170].

Kanun'un lafzına bakıldığında 10. maddede yer alan aydınlatma yükümlülüğü Kanun'un 11. maddesini de kapsamaktadır. "İlgili kişinin hakları "başlıklı 11. maddeye göre herkes, veri sorumlusuna başvurarak kendisiyle ilgili;

Kişisel veri işlenip işlenmediğini öğrenme, kişisel verileri işlenmişse buna ilişkin bilgi talep etme, kişisel verilerin işlenme amacını ve bunların amacına uygun kullanılıp kullanılmadığını öğrenme, yurt içinde veya yurt dışında kişisel verilerin aktarıldığı üçüncü kişileri bilme, kişisel verilerin eksik veya yanlış işlenmiş olması hâlinde bunların düzeltilmesini isteme, Kanunun 7. maddesinde öngörülen şartlar çerçevesinde kişisel verilerin silinmesini veya yok edilmesini isteme, silme, düzeltme ve yok etme işlemlerin, kişisel verilerin aktarıldığı üçüncü kişilere bildirilmesini isteme, işlenen verilerin münhasıran otomatik sistemler vasıtasıyla analiz edilmesi suretiyle kişinin kendisi aleyhine bir sonucun ortaya çıkmasına itiraz etme, kişisel verilerin kanuna aykırı olarak işlenmesi sebebiyle zarara uğraması hâlinde zararın giderilmesini talep etme, haklarına sahiptir.

10.03.2018 tarihinde yayınlanan ve yürürlüğe giren Veri Sorumlusuna Başvuru Usul ve Esasları Hakkında Tebliğ'e göre; kişisel verisi işlenen her gerçek kişi veri sorumlusuna Türkçe bir başvuru ile başvurma hakkına sahiptir, yani bilgi edinme hakkından yararlanabilir. Veri Sorumlusuna Başvuru Usul ve Esasları Hakkında Tebliğ, başvuru usul ve araçları hakkında da bilgi vermektedir. Veri sorumlusu verisi işlenen gerçek kişinin başvuru hakkını en etkin biçimde kullanmasını sağlayacak her türlü tedbiri almalı ve bu hakkın kullanımını engelleyecek herhangi bir faaliyette bulunmamalıdır. Bu kapsamda veri

[170] ÇEKİN, s. 89.

sorumlusu, ilgili kişilerin başvurularını iletirken kullanacağı araçları zorlaştırmayarak, haklarını kullanmada destek olmalıdır.[171].

Veri sorumlusu başvuruları kabul edebilir veya reddedebilir ancak, red kararı Kanun'un 13. maddesinde de belirtildiği gibi gerekçeli olmalıdır. Cevap yazılı ya da elektronik ortamda başvurucuya bildirilmelidir. Bu kapsamda veri sorumlusuna yüklenmiş olan yükümlülüklerin aydınlatma yükümlülüğü kapsamında ilgili kişiye sunulması gereken şeffaflık doğrultusunda amaca uygun yerine getirilmesi önemli noktalardan biridir. Veri sorumlusunun vereceği cevaplar, ilgili kişinin yeterli bilgilendirilmesi koşulunu sağlamalıdır. Veri Sorumlusuna Başvuru Usul ve Esasları Hakkında Tebliğ'in 6. maddesinin 4. fıkrasında cevap yazısında olması gereken bilgiler sayılmıştır. Ancak bu bilgilerin olmadığı bir cevap yazısının akıbetinin ne olacağı ile ilgili bir bilgi yer almamaktadır. Cevap yazısında muhakkak bulunması gereken ifadelerin tek tek sayılması, veri sorumlusunun, muhakkak bulunması gereken ifadelerden herhangi birini içermeyen cevap yazısının geçerli bir cevap yazısı olmadığını, cevap verilmemiş sayılması gerektiği gösterebilir[172].

Veri Sorumlusuna Başvuru Usul ve Esasları Hakkında Tebliğ'in 6. maddesinin 5. fıkrasına göre; veri sorumlusunun başvuruyu en kısa sürede ve en geç otuz gün içinde ücretsiz olarak sonuçlandırması gerekmektedir. Ancak fıkranın devamında "işlemin ayrıca bir maliyet gerektirmesi halinde, 7. maddede belirtilen ücret alınabilir, başvurunun, veri sorumlusunun hatasından kaynaklanması halinde alınan ücret ilgiliye iade edilir." denmiştir. Kanun'un 13. maddesi, ücret konusunda Kurul'a düzenleme olanağı bırakmışsa da "ayrıca bir maliyeti gerektirmesi halinde" ibaresiyle asıl olanın ücretsiz bir şekilde yükümlülük kapsamında bilgi verilmesi olduğu açıktır. 7. maddenin 1. fıkrası; ilgili kişinin başvurusuna yazılı olarak cevap verilecekse, on sayfaya kadar ücret alınmaz. On sayfanın üzerindeki her sayfa için 1 Türk Lirası işlem ücreti

[171] DÜLGER, Aydınlatma Yükümlüğünün Yerine Getirilmesi ve Veri Sorumlusuna Başvuru s. 10.
[172] DÜLGER, Aydınlatma Yükümlüğünün Yerine Getirilmesi ve Veri Sorumlusuna Başvuru s. 11.

alınabilir, 2. fıkrası ise; başvuruya cevabın CD, flash bellek gibi bir kayıt ortamında verilmesi halinde veri sorumlusu tarafından talep edilebilecek ücret kayıt ortamının maliyetini geçemez" şeklinde düzenlenmiştir. Veri Sorumlusuna Başvuru Usul ve Esasları Hakkında Tebliğ'in 6. maddesinin 5. fıkrası ve 7. maddesi her ne kadar bağlantılı gözükse de çelişkiler doğurabilecek iki düzenleme olarak karşımıza çıkmaktadır. Şöyle ki; 6. maddenin 5. fıkrası "işlemin ayrıca bir maliyet gerektirmesi halinde" ibaresini kullanarak 7. maddeye atıfta bulunmuş, ancak 7. madde ise on sayfaya kadar ücret alınmayacağını belirtmiştir, ki bu ücret yazılı olarak verilen cevaba mahsustur, cevabın CD, flash bellek gibi kayıt ortamında verilmesi halinde veri sorumlusuna kayıt ortamının maliyetini geçemeyeceği belirtilmiştir. Bu iki madde arasındaki belirsizlik nihayetinde yasal olarak verilen hakkını kullanmak için ücret ödemek zorunda bırakılan ilgili kişiye yansıtılacaktır. Ücret konusu için yapılacak yasal düzenleme, aydınlatma yükümlülüğünün amacına aykırı olmayan ve ilgili kişilerin bu haklarını kullanırken tereddüt yaşamadan başvurabilecekleri bir şekilde hayata geçmelidir.

3.4.1.5.Doğru ve Gerektiğinde Güncel Olma

Veri sorumlusu, faaliyeti kapsamında elde ettiği ve işlediği verileri doğru ve güncel tutmakla da yükümlüdür. Bu yükümlülük ile birlikte ilgili kişi, kişisel verilerinin doğru şekilde işlenip işlenmediğini öğrenme ve bu verilerin doğruluklarını belirli aralıklarla kontrol etme hakkına sahip olacağından, hakları da korunma altına alınmış olacaktır. "İlgili kişinin hakları" başlıklı, Kanunun 11. maddesinin 1. fıkrasının (d) bendi de herkesin kişisel verilerin eksik veya yanlış işlenmiş olması halinde bunların düzeltilmesini isteme hakkı olduğunu ve veri sorumlusuna bu konuda başvurabileceğini düzenlemiştir. Kanun'da detaylı olarak ifade edilmeyen ancak Regülasyon'da açık olarak düzenlenen, ilgili kişilerin verilere erişim ve düzeltme talep hakkı işbu yükümlülükler ile somutlaşarak, bu hakların uygulamada vücut bulmasına imkân sağlamaktadır. Bahsedilen haklar Kanun'un 11. maddesinin 1. fıkrasının (a) ve (d) bentlerinde Regülasyon'a paralel

olacak şekilde düzenlenmiştir. Anayasanın 20. maddesinde de "verilere erişme, bunların düzeltilmesini talep etme" hakkı doğrultusunda ilgili kişinin hakları açıkça ifade edilmiştir.

Kanunda ilgili kişiye böyle bir hak tanınmış olması, veri sorumlusunun verileri doğru ve gerektiğinde güncel tutma yükümlülüğünü etkilememektedir. Veri sorumlusu verilerin doğru ve güncel tutulabilmesi açısından her türlü teknik tedbirleri almalı, ilgili kişilerin müdahale imkânı olan hallerde de onların doğru ve güncel tutabilmeleri adına imkân sağlamalıdır. Günümüzde veri sorumlularının birçoğu ilgili kişilere internet sayfaları üzerinden bu şekilde bir hizmet sunmaktadırlar, genellikle "Hesabım" başlıklı sekmelerle ilgili kişiler, veri sorumlusunda bulunan verilerini güncelleme imkanına sahiptirler.

Delillerin muhafaza edilmesi gibi, verilerin güncel tutulması gerekliliğine istisna olarak gösterilebilecek durumlar da söz konusu olduğunda, verilerin güncellenmemesi ya da en azından eski verilerin de muhafaza edilmesi haklı görülebilir[173]. Kanunun lafzına da bakıldığında "gerektiğinde güncel olma" ifadesi de bu görüşü destekler nitelikte gösterebilir.

İlgili kişinin veri sorumlusuna ilettiği haklı bir düzeltme talebi üzerine, talep doğrultusunda işlem yapmayan veri sorumlusunun veri işleme faaliyeti, kanunda açık olarak düzenlenmiş olan, doğru ve gerektiğinde güncel olma şartını artık sağlamadığından dolayı hukuka aykırı şekilde işleniyor olarak değerlendirilecektir.

3.4.1.6.Veri Güvenliğine İlişkin Yükümlülükleri Yerine Getirme

Kanun'un 12. maddesi uyarınca kişisel verilerin hukuka aykırı olarak işlenmesini ve bu verilere hukuka aykırı olarak erişilmesini önlemeye yönelik

[173] ÇEKİN, s.53.

idari ve teknik tedbirlerin alınması ve bunların hukuka uygun olarak muhafazasının sağlanması veri sorumlusuna, veri güvenliğini sağlamak adına yüklenmiş sorumluluklar olarak düzenlenmiştir. Veri güvenliği ilkesinin gerçekleşmesiyle koruma altına alınan veriler, ilgili ilgili kişilerin korunmasını dolaylı da olsa sağlayacaktır, bu nedenle oldukça önem arz eden bir ilke olduğu açıktır.

Veri güvenliği, zaman itibariyle veri ihlalinin gerçekleşmesinden önce kişisel verilerin teknik ve idari yollardan korunmasına hizmet eder ve verinin kötü niyetli bir şekilde işlenmesinin önüne geçmeye çalışır. Kişisel verilerin korunması bağlamında veri güvenliği ise, bilgi sisteminin değil, sistem içerisindeki verilerin içeriğinin korunmasına hizmet etmektedir[174].

Teknolojilerin sağladığı imkanlar ve oluşturduğu tehlikeler dikkate alındığında kişisel verilerin korunmasının sadece hukuki yöntemlerin yanı sıra teknolojik yollarla da korunma altına alınması kaçınılmazdır. Bu kapsamda veri sorumlusundan işlevsel ve güvenilebilir bir koruma sağlayabilmesi için gerekli bütün önlemleri alması beklenmektedir[175].

Verilerin elde edildiği ilk an ile sonrasında bu verilerin üzerinde gerçekleştirilen her işlem işleme olarak adlandırılır. Verilerin işlenmesi, zincirleme bir döngü olarak düşünülmelidir ve verilerin nasıl tutulduğu ve kullanıldığı verinin kendisi kadar önemlidir[176]. Kanun'un esas noktalarından biri olan ve tüm süreci kapsayan "veri işleme" otomatik yolla olabileceği gibi herhangi bir veri kayıt sisteminin parçası olmak kaydıyla otomatik olmayan yollarla da işlenebilir. Veri kayıt sistemi ise Kanun'un 3. maddesinde; kişisel verilerin belirli kriterlere göre yapılandırılarak işlendiği kayıt sistemi olarak tanımlanmıştır. Otomatik yolla işlemenin bir bilişim sistemi üzerinden

[174] TAŞTAN, s. 74.
[175] ÇEKİN, s. 11.
[176] Kişisel Verileri Koruma Kurumu, 6698 Sayılı Kişisel Verilerin Korunması Kanunu'nda Yer Alan Temel Kavramlar s. 11-12.

gerçekleştiği düşünülürse, bir bilişim sistemi üzerinden işlenen veri yerine, eski usul elle tutulan kayıtlar, geleneksel dosyalama vs. yoluyla işlenen verinin Kanun tarafından kabul görmesi veri kayıt sisteminin bir parçası olması halinde mümkün olacaktır. Kurul, ilgili madde gereği, kişisel verilerin tamamen veya kısmen otomatik olan ya da herhangi bir veri kayıt sisteminin parçası olmak kaydıyla otomatik olmayan yollarla elde edilmesi, kaydedilmesi, depolanması, muhafaza edilmesi, değiştirilmesi, yeniden düzenlenmesi, açıklanması, aktarılması, devralınması, elde edilebilir hale getirilmesi, sınıflandırılması ya da kullanılmasının engellenmesi gibi veriler üzerinde gerçekleştirilen her türlü işlemin, kişisel verilerin işlenmesi olarak düzenlendiği ve sayılan eylemlerin gerçekleştirilebilmesi için öncelikle Kanun'un 5. ve 6. Maddelerinde sayılan işlenme şartlarından birinin bulunması, ayrıca Kanun ile öngörülen diğer yükümlülüklerin yerine getirilmesi gerektiğini belirtmiş, Kanun hükümlerine aykırı olarak ilgili kişilerin açık rızalarını almaksızın isimden telefon numarası veya telefon numarasından isim sorgulanması şeklinde rehberlik hizmeti veren internet siteleri ve uygulamalara ilişkin olarak, Kanun'da ve ilgili mevzuatta dayanağı olmaksızın veri işlenmesinin Kanun'un 15. Maddesinin 7. Fıkrası uyarınca derhal durdurulması gerektiğini ve aynı zamanda TCK kapsamında da "Verileri Hukuka Aykırı Olarak Verme veya Ele Geçirme" başlıklı 136. madde gereğince ilgili Cumhuriyet Başsavcılığına bildirimde bulunacağını 21.12.2017 Tarih 2017/61 Sayılı İlke Kararı ile bildirmiştir[177].

Kanun'un 12. maddesinin 1. fıkrası uyarınca veri sorumlusu; kişisel verilerin hukuka aykırı olarak işlenmesini, erişilmesini önlemek ve muhafazasını sağlamak için gerekli tüm teknik ve idari tedbirleri almakla yükümlüdür. Veri sorumlusunun ilgili madde uyarınca alması gereken tedbirlerin yalnızca teknik tedbirlerden ibaret olmadığının altını çizmek gerekmektedir. Veri sorumlusu, organizasyon gereği, işlenen kişisel verilere erişim yetkisi bulunan çalışanların yetkilerini aşmamaları, Kanun'a aykırı eylemlerden kaçınmaları için "idari" tedbirleri de

[177] Kişisel Verileri Koruma Kurulu, https://kvkk.gov.tr/Icerik/4113/2017-61, Erişim Tarihi: 22.02.2019.

almakla yükümlüdür. Bahsedilen yükümlülükle alakalı olarak Kurul'un "Veri sorumlusu nezdindeki kişisel verilere erişim yetkisi bulunan personelin yetkisi ve amacı dışında söz konusu verileri işlemesi hususunun değerlendirilmesine ilişkin 31.05.2018 Tarih ve 2018/63 Sayılı İlke Kararı" ile, konuyla alakalı Kurum'a yapılan şikayetler doğrultusunda; *"bir veri sorumlusu nezdinde bulundukları pozisyon veya görev itibariyle kişisel verilere erişme yetkisi olanlar tarafından, yetkileri aşmak ve/veya yetkilerini kötüye kullanmak suretiyle, kişisel amaçlara veya nedenlere bağlı olarak işleme amacı dışında söz konusu kişisel verilerin işlenmesi ve/veya bu verilerin üçüncü kişilerle paylaşılması Kanun'un 12. Maddesinin 1. Fıkrasına aykırılık teşkil edeceğinden, bu kapsamdaki eylemlerin önlenmesi amacıyla veri sorumlularınca uygun güvenlik düzeyini temin etmeye yönelik gerekli her türlü teknik ve idari tedbirin alınması gerektiği hususunda veri sorumlularının bilgilendirilmesine karar verilmiştir*[178]*."*

Veri sorumlusu, her türlü saldırıyı önlemekle yükümlü değildir. Kanun'da öngörülen düzenleme, neticeye bağlı bir sorumluluk hali değildir. Bilakis Kanun, veri sorumlusunun "gerekli" önlemleri almasını zorunlu kılmakla, veri sorumlusunun kendi üzerine düşen önlemleri alması halinde artık sorumluluktan kurtulabileceğine işaret etmektedir. Dolayısıyla bu çerçevede bir özen sorumluluğu halinden bahsetmek daha uygun olacaktır[179].

Veri sorumluları ve veri işleyenler teknik idari ve hatta hukuki süreçlerini Kanun'a ve Kanun'un getirdiği gerekliliklere uyumlaştırmakla yükümlüdürler. Bu yükümlülükler veri sorumlusunun işlediği verilere, önemine vs. göre değişiklik gösterecektir, yasal olarak herhangi bir model belirlenmemiştir. Veri güvenliğine ilişkin alınacak tedbirler, öncelikle veri sorumlusunun bulundurduğu verilere ilişkin tespitleri sonrasında belirlenmelidir. Veri sorumlusu verilerin üst düzey güvenlik tedbirleri gerektirdiğini veya standart bir güvenlik tedbiriyle

[178] Kişisel Verileri Koruma Kurulu, https://kvkk.gov.tr/Icerik/5248/2018-63, Erişim Tarihi: 22.02.2019.
[179] ÇEKİN, s. 105.

koruyabileceği verilerin tespitini yaptıktan sonra zaman, maliyet, yarar gibi etkenleri de göz önüne alarak kendisi, işletmesi ve elinde bulundurduğu veriler için en uygun teknik ve idari güvenlik tedbirlerini uygulamaya geçirmelidir.

Veri güvenliğini sağlamak adına alınacak tedbirler, standart bir özellik taşımamaktadır. Yani her bir veri sorumlusu, kendi işletmesi ve işlediği kişisel verilerin niteliği karşısında oluşabilecek muhtemel riskleri dikkate alarak alınacak önlemleri özgün surette kendisi belirleyecektir[180].

Veri güvenliği, işlenen veriler doğrultusunda ortaya çıkabilecek riskler dikkate alınarak, hem teknolojik gelişmeler doğrultusunda alınabilecek en iyi, hem de maliyet açısından en uygun yöntemlerle en makul ve uygun güvenlik seviyesinin yer aldığı tedbirlerin alınmasıyla sağlanabilir[181].

Kanun'un 12. maddesinin 2. fıkrası; veri sorumlusunun, kişisel verilerin kendi adına başka bir gerçek veya tüzel kişi tarafından işlenmesi hâlinde, birinci fıkrada belirtilen tedbirlerin alınması hususunda bu kişilerle birlikte müştereken sorumlu olacağını düzenlemiştir.

12. maddenin 4. fıkrasına göre; 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. Bu fıkra uyarınca veri sorumlusuna bağlı olarak çalışan her bir çalışanın bilgilendirilmesi gereği açıktır. İlgili fıkrayı, salt verinin bilinçli olarak hukuka aykırı şekilde paylaşımını engellemeyi amaçlayan bir düzenleme olarak görmek eksik olacaktır. Bu nedenle ki tüm çalışanların sorumluluk altına gireceği düşünülmelidir. Sorumluluk düzeyleri değişebileceği gibi tüm çalışanların veri güvenliğine ve ilgili tedbirlere ilişkin bilgilendirilmesi,

[180] TAŞTAN, s. 74.
[181] Doğan KILIÇ, Anayasal Bir Hak Olarak Kişisel Verilerin Korunması, AÜHFD 61 (3) 1089-1169, 2012, s. 1154.

gerekli çalışanlarla gizlilik anlaşmalarının yapılması fıkra uyarınca alınabilecek tedbirlerden gösterilebilir. Örneğin, bir hastanede, Hekimlik Meslek Etiği Kuralları[182] 9. maddesinde, *"Hekim, hastasından mesleği uygularken öğrendiği sırları açıklayamaz. Hastanın ölmesi, ya da o hekimle ilişkisinin sona ermesi, hekimin bu yükümlülüğünü ortadan kaldırmaz."* Denmektedir, ancak madde her ne kadar hekim için düzenlenmiş olsa da tüm sağlık çalışanları, kişisel verilerin gizliliği, hastanın sırlarının açıklanmaması gibi yükümlü olmaya devam edecektir[183].

Kurul'un da Kişisel Veri Güvenliği Rehberi[184] içerisinde yer verdiği başlıklar veri sorumlusuna "gerekli" teknik ve idari tedbirleri almasında yol gösterici olarak ışık tutacaktır. Rehberin içeriği de göz önüne alındığında veri sorumluları idari olarak; mevcut risk ve tehlikeleri belirlemeli, çalışanlarını eğitmeli, elindeki kişisel verileri mümkün olduğunca azaltmalı ve kendi veri güvenliği politikası ve prosedürlerini belirleyerek gerekli tedbirleri alma konusunda bir yol izleyebilmelidir. Rehber teknik tedbirler olarak; siber güvenliğin sağlanması, veri güvenliğinin takibi, veri içeren ortamların güvenliğinin sağlanması, verilerin bulutta depolanması, bilgi teknolojileri sistemleri tedariği, geliştirme ve bakımı ve veri yedeklenmesi başlıklarını belirleyerek veri sorumlularına yol göstermekte ve belirlenen başlıklar dahilinde veri sorumlularının kendi güvenlik politikaları ve teknik yöntemleri belirlemeleri yolunu açmaktadır.

3.4.1.7.Verileri Gerekli Olduğu Sürece Saklama

Söz konusu yükümlülük verilerin işlenme sürelerine ilişkin olarak düzenlenmiş bir yükümlülüktür. Kişisel verilerin işleme sürelerinin belirlenmesinde kural olarak kanunlarda yazılan sürelerin dikkate alınması

[182] http://www.ttb.org.tr/mevzuat/index.php?option=com_content&view=article&id=65:hekl-meslek-etkurallari&catid=4:t&Itemid=31, Erişim Tarihi: 25.02.2019.
[183] YILMAZ, s. 277.
[184] Kişisel Verileri Koruma Kurumu, Kişisel Veri Güvenliği Rehberi (Teknik ve İdari Tedbirler).

gerekir. Bunun dışında Kurul'un ilke karar almak suretiyle sektörlere özgü işleme süreleri belirlemeleri de mümkündür. Kanunlarda bir sürenin öngörülmemesi ve Kurul tarafından da bir kararın alınmamış olması durumunda, veri sorumluları, kişisel verileri ancak işledikleri amaç için gerekli olan süre kadar muhafaza edebilecektir[185]. Kanunun 16. maddesinin 3. fıkrasının (f) bendinde, veri sorumluları, Sicile kaydolurken, kişisel verilerin işlendikleri amaç için gerekli olan azami süreyi bildirmeleri gerektiğini düzenlemiştir.

Bu yükümlülük ile amaçlanan, veri sorumlusunun amaca ulaşması ya da amacın imkansızlaşması halinde, elinde bulunan kişisel verileri artık daha fazla muhafaza edilmesinin engellenmesidir. Kanun'un gerekçesinde de belirtildiği üzere; veri sorumluları, ilgili mevzuatta verilerin saklanması için öngörülen bir süre varsa bu süreye uyacak; yoksa verileri, ancak işlendikleri amaç için gerekli olan süre kadar muhafaza edebilecektir. Bir verinin daha fazla saklanması için geçerli bir sebep olmaması durumunda, o veri silinecek veya anonim hale getirilecektir. Gelecekte kullanma ihtimalinin varlığına dayanarak veri saklanamayacaktır.

Kanun, kişisel verilerin silinmesi, yok edilmesi veya anonim hale getirilmesini ayrı bir başlık altında değerlendirmiştir. Hukuka uygun olarak işlenmiş olmasına rağmen, işlenmesini gerektiren sebeplerin ortadan kalkması halinde kişisel verilerin resen veya ilgili kişinin talebi üzerine 7. madde uygulama alanı bulacaktır. 7. maddeye ilişkin usul ve esasların yönetmelikle düzenleneceği belirtilen madde üzerine, Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hala Getirilmesi Hakkında Yönetmelik yürürlüğe girmiştir[186]. İlgili Yönetmeliğin "İlkeler" başlıklı 7. maddesine göre; veri sorumlusu, ilgili Yönetmelik kapsamında yapılan tüm işlemler kayıt altına alınır ve söz konusu kayıtlar, diğer hukuki yükümlülükler hariç olmak üzere en az üç yıl süreyle saklar, uyguladığı yöntemleri açıklamakla yükümlüdür, Kurul tarafından aksine bir karar

[185] TAŞTAN, s. 52.
[186] http://www.resmigazete.gov.tr/eskiler/2017/10/20171028-10.htm, 18.12.2018.

alınmadıkça, kişisel verileri resen silme, yok etme veya anonim hale getirme yöntemlerinden uygun olanını seçer. İlgili kişinin talebi halinde uygun yöntemi gerekçesini açıklayarak seçer. Kişisel verilerin silinmesi, yok edilmesi veya anonim hale getirilmesinde Kanun'un 4. maddesindeki genel ilkeler ile kişisel veri saklama ve imha politikasına uygun hareket edilmesi gereklidir. Yönetmelik'in 4. maddesinde belirtildiği üzere; *"kişisel veri saklama ve imha politikası: veri sorumlularının, kişisel verilerin işlendikleri amaç için gerekli olan azami süreyi belirleme işlemi ile silme, yok etme ve anonim hale getirme işlemi için dayanak yaptıkları politikayı ifade etmektedir."* Yönetmelik'in 5. maddesi, *"Kanun'un 16. maddesi gereğince Veri Sorumluları Siciline kayıt olmakla yükümlü olan veri sorumlularının, kişisel veri işleme envanterine uygun olarak kişisel veri saklama ve imha politikası hazırlamakla yükümlü"* olduğunu belirtmektedir.

Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hala Getirilmesi Hakkında Yönetmeliğe göre;

Kişisel verilerin silinmesi, yok edilmesi veya anonim hale getirilmesi imha olarak adlandırılmaktadır. Yönetmelik, silme, yok etme ve anonim hale getirme hallerini ayrı maddeler altında düzenlemiştir.

Silme, kişisel verilerin ilgili kullanıcılar için hiçbir şekilde erişilemez ve tekrar kullanılamaz hale getirilmesi işlemidir (8. madde).

"Kişisel verilerin silinmesi işleminde; silinecek verilerin tespiti, her bir kişisel veri için ilgili kullanıcıların tespit edilmesi, kullanıcıların erişim yöntemlerinin tespit edilmesi, verilerin silinmesi ve ilgili kullanıcıların kişisel verilere erişiminin kaldırılması şeklinde bir süreç izlenmelidir[187]. İlgili Kullanıcı ise, Yönetmelik'in 4. maddesinde; *"Verilerin teknik olarak depolanması, korunması ve yedeklenmesinden sorumlu olan kişi ya da birim hariç olmak üzere veri sorumlusu*

[187] Kişisel Verileri Koruma Kurumu, Kişisel Verilerin Silinmesi, Yok edilmesi veya Anonim Hale Getirilmesi Rehberi, s. 6.

organizasyonu içerisinde veya veri sorumlusundan aldığı yetki ve talimat doğrultusunda kişisel verileri işleyen kişi" olarak tanımlanmıştır.

Yok edilme, kişisel verilerin hiç kimse tarafından hiçbir şekilde erişilemez, geri getirilemez ve tekrar kullanılamaz hale getirilmesi işlemidir (9. madde).

"Kişisel verilerin yok edilmesi için, verilerin bulunduğu tüm kopyaların tespit edilmesi ve verilerin bulunduğu sistemlerin türüne göre, Kurum'un "Kişisel Verilerin Silinmesi, Yok edilmesi veya Anonim Hale Getirilmesi Rehberi"nde yer alan yöntemlerden bir ya da birkaçının kullanılmasıyla tek tek yok edilmesi gereklidir"[188].

Anonim hale getirilme, kişisel verilerin başka verilerle eşleştirilse dahi hiçbir surette kimliği belirli veya belirlenebilir bir gerçek kişiyle ilişkilendirilemeyecek hale getirilmesidir (10. madde).

"Anonim hale getirmedeki amaç, veri ile bu verinin tanımladığı kişi arasındaki bağın kopartılmasıdır. Kişisel verinin tutulduğu veri kayıt sistemindeki kayıtlara uygulanan otomatik olan veya olmayan gruplama, maskeleme, türetme, genelleştirme, rastgele hale getirme gibi yöntemlerle yürütülen bağ koparma işlemlerinin hepsine anonim hale getirme yöntemleri adı verilir. Bu yöntemlerin uygulanması sonucunda elde edilen verilerin belirli bir kişiyi tanımlayamaz olması gerekmektedir"[189].

Yönetmelik, periyodik imha kavramına yer vermiştir. Bu kavram 4. maddede; *"Kanun'da yer alan kişisel verilerin işlenme şartlarının tamamının ortadan kalkması durumunda kişisel verileri saklama ve imha politikasında belirtilen ve tekrar eden aralıklarla resen gerçekleştirilecek silme, yok etme veya anonim hale getirme işlemi"* olarak tanımlanmıştır. Yönetmelik'in 11. maddesinin 2. fıkrasında

[188] Kişisel Verileri Koruma Kurumu, Kişisel Verilerin Silinmesi, Yok edilmesi veya Anonim Hale Getirilmesi Rehberi, s. 9.
[189] Kişisel Verileri Koruma Kurumu, Kişisel Verilerin Silinmesi, Yok edilmesi veya Anonim Hale Getirilmesi Rehberi, s. 16.

ise, *"Periyodik imhanın gerçekleştirileceği zaman aralığı, veri sorumlusu tarafından kişisel veri saklama ve imha politikasında belirlenir ve bu süre her halde altı ayı geçemez"* denmiştir. 3. fıkra, kişisel veri saklama ve imha politikası hazırlama yükümlülüğü olmayan veri sorumluları için *"kişisel verileri silme, yok etme veya anonim hale getirme yükümlülüğünün ortaya çıktığı tarihi takip eden üç ay içinde kişisel verilerin silinmesi, yok edilmesi veya anonim hale getirilmesi"* gerektiğini hüküm altına almıştır.

Yönetmelik, kişisel verilerin silinmesi, yok edilmesi ve anonim hale getirilmesi işlemlerinin ilgili kişinin talebi sonucu gerçekleştirilmesi durumunu ise 12. maddede düzenlemiştir. Buna göre; *"Kişisel verileri işleme şartlarının tamamı ortadan kalkmışsa; veri sorumlusu talebe konu kişisel verileri siler, yok eder veya anonim hale getirir. Veri sorumlusu, ilgili lişinin talebini en az otuz gün içinde sonuçlandırır ve ilgili kişiye bilgi verir. Kişisel verileri işleme şartlarının tamamı ortadan kalkmış ve talebe konu olan kişisel veriler üçüncü kişilere aktarılmışsa veri sorumlusu bu durumu üçüncü kişiye bildirir. Kişisel verileri işleme şartlarının tamamı ortadan kalkmamışsa, bu talep veri sorumlusunca Kanun'un 13. maddesinin 3. fıkrası uyarınca gerekçesi açıklanarak reddedilebilir ve ret cevabı ilgili kişiye en geç otuz gün içinde yazılı olarak ya da elektronik ortamda bildirilir."*

Veri sorumlusunun bu yükümlülüğü çalışmanın önceki bölümlerinde detaylı olarak anlatılan "unutulma hakkı"[190] ile de yakından alakalıdır. İlgili kişinin, artık daha fazla işlenmesinde herhangi bir yarar bulunmayan verilerinin unutulma hakkı kapsamında silinmesi, yok edilmesi ya da anonim hale getirilmesi ile bu hak kullanılabilir duruma gelecektir. Regülasyon'da yer almadan önce yasal bir düzenleme içerisinde yer almadan, mahkeme kararlarıyla ortaya çıkan ve bugünkü yasal düzenlemelerin temelleri atılan bu hak, ilgili kişilerin sahip oldukları en önemli haklardan biri olarak görülmektedir.

[190] Bkz: s. 11.

3.4.2. Veri İşleyen

Veri işleyen, Kanunun "Tanımlar" başlıklı 3. maddesinin 1. fıkrasının (ğ) bendinde, veri sorumlusunun verdiği yetkiye dayanarak onun adına kişisel verileri işleyen gerçek veya tüzel kişi olarak tanımlanmıştır. Veri işleyenin gerçekleştireceği işleme eylemlerinin hangi sınırlar içerisinde gerçekleşeceğinin belirlenmesi veri sorumlusuna aittir. Bu kapsamda veri sorumlusunun veri işleyenin sınırlarını belirlemek gibi bir yükümlülüğü olduğundan da bahsedilebilecektir[191]. Bu tanımdan da yola çıkılabileceği üzere, veri sorumlusu verileri bizzat işleme zorunluluğunda değildir. Kanun'un gerekçesi, veri işleyenin, kişisel verileri kendisine verilen talimatlar çerçevesinde işleyen çalışanlar olabileceği gibi, veri sorumlusunun hizmet satın almak suretiyle belirlediği ayrı bir gerçek veya tüzel kişi de olabileceğini belirtmiştir. Aynı anda veri sorumlusu ve veri işleyen olunabileceğini de belirten Kanun gerekçesi bu konuya örnek olarak; bir muhasebe şirketinin kendi personeliyle ilgili tuttuğu verilere ilişkin olarak veri sorumlusu sayılmasının yanı sıra, müşterisi olan şirketlere ilişkin tuttuğu veriler bakımından da veri işleyen konumunda olabileceğini belirtmiştir.

Veri işleyenin, veri sorumlusuyla arasında sözleşmesel bir ilişki kuran ayrı bir gerçek veya tüzel kişi olması durumunda bu iki kişi arasında kurulacak bir kişisel veri işleme sözleşmesi gündeme gelecektir. Kanun'un 12. maddesi veri sorumlusunu, kişisel verilerin kendisi adına başka bir veri işleyen tarafından işlenmesi halinde, kişisel verilerin hukuka aykırı olarak işlenmesini, erişilmesini önlemek ve muhafazasını sağlamak konusunda gerekli her türlü teknik ve idari tedbirlerin alınması hususunda veri işleyenlerle birlikte müştereken sorumlu tutmuştur. Veri sorumlusuna yüklenen bu müştereken sorumluluk, veri sorumlusunun, veri işleyeni hukuka ve Kanun'a uygun davranmaya teşvik etmesi

[191] Elif KÜZECİ, Veri Sorumlusunun Yükümlülükleri, 2. Kişisel Verilerin Korunması Sempozyumu Sunum Notları, İstanbul, 7 Şubat 2019, s. 2.

açısından zorlayıcı bir etki olarak değerlendirilebilir. Veri işleyenin, veri sorumlusunun bir çalışanı olması durumunda, verilerin hukuka aykırı şekilde işlenmesinden zarar gören ilgili kişi, veri sorumlusuna karşı Kanun'da sahip olduğu hakların yanı sıra TBK 66. maddede belirtilen adam çalıştıranın sorumluluğu hükümlerine de başvurabilecektir[192]. İlgili madde, *"Adam çalıştıran, çalışanın kendisine verilen işin yapılması sırasında başkalarına verdiği zararı gidermekle yükümlüdür."* demektedir. Burada önem verilmesi gereken nokta veri işleyen ve veri sorumlusu arasındaki ilişkinin çalıştırma ilişki olması yani bağımlı olarak bir çalışma ilişkisinin varlığıdır. Veri sorumlusunun, bu madde kapsamında sorumlu tutulmasının nedeni veri işleyeni seçmede, denetlemede ve talimat vermede dikkatsiz ve özensiz olması olarak gösterilebilir[193]. Aynı zamanda TBK 49. madde *"Kusurlu ve hukuka aykırı bir fiille başkasına zarar veren, bu zararı gidermekle yükümlüdür"* demektedir. Bu hüküm göz önüne alındığı takdirde de veri işleyenin kusurlu ve hukuka aykırı fiilinin varlığı halinde haksız fiillerden doğan borç ilişkileri kapsamında sorumluluğunun gündeme gelecektir.

Kanun, veri sorumlusu ile veri işleyen arasındaki hukuki ilişki konusunda, bilhassa aradaki hukuki ilişkinin niteliği ve asgari şartları hususunda, herhangi bir hüküm sevk etmemiştir. Ancak sorumluluğa dair ilgili hüküm sayesinde veri sorumlusu, Kanun'da öngörülen bütün yükümlülüklere uyması için kendi adına veri işleyen ile aralarında akdettikleri sözleşmede gerekli hükümlere yer vermelidir[194].

Veri sorumlusu, verilerin toplanmasına ilişkin uyulması gereken ilkeler, belirlenen hukuki sebep ve amaçlar, hangi verilerin işlenmesi gerekliliği, saklanma süreleri gibi konularda karar alabilecek kişi iken, veri işleyen, veri işlemede, silmede ve anonimleştirmede kullanılacak yöntemler, güvenlik önlemleri konularında karar alabilecektir. Keza Kanunun "Kabahatler" başlıklı 18.

[192] TAŞTAN, s. 72.
[193] Ahmet KILIÇOĞLU, Borçlar Hukuku Genel Hükümler (Yeni Borçlar Kanunu'na Göre Hazırlanmış), 14. Bası, Turhan Kitabevi Yayınları, Temmuz 2011, Ankara, s. 313.
[194] ÇEKİN, s. 111.

maddesinin 2. fıkrasında da belirtildiği üzere; öngörülen idari para cezaları veri sorumlusu olan gerçek kişiler ile özel hukuk tüzel kişileri hakkında uygulanacaktır, yani sorumluluk Kanun'da veri işleyene değil veri sorumlusuna yüklenmiştir. Veri işleyen, verilerin işlenmesiyle alakalı olarak yukarıda açıklanan şekilde çeşitli yükümlülükler altında olsa da Kanun kapsamında ayrı bir sorumluluk öngörülmemiştir. Kabahatler Kanunu sorumluluğu dışında, TCK kapsamında düzenlenen 135. Ve 136. maddede düzenlenen; *"kişisel verilerin kaydedilmesi, verileri hukuka aykırı olarak verme veya ele geçirme"* suçları, kanunun lafzına bakıldığında direkt olarak veri sorumlusunu işaret etmemekte, hukuka aykırı olarak kişisel verileri kaydeden kimselerin ve kişisel verileri hukuka aykırı olarak bir başkasına veren, yayan veya ele geçiren kişilerin cezalandırılacağını hüküm altına almaktadır. 138. maddede düzenlenen *"Verileri yok etmeme"* suçu ise; kanunların belirlediği sürelerin geçmiş olmasına karşın verileri sistem içinde yok etmekle yükümlü olanların cezalandırılacağını hüküm altına almıştır. Kanun'un 7. maddesi, kişisel verilerin silinmesi, yok edilmesi veya anonim hale getirilmesi yükümlülüğünü veri sorumlusuna yüklemiş olsa da veri işleyen, veri sorumlusunun verdiği yetkiye dayanarak onun adına işleme süreçlerini gerçekleştirdiğinden, sorumluluğu gündeme gelebilecektir.

3.5.Veri Sorumlusu Temsilcisi

Kanun'un Veri Sorumlusunun Aydınlatma Yükümlülüğü başlıklı 10. maddesinde, veri sorumlusunun, ilgili kişilere kimlik bilgilerini vermekle yükümlü olduğu veri sorumlusu temsilcisi, Yönetmelik'in 4. maddesinde tanımlanmıştır. Buna göre; Türkiye'de yerleşik olmayan veri sorumlularını, aşağıda belirtilen konularda asgari temsile yetkili Türkiye'de yerleşik tüzel kişi ya da T.C. vatandaşı gerçek kişi olarak tanımlanabilir.

Veri Sorumluları Sicili Hakkında Yönetmelik'in 11. maddesine göre: *"Tüzel kişilerde veri sorumlusu tüzel kişiliğin kendisidir."* Bu kısa ve yalın cümle, veri

sorumlusu, veri sorumlusu temsilcisi ve irtibat kişisinin belirlenmesinde oldukça etkili olacaktır. Veri sorumlusu temsilcisi ve irtibat kişisi'nin sorumluluklarının belirlenmesi hususunda ortaya çıkabilecek karışıklıkları gideren bu hüküm, veri sorumlusu sıfatının tüzel kişiliğin kendisinden başkasında olmayacağını belirtmektedir. Madde devamında şu ifadelere yer vermiştir: *"Türkiye'de yerleşik olan tüzel kişilerin Kanun kapsamındaki veri sorumlusu yükümlülükleri, ilgili mevzuat hükümlerine göre tüzel kişiliği temsil ve ilzama yetkili organ veya ilgili mevzuatta belirtilen kişi veya kişiler marifetiyle yerine getirilir. Tüzel kişiliği temsile yetkili organ, Kanun'un uygulanması bakımından yerine getirilecek yükümlülükler ile ilgili olarak bir veya birden fazla kişiyi görevlendirebilir."* Görüleceği üzere; Türkiye'de yerleşik bir veri sorumlusunun, Kanun'da belirlenen yükümlülükleri yerine getirmesi, temsile yetkili organ veya kişiler marifetiyle yerine getirilebilecektir. Yükümlülüklerin yerine getirilmesi hususunda görev şirketler açısından yönetim kurullarında olacaktır, yönetim kurulu belirleyeceği kişiler marifetiyle de bu yükümlülüklerin yerine getirilmesini sağlayabilir. Yönetmelik'te belirtilmemiş olsa da şirketler hukukunun genel ilkeleri ve TTK gereğince, yükümlülüklerin yerine getirilmesinde görevlendirilecek bu kişilerin görevlendirme işlemleri yönetim kurulu kararı şeklinde ve yazılı olarak yapılmalıdır[195]. Ancak burada dikkat edilmesi gereken husus, veri sorumlusunun belirleyeceği bu organ veya kişilerin, sorumluluk altına girmediği, veri sorumlusunun "yükümlülüklerini" yerine getirme görevi ile yetkilendirilebilecekleri açıkça belirtilmiş, ilgili maddenin devamında da *"Bu görevlendirme, Kanun hükümleri uyarınca tüzel kişiliğin sorumluluğunu ortadan kaldırmaz"* denilerek hüküm altına alınmıştır.

11. maddenin 2. fıkrası, *"Türkiye'de yerleşik olmayan veri sorumlusunun, veri sorumlusu temsilcisi atanmasına ilişkin yetkili organı veya kişisi tarafından alınacak kararın tasdikli örneği, kayıt başvurusu sırasında veri sorumlusu temsilcisi tarafından Kurum'a sunulur"* denilmiştir. Bir veri sorumlusunun Kanun

[195] Murat Volkan DÜLGER, Veri Sorumluları Sicili Hakkında Yönetmelik'in Getirdikleri ve Yönetmelikte Dikkat Edilmesi Gereken Hususlar, s. 9.

kapsamında veri sorumlusu olarak adlandırılması ve veri sorumlusuna yüklenen sorumlulukları yerine getirmesi için Türkiye'de yerleşik olmasına gerek yoktur. Bu gibi durumlarda, veri sorumlusu temsilcisi tanımında da açıkça belirtildiği üzere Türkiye'de yerleşik olmayan veri sorumlularının Veri Sorumluları Sicili Hakkında Yönetmelik'in 11. maddesinde belirlenen yükümlülükleri yerine getirebilmesi açısından, belirlenen konularda asgari temsille yetkilendirilen kişiler belirlenecektir. Belirlenen bu kişiler veri sorumlusu temsilcisi olarak adlandırılmakla birlikte 11. maddenin 2. fıkrası gereği, kendilerini veri sorumlusu temsilcisi olarak atayan organ veya kişilerin aldıkları kararı Kurum'a sunması gerekmektedir. İlgili kararın Kurum'a sunulmasının veri sorumlusu temsilcisi tarafından yerine getirilmesi iki şekilde değerlendirilebilir. Veri sorumlusu temsilcisinin, veri sorumlusu tarafından verilen "veri sorumlusu temsilcisi atanması karar"ını Kurum'a kendi sunması, Yönetmelik'te kendisine tanınan yetkileri aşacaktır. Bu aşamada veri sorumlusu temsilcisi atanması kararının Kurum'a veri sorumlusu tarafından sunulması daha isabetli olacaktır. Ancak ilgili kararın sunulması, veri sorumlusu temsilcisinin Kurum'a yaptığı bir "başvuru" olarak değerlendirilir ise, yetkiyi aşan bir işlemin varlığından söz edilemez. Bu kapsamda ilgili kararın kim tarafından hangi gerekçelerle Kurum'a yöneltileceği net ifadelerle belirtilmesi daha isabetli olacaktır.

Veri sorumlusu temsilcisinin temsile yetkili olduğu konular ise şu şekildedir:

- Kurum tarafından yapılan tebligat veya yazışmaları veri sorumlusu adına tebellüğ veya kabul etme
- Kurum tarafından veri sorumlusuna yöneltilen talepleri veri sorumlusuna iletme, veri sorumlusundan gelecek cevabı Kuruma iletme
- Kurul tarafından başkaca bir esasın belirlenmemiş olması halinde; ilgili kişilerin Kanunun 13. maddesinin 1. fıkrası uyarınca veri sorumlusuna yönelteceği başvuruları veri sorumlusu adına alma ve veri sorumlusuna iletme

- Kurul tarafından başkaca bir esasın belirlenmemiş olması halinde; ilgili kişilere Kanunun 13. maddesinin 3. fıkrası uyarınca veri sorumlusunun cevabını iletme
- Veri sorumlusu adına Sicile ilişkin iş ve işlemleri yapma

Görüldüğü üzere veriler üzerindeki tasarruf yetkisi halen veri sorumlusunda kalmakla birlikte veri sorumlusu temsilcisi, Kurum ve ilgili kişiler ile veri sorumlusu arasındaki iletişimi sağlamakla yetkilidir[196].

Veri sorumlusu temsilcisi ve veri sorumlusu arasındaki hukuki ilişki ise veri sorumlusunun görevlendirdiği veri sorumlusu temsilcisinin işletme içerisindeki konumuna göre de farklılık gösterebilecektir. Veri sorumlusu, veri sorumlusu temsilcisini belirlerken, bu kişiyi aynı zamanda veri sorumlusunun bir çalışanı olarak belirler ise bu durum işçi-işveren haline geleceğinden taraflar arasında bir hizmet sözleşmesi kurulması gündeme gelecektir. Veri sorumlusu, veri sorumlusu temsilcisini belirlerken, işletme dışından, aralarında herhangi bir işçi-işveren ilişkisi olmayacak şekilde bir ilişki kurulacak ise, veri sorumlusu ve veri sorumlusu temsilcisi arasındaki ilişki vekalet sözleşmesi olarak adlandırılabilecektir.

3.5.1. Veri Sorumlusu Temsilcisinin Hizmet Akdi Kapsamında Görevlendirilmesi

Hizmet sözleşmesi, TBK 393. maddesinde şu şekilde tanımlanmıştır: *"Hizmet sözleşmesi, işçinin işverene bağımlı olarak belirli veya belirli olmayan süreyle işgörmeyi ve işverenin de ona zamana veya yapılan işe göre ücret ödemeyi üstlendiği sözleşmedir."* Hizmet sözleşmesini taraflardan birinin iş gördüğü diğer sözleşmelerden ayıran en önemli etken "bağımlılık" unsurudur[197]. Bağımlılık

[196] ÇEKİN, s. 129.
[197] Sinan Sami AKKURT, Türk Özel Hukukunda İş Sözleşmesi ile Eser Sözleşmesinden Kaynaklanan Başlıca Yükümlülükler ve Anılan Sözleşmelerin Ayırt Edilmesi, 2008, s. 18-19.

unsuru, hizmet sözleşmesini diğer iş görme sözleşmelerinden ayırarak hizmetin hiyerarşi içerisinde işverene bağımlı olarak yerine getirilmesi sonucunu doğurur[198]. Veri sorumlusu temsilcisinin veri sorumlusu ile arasındaki ilişkiyi bir hizmet sözleşmesi olarak adlandırmak veri sorumlusu temsilcisinin veri sorumlusuna bağımlı olarak çalışması sonucu mümkün hale gelmektedir, aksi halde arada bağlılık unsuru olmadığında bu iki taraf arasındaki ilişkinin hizmet sözleşmesi olarak adlandırılamayacağı gündeme gelecektir.

Keza 4857 Sayılı İş Kanunu 2. maddesine göre, *"Bir iş sözleşmesine dayanarak çalışan gerçek kişiye işçi, işçi çalıştıran gerçek veya tüzel kişiye yahut tüzel kişiliği olmayan kurum ve kuruluşlara işveren"* denmektedir. Belirtildiği üzere, taraflar arasında işçi-işveren ilişkisi geçerli olduğu takdirde İş Kanunları hükümleri de gündeme gelecektir. İlgili kanunun 8. maddesi *"İş sözleşmesi, bir tarafın (işçi) bağımlı olarak iş görmeyi, diğer tarafın (işveren) da ücret ödemeyi üstlenmesinden oluşan sözleşmedir."* Demektedir. Hizmet sözleşmesini diğer iş görme sözleşmelerinden ayıran en önemli unsurun "bağımlılık" olduğu belirtilmiştir.

Hizmet sözleşmesinin hukuki niteliği gereği, tam iki tarafa borç yükleyen, belirli ya da belirsiz süreli olsa da sürekli borç ilişkisi doğuran bir sözleşme türüdür. Aynı zamanda hizmet sözleşmesi, işçinin kişiliğine bağlı bir sözleşme olarak da karşımıza çıkacaktır. İşçinin yerine getirmesi gereken edim söz konusu ilişkide "hizmet"tir ve bu hizmet işçinin kişiliğiyle yakından alakalı olabilecektir. Keza veri sorumlusu temsilcisi olarak belirlenen kişinin bu görevi bizzat yerine getirmesi gerekliliği de bu düşünceyi destekler niteliktedir. Veri sorumlusu ile arasında işçi-işveren ilişkisi bulunan herhangi bir kişi veri sorumlusu temsilcisinin görevlerini yerine getiremeyeceğinden dolayı, bu hizmetin yerine getirilmesi veri sorumlusu temsilcisi olarak atanan işçi tarafından yerine getirilmelidir.

[198] Cevdet YAVUZ, 6098 Sayılı Türk Borçlar Kanunu'na Göre Borçlar Hukuku Dersleri (Özel Hükümler), 12. Baskı, Beta Yayınevi, İstanbul, Ekim 2013, s. 452.

Hizmet sözleşmesi kapsamında işçinin bizzat çalışma borcu, özen ve sadakat borcu, teslim ve hesap verme borcu, fazla çalışma borcu ve düzenlemelere ve talimata uyma borcu TBK 395-400. maddeleri arasında düzenlenmiştir.

Veri sorumlusu temsilcisi ve veri sorumlusu arasındaki ilişkinin işçi-işveren ilişkisi olması halinde hizmet sözleşmesi uyarınca veri sorumlusu temsilcisi, Veri Sorumluları Sicili Hakkında Yönetmelik'te belirtilen işleri görebilecektir. Hizmet sözleşmesi ile çalışan bir veri sorumlusu temsilcisi, TBK 396. maddede de belirtildiği üzere: *"iş gördüğü sırada öğrendiği, özellikle üretim ve iş sırları gibi bilgileri, hizmet ilişkisinin devamı süresince kendi yararına kullanamaz veya başkalarına açıklayamaz. İşverenin haklı menfaatinin korunması için gerekli olduğu ölçüde işçi, hizmet ilişkisinin sona ermesinden sonra da sır saklamakla yükümlüdür."* Veri sorumlusu temsilcisi, Veri Sorumluları Sicili Hakkında Yönetmelik'te belirtilen yükümlülükleri yerine getirirken veri sorumlusuna ilişkin birçok bilgiye sahip olacaktır. Kanun'un ve TBK'nın ilgili maddeleri uyarınca bu bilgileri ifşa etmemek veri sorumlusu temsilcisinin bir diğer görevi olarak da karşımıza çıkacaktır. Veri sorumlusu temsilcisi, her hizmet sözleşmesinde olacağı gibi veri sorumlusuna karşı kusuruyla verdiği zararlardan sorumlu tutulacaktır, bu durum TBK 400. maddede düzenlenmiştir.

Hizmet sözleşmesi belirli süreli olarak yapılmış ise sürenin sona ermesiyle sözleşme de sona erecektir. Hizmet sözleşmesi belirsiz süreli olarak yapılmış ise TBK 431. Madde gereği *"Taraflardan her birinin, belirsiz süreli sözleşmeyi fesih sürelerine uyarak feshetme hakkı vardır".* Hizmet sözleşmeleri aynı zamanda TBK 435. maddeye göre tarafların haklı sebeplerle derhal fesih yoluna gidebileceği gibi, TBK 440. madde gereği işçinin, TBK 441. madde gereği işverenin ölümü halinde de sona erecektir. İş Kanunu kapsamında fesih ilgili maddeler kapsamında düzenlenmiştir. Bu sürelere ve usullere uyulması ile birlikte işçi ve işveren arasında gerçekleşecek bir fesih gündeme gelebilecektir.

3.5.2. Veri Sorumlusu Temsilcisinin Vekalet Akdi Kapsamında Görevlendirilmesi

Vekalet sözleşmesi de TBK'da düzenlenmiş iş görme borcunu doğuran sözleşme tiplerinden biridir. TBK 502. maddede tanımlandığı üzere, *"Vekalet sözleşmesi, vekilin vekalet verenin bir işini görmeyi veya işlemini yapmayı üstlendiği sözleşmedir. Vekalete ilişkin hükümler, niteliklerine uygun düştükleri ölçüde, bu Kanunda düzenlenmemiş olan işgörme sözleşmelerine de uygulanır. Sözleşme veya teamül varsa vekil, ücrete hak kazanır." "Vekalet sözleşmesi, vekilin sözleşme ile belirlenen iş görmeyi veya işlemi yapmayı borçlandığı ve vekilin sözleşme ile belirlenen işi görmeyi veya işlemi yapmayı borçlandığı ve vekilin yerine getireceği edimin kanun hükümleriyle düzenlenen akitlerden herhangi birinin konusuna girmediği, buna karşılık ancak sözleşme veya teamül olan durumlarda vekilin ücrete hak kazandığı bir sözleşmedir"* [199]. Aynı zamanda vekalet sözleşmesinin vekalet verenin menfaatleri ve istekleri doğrultusunda bir sonuç elde etmeye yönelik bir iş görme eylemini, zaman kaydı olmadan ve diğer sözleşme tiplerine nazaran bağımsız olması ve sonucun elde edilememesi rizikosunu ona ait olmamak üzere yüklediği bir tür sözleşme olarak da adlandırılabilir[200]. Şayet; veri sorumlusu, belirlenen görevleri yerine getirmesi için veri sorumlusu bünyesinde çalıştırmak üzere işçi-işveren ilişkisinden ayrı olarak, dışarıdan bir hizmet alacak şekilde bir veri sorumlusu temsilcisi atar ise taraflar arasındaki sözleşme hizmet sözleşmesi olarak nitelendirilmeyecek, vekalet sözleşmesi olarak adlandırılabilecektir. Yapılan iş kanunda düzenlenen başkaca bir iş görme sözleşmenin içerisine girmemiş olması veri sorumlusu ve veri sorumlusu temsilcisi arasındaki hukuki ilişkinin niteliğinin belirlenmesinde önem arz etmektedir.

Vekalet sözleşmesinde işin görülmesi bir zaman kaydına bağlı tutulmamıştır. Hizmet sözleşmesinde ise belirli ya da belirli olmayan bir zamana bağlı olarak işin

[199] YAVUZ, s. 602.
[200] YAVUZ, s. 602.

görüldüğü göz önüne alındığında hizmet ve vekalet sözleşmelerinin birbirinden ayırt edilebileceği de görülecektir. Taraflar arasındaki işçi-işveren ilişkisinin varlığı ihtimalinde de bağımsız olma konusu tartışılır hale gelecektir. Vekalet sözleşmesinde, vekilin vekalet verene karşı nisbi bir bağımsızlığının bulunduğu doktrinde kabul edilmektedir, iş görme borçlusunun bağımsızlığından söz edilemediği durumlarda vekalet sözleşmesinden değil hizmet sözleşmesinden bahsedilmesi gerekir[201] çünkü doktrin ve yargı kararlarına göre bağımlılık unsuru hizmet sözleşmesini diğer iş görme sözleşmelerinden ayıran en önemli ölçüttür[202]. Aynı zamanda, belirtildiği üzere veri sorumlusu ve veri sorumlusu temsilcisi arasındaki ilişki de söz konusu hukuki ilişkinin tespitinde yararlı olacaktır.

TBK 504. maddenin 2. fıkrasında belirtildiği üzere, "Vekalet, özellikle vekilin üstlendiği işin görülmesi için gerekli hukuki işlemlerin yapılması yetkisini de kapsar". Bu fıkra ile, vekalet sözleşmesinin beklenen şekilde ifa edilip edilmediğinin tespiti vekilden beklenen hukuki işlemlerin yapılıp yapılmadığının takibi ile kolaylaşacaktır.

Vekalet sözleşmesi kapsamında, vekilin borçları şu şekilde sayılabilir; vekalet çerçevesinde iş görme borcu, sadakat ve sır saklama borcu, hesap verme borcu ile vekalet ilişkisi dolayısıyla aldıklarını verme borcu, işi özenle yapma borcu ve işi bizzat kendisi yapma borcu[203]. Veri sorumlusu temsilcisi, bir vekalet sözleşmesi kapsamında kendinden beklenen tüm bu borçlara uygun davranma yükümlülüğü altına girerek belirlenen görevlerini bu borçlar çerçevesinde yerine getirmelidir. Tüm bu hususları vekalet sözleşmesi kapsamında yerine getirmesi kendisinden beklenecektir.

Vekalet sözleşmesi, işin görülmesi, taraflardan birinin tek taraflı iradesi ve taraflardan birinin ölümü, ehliyetsizliği ya da iflası sebebiyle sona erecektir. Veri

[201] YAVUZ, s. 611.
[202] YAVUZ, s. 452.
[203] YAVUZ, s. 622.

sorumlusu temsilcisinin yapması beklenen iş tek seferlik bir iş olmadığından, bu şekilde sona erme somut olaylarda çok fazla karşılaşılmama ihtimalini doğuracaktır. Ancak veri sorumlusu temsilcisinin, Türkiye'de yerleşik olmayan veri sorumluları için gerekli olduğu göz önüne alınırsa, ilgili veri sorumlusunun Türkiye'de yerleşik olmaya başlamasıyla birlikte işin görüldüğü varsayımıyla birlikte aradaki vekalet sözleşmesi sona ermiş olacaktır. Diğer sona erme sebepleri olan, taraflardan birinin ölümü, ehliyetsizliği ya da iflası ile alakalı olarak TBK 513. madde, *"Sözleşmeden veya işin niteliğinden aksi anlaşılmadıkça sözleşme, vekilin veya vekalet verenin ölümü, ehliyetini kaybetmesi ya da iflası ile kendiliğinden sona ermiş olur. Bu hüküm, taraflardan birinin tüzel kişi olması durumunda, bu tüzel kişiliğin sona ermesinde de uygulanır"*. Demektedir. "sözleşmeden veya işin niteliğinden aksi anlaşımadıkça" diyen ilgili madde, vekalet sözleşmesinin, taraflardan birinin ölümü, ehliyetsizliği ya da iflası ile sona ereceğine ilişkin düzenlemenin emredici bir hüküm olmadığına işaret etmektedir[204].

Temsil yetkisi, hukuk sistemimizde ise temsil olunanın temsilciye varması gerekli irade beyanına dayalı tek taraflı bir hukuki işlemdir ve temsilci tarafından kabulüne ihtiyaç duyulmamaktadır. Veri sorumlusu temsilcisi ile veri sorumlusu arasındaki hukuki ilişki hizmet sözleşmesi ya da vekalet sözleşmesi içerisine girse de içerisinde temsil yetkisini barındıran bir ilişkidir. Temsil olunan kişi, temsil yetkisini bir sözleşme ilişkisi içerisinde vermiş olabilir, bu sözleşme vekalet, hizmet, ortaklık ya da eser sözleşmesi olarak da kurulmuş olabilir[205]. Örneğin, temsil yetkisi, tek taraflı irade beyanıyla verilirken, vekalet sözleşmesinin kurulabilmesi için her iki tarafın da iradelerinin uyuşması gerekmektedir. Bu kapsamda vekalet ilişkisi içerisinde temsil yetkisini de barındırır, ancak temsil yetkisinin dayandığı ilişkinin mutlaka vekalet olmasına gerek yoktur, vekaletsiz bir temsil yetkisi de söz konusu olabilmektedir[206]. İçerisinde temsili barındıran bu

[204] YAVUZ, s. 645.
[205] KILIÇOĞLU, s. 222.
[206] ANTALYA, s. 365.

ilişki hizmet sözleşmesinden de kaynaklanan bir ilişki olabilecektir. Bu nedenle veri sorumlusu temsilcisinin, veri sorumlusuna karşı temsil yetkisine haiz olduğu, aralarındaki sözleşmenin hukuki niteliğinden bağımsız kabul edilebilecektir. Temsil olunan kişi, temsil yetkisini

Veri sorumlusu temsilcisinin yukarıda sayılan hususlarda veri sorumlusunu temsil yetkisine haiz olduğu belirtilmiştir. Bu hususta hukuki düzen içerisinde temsil konusunun yeri de bu iki taraf arasındaki ilişki bakımından değerlendirilebilir. Temsil, bir kimsenin, hüküm ve sonuçlarını başka biri üzerinde doğuracak şekilde o kişi ad ve hesabına hukuki işlem yapma yetkisi olarak adlandırılabilir[207]. Veri sorumlusu temsilcisinin veri sorumlusu üzerinde temsil yetkisini kullanmasına örnek olarak Kurum tarafından yapılan tebligatları kabul etme görevi gösterilebilir. Tüzel kişilerin temsili konusunda "organ" kurumunun hukuki niteliğiyle alakalı olarak, tüzel kişinin organlar aracılığıyla temsilini "kendine özgü yasal temsil"[208] olarak değerlendiren bir görüş olmakla birlikte, organların tüzel kişilerin temsilcisi değil, bizzat kendisi[209] olduğunu değerlendiren görüşler de yer almaktadır. Veri sorumlusu temsilcisi söz konusu olduğunda, temsil, salt irade beyanı dışında yasal olarak başka bir olguya dayandığından kanuni temsilden bahsedilecektir, bu durumda temsilci belirlenmesi hukuki düzenlemeye dayansa da temsilci veri sorumlusu tarafından belirlenecektir210. Her iki görüş için de veri sorumlusu tarafından yasal bir düzenlemeye dayalı bir atama ile görevli hale geleceğinden ve organ sıfatını taşımadığından, veri sorumlusu temsilcisinin kanuni temsil yetkisine sahip olduğu görülecektir.

Veri sorumlusu temsilcisinin yetkileri Yönetmelik'te belirlenmiştir. Bu yetkiler kapsamında, veri sorumlusu temsilcisi, yasal olarak belirlenmiş yetkiler dışında işlem yapamayacaktır.

[207] ANTALYA, s. 361.
[208] ANTALYA, s. 363.
[209] KILIÇOĞLU, s. 217.
[210] ANTALYA, s. 362.

3.6.İrtibat Kişisi

İrtibat kişisi, Kanun'da belirtilen bir kavram olarak karşımıza çıkmamaktadır. Kanun'un 31. maddesi, *"Bu Kanunun uygulanmasına ilişkin yönetmelikler Kurum tarafından yürürlüğe konulur."* Denmiştir. Kanun'un Kurul'a düzenleyici işlem yapma yetkisi verdiği konular "Kişisel Verileri Koruma Kurulu" başlığı[211] altında da sayıldığı üzere; Kurul'un görev alanı ile Kurum'un işleyişine, veri güvenliğine ilişkin yükümlülüklerin belirlenmesine ve veri sorumlusunun ve temsilcisinin görev, yetki ve sorumluluklarına ilişkin konular olarak belirlenmiştir. Bu kapsamda bir değerlendirme yapılması gerekir ise; Kurul'un yapmış olduğu düzenleyici işlemler içerisinde yer alan irtibat kişisinin, Kurul'a düzenleyici işlem yapma yetkisi tanınan konulardan sayılması gerekliliği doğacaktır.

İrtibat kişisi, Yönetmelik'in 4. maddesinde tanımlanmıştır. Buna göre; Türkiye'de yerleşik olan tüzel kişiler ile Türkiye'de yerleşik olmayan tüzel kişi veri sorumlusu temsilcisinin Kanun ve bu Kanun'a dayalı olarak çıkarılacak ikincil düzenlemeler kapsamındaki yükümlülükleriyle ilgili olarak, Kurum ile kurulacak iletişim için veri sorumlusu tarafından Sicil'e kayıt esnasında bildirilen gerçek kişiyi ifade eder. Yönetmelik'in 11. maddesinin 4. fıkrasında ise: *"Türkiye'de yerleşik olan tüzel kişiler Sicil'e kayıt sırasında irtibat kişisi bilgilerini Sicil'e işlerler."* Denmektedir. Bu iki madde arasındaki fark, Türkiye'de yerleşik olmayan tüzel kişi veri sorumlusu temsilcisinin Sicil'e kayıt esnasında bildirim yapıp yapmaması hususundadır. Türkiye'de yerleşik olmayan tüzel kişi veri sorumlusu temsilcilerinin 4. Maddeye göre irtibat kişisi bildirim yapmaları gerekirken, 11. Maddeye göre böyle bir yükümlülüklerinin olmadığı kabul edilecek, bu durum ise uygulamada farklılıklara yol açacaktır. Veri sorumlusu'nun Sicil'e kayıt yükümlülüğü kapsamında Kanun'un 18. maddesinin 1. fıkrasının ç bendi gereği Sicil'e kayıt ve bildirim yükümlülüğüne aykırı hareket edenler hakkında 20.000 TL ila 1.000.000 TL idari para cezası uygulanacaktır. Bu

[211] Bkz: s. 66.

şekilde idari para cezasına konu olan bir yükümlülüğün karşısında, Türkiye'de yerleşik olmayan bir veri sorumlusunun, veri sorumlusu temsilcisi aracılığıyla irtibat kişisinin bilgilerini Sicil'e işlememesi karşısında net bir hüküm olmaması düzenlemeler kapsamında yer alan bir eksiklik olarak değerlendirilebilir.

İrtibat kişisi, veri sorumlusunu temsile yetkili bir kişi olarak belirlenmemiş, aksine ilgili kişiler tarafından veri sorumlusuna yapılan başvurular, iletilen talepler konusunda ilgili kişi ve veri sorumlusu arasındaki iletişimin sağlanmasından sorumlu olacak şekilde konumlandırılmıştır.

Tanımda yer alan Kurum ile iletişim yükümlülüğünün dışında, Yönetmelik'in 11. maddesinin 4. fıkrasında irtibat kişisi, ilgili kişilerin veri sorumlusuna yönelteceği taleplerin cevaplandırılması konusunda da iletişimi sağlamakla yükümlüdür. İrtibat kişisinin görevlerinin belirlenmesinde de tanımında olduğu gibi, 4. madde ve 11. maddede farklılıklar olduğu görülmektedir. 4. madde, *"Kurum ile kurulacak iletişim için veri sorumlusu tarafından Sicil'e kayıt esnasında bildirilecek gerçek kişi"* olarak bir görev addetmişse de 11. madde, *"İlgili kişilerin veri sorumlusuna yönelteceği taleplerin cevaplandırılması konusunda iletişimi sağlar"* diyerek irtibat kişisine 4. maddede belirtilenden farklı bir görev yüklemiştir. İrtibat kişisinin veri sorumlusunu temsile ilişkin herhangi bir yetkisi ise bulunmamaktadır.

İrtibat kişisi de veri sorumlusu temsilcisi ve veri sorumlusu arasındaki ilişkiler doğrultusunda hizmet sözleşmesi ya da vekalet sözleşmesi gereği kendisine yüklenen görevleri yerine getirebilecektir. Taraflar arasındaki hukuki ilişkilerin niteliği Veri Sorumlusu Temsilcisi başlığı[212] altında detaylı olarak değerlendirilmiştir. Bu kapsamda taraflar arasındaki sözleşmelerin niteliği belirlenen yetkiler doğrultusunda görevlerini yerine getirmelerini engellemelidir.

[212] Bkz: s. 109.

4. VERİ SORUMLUSU TEMSİLCİSİ VE İRTİBAT KİŞİSİNİN VERİ KORUMA GÖREVLİSİ KARŞISINDAKİ KONUMU

4.1. Avrupa, AB ve Türkiye'nin Veri Koruma Hukuku'ndaki Güncel Durumu hakkında Bazı Genel Değerlendirmeler

Avrupa, kişisel verilerin korunması hususunda oldukça köklü bir geçmişe sahiptir. Avrupa'da 1950'li yıllardan itibaren kişisel verilerin korunmasına ilişkin tartışmaların yaşandığı görülmüştür. 2. Dünya Savaşı ve teknolojik gelişmelerle birlikte devlet kanalıyla toplanacak ve sistematize edilerek depolanacak verilerin, kişilerin hak ve özgürlüklerinin kısıtlanmasına yol açacağı endişesi ile Avrupa'da kişisel verilerin korunmasına ilişkin yasal düzenlemeler oluşturulmaya başlanmıştır. İlk olarak 1970 yılında Almanya'nın Hessen eyaletinde daha sonra da 1973 yılında İsveç'te hazırlanan yasal düzenlemeleri, Almanya, İrlanda, İtalya, İngiltere gibi diğer Avrupa devletleri takip etmiştir. 1995 yılında AB'nin kurulması sonrasında da bu alanda çalışmalar yoğunlaşmış, 1995 tarihinde Yönerge ve daha sonrasında da 2016 tarihinde Regülasyon'un kabul edilmiştir. Tüm bu süreç dikkate alındığında kişisel verilerin korunması hususunun anavatanının Batı Avrupa olduğu söylenebilecektir[213].

Türkiye'de ise kişisel verilerin korunması, çalışmanın önceki bölümlerinde detaylı bir şekilde aktarıldığı üzere, uzun bir geçmişe dayanmamaktadır. Türkiye, AK, BM, OECD gibi kuruluşların üyesi olmasına rağmen, bu kuruluşlarca belirlenen temel prensipleri ulusal düzenlemelerine dahil etmemiş, bu nedenle de veri koruması alanındaki gelişmelerde geride kalmıştır[214]. Avrupa ve AB'de yer alan yasal düzenlemelerden çok sonra bu alanda Türkiye'de de çalışmalar yapılmaya başlanmıştır. 2016 yılında Kanun'un kabul edilmesiyle birlikte AB de Regülasyon'u kabul etmiştir. Halbuki bakıldığında, Kanun'un Yönerge'yi temel alan bir çalışma olarak hazırlandığı görülecektir. Yönerge'nin AB üye

[213] KÜZECİ, s. 110.
[214] KÜZECİ, s. 304.

devletlerinde uygulanma şekli, çalışmanın önceki bölümlerinde detaylı olarak ele alındığı üzere; çerçeve bir düzenleme olarak adlandırılabilir. Üye devletler, bu çerçeve düzenleme kapsamında, kendi ulusal düzenlemelerini oluşturmuşlardır. Örneğin; İtalya 186, Birleşik Krallık 74, Almanya 46 maddelik ulusal yasalar düzenleyerek, Yönerge'ye uyumlu iç hukuk kuralları benimsemişlerdir[215]. Tüm bunlar dikkate alındığında, Kanun'un uygulamada belirli konularda eksiklik, belirsizlik yaşaması gündeme gelebilecekken, detaylı hükümlere yer verilmemesi de belirli alanlarda, daha sonraki süreçte düzenlemeler yapılması gerekliliğini gündeme getirebilir. Türkiye'de veri korumasına ilişkin yürürlüğe giren ilk kanunun çerçeve hükümler altında düzenlenmesi etkin bir güvence sistemi için atılmış ilk adım olarak kabul edilebilir[216].

Regülasyon, Yönergeden farklı olarak çeşitli kurumlara yer vermiş ve belirli alanlarda da daha detaylı düzenlemelere gitmiştir. Veri sorumlusunun yükümlülükleri Yönerge'ye kıyasla çok daha detaylı hale getirilmiş ve bu sorumluluklar veri işleyene de yüklenmiştir. Veri Koruma Görevlisi de, Yönerge'de yer almayan, Regülasyon ile hayata geçirilen bir kurum olarak veri koruma hukuku alanında kendine yer bulmuştur. Regülasyon yürürlüğe girmeden çeşitli çalışmalarla benzer hukuki kurumlar yer almasına karşın, yasal olarak Regülasyon'da düzenleme altına alınan bu kurum veri sorumluları için oldukça önemli bir yere sahiptir ve uygulama ile birlikte de önemi daha da ortaya çıkacaktır. Türkiye, yasal çalışmalarında Yönerge'yi temel aldığından, veri sorumlusuna yüklenen yükümlülükler, Regülasyon'da yer alan yükümlülüklere nazaran daha geniş çerçevede kalmış ve Veri Koruma Görevlisi'ne ilişkin bir düzenleme de oluşturulmamıştır. Kanun, veri sorumlusu ve veri işleyen dışında, irtibat kişisi ve veri sorumlusu temsilcisi kavramlarına yer vermiştir.

[215] KÜZECİ, s. 316.
[216] KÜZECİ, s. 317.

4.2.Veri Sorumlusu Temsilcisi ve İrtibat Kişisi'nin Veri Koruma Görevlisi Karşısındaki Konumu

Regülasyon her ne kadar belirli veri sorumluları açısından Veri Koruma Görevlisi atanmasını zorunlu kılmış olsa da isteğe bağlı olarak da veri sorumluları Veri Koruma Görevlisi atayabileceklerdir. Veri Koruma Görevlisi, bir bakımdan Regülasyon'un herhangi bir veri sorumlusu üzerindeki yansımasının oluşturulması için gerekli bir araçtır. Veri koruma hukukuna ilişkin tüm gerekliliklerin belirlenmesi, uygulanması hem hukuki hem teknik açıdan yeterli düzeyde bilgi ve tecrübeye sahip olan bu kurum ile hayata geçecektir. Veri Koruma Görevlisi Regülasyon'a uyum konusunda veri sorumluları açısından önemli bir rol oynayacaktır. Uyumluluğun sağlanması açısından, işleme faaliyetlerine katılan çalışanların bilinçlerinin artırılması adına eğitimler düzenleyerek veri sorumlusunun kendine özgü bir veri politikası ve bilinci geliştirmesini sağlayacaktır. Veri Koruma Görevlisi salt bu görevle dahi bir veri sorumlusu için hayati önem taşıyan bir kurum haline gelmektedir. İşleme kavramının, verinin elde edilmesi anından başladığı düşünüldüğünde, yasal düzenlemelere uyumluluğun, sürecin en başından itibaren uygun şekilde sağlanması gerekliliği Veri Koruma Görevlisi'nin görevlerini yerine getirmesiyle mümkündür. Yasal düzenlemelere uygunluğun dışında, veri güvenliğine ilişkin hükümlerin de uygulanması Veri Koruma Görevlisi'nin görev alanına girebilecektir. Çalışmanın önceki bölümlerinde anlatılan veri koruma etki değerlendirmesi[217] de yine Veri Koruma Görevlisi'nin tavsiyelerine uyulması gereken bir başka konudur. Veri Koruma Görevlisi, veri koruma etki değerlendirmesi için yalnızca tavsiye vermekle kalmamakta aynı zamanda da uygulanmasını takip etme yükümlülüğü altındadır. Veri Koruma Görevlisi, rutin olarak, veri sorumlusunun veri işleme faaliyetleri bakımından denetimle yükümlüdür. Ancak, rutin denetimlerin yanı sıra Çalışma Grubu, Veri Koruma Görevlisi'nin yüksek risk taşıyan konulara öncelik verilmesi gerektiğini

[217] Bkz: s. 15.

savunmuştur[218]. Tüm bu görevler dikkate alındığında, belirtildiği gibi, Veri Koruma Görevlisi, bir veri sorumlusunun, başından sonuna kadar, olması gereken veri işleme politikasının oluşmasında kilit bir rol oynamaktadır.

Türk Hukukunda ise Kanun'a uyumluluk ve çalışmanın üçüncü bölümünde detaylı olarak yer verilen tüm yükümlülüklerin[219], veri sorumlusuna yüklenmiş yükümlülükler olarak karşımıza çıkmaktadır. Ancak tüm bu yükümlülüklerin yerine getirilmesi veri sorumlusuna yüklenmişken, veri sorumlusu karmaşık organizasyon yapıları karşısında özellikle veri koruma mevzuatına uyumluluğun sağlanması noktasında profesyonel bir destek mekanizmasına muhtaçtır. Ayrıca veri sorumlusu kendi uyumluluğunu, veri işleme politikasını ve yükümlülüklerini yerine getirirken idari ve teknik tedbir alma yükümlülüğü özelinde de gerekli organizasyonu kurmakla yükümlüdür. Bu durum da veri sorumlularının, kendilerini bu yükümlülüklerin yerine getirilmesi adına görevlendireceği kişilerle mümkün olacaktır. Ancak Kanun, Regülasyon'daki gibi veri sorumlusunun tüm bu görevler için belirleyeceği kişiyi düzenlememekle birlikte, Veri Koruma Görevlisi kurumunun Kanun uyumluluğu kapsamında da benimsenebileceği ifade edilmelidir. Türk hukukuna göre veri sorumlusu belirli yükümlülükler ile görevlendirilmiş ancak tüm bu yükümlülüklerin hukuki düzene uygun ve işler halde yerine getirilmesi için belirli bir kurum öngörmemiştir. Çalışmanın önceki bölümlerinde anlatılan yer bakımından uygulama[220], Türkiye'de hizmet veren bir veri sorumlusunun, AB içerisindeki ilgili kişilerin verilerini işlediği takdirde, Regülasyon kapsamına gireceğini ve yükümlülüklere uyması gerektiğini vurgular. Böyle bir örnekte söz konusu Türk işletme, Kanun kapsamında her ne kadar Veri Koruma Görevlisi atanması gibi bir yükümlülük olmasa da AB içerisinde veri işlemesinden dolayı Regülasyon'a uyma zorunluluğu olduğundan, Veri Koruma Görevlisi ataması gerekecektir. Bu durumda, zorunlu ya da ihtiyari olarak Veri Koruma Görevlisine sahip olan bir veri sorumlusu tüm bu idari ve teknik süreçleri

[218] Art. 29 WP, s. 17.
[219] Bkz: s. 72.
[220] Bkz: s. 7.

daha kolay yürütecektir. Çalışmanın önceki bölümlerinde Veri Koruma Görevlisi[221], veri sorumlusu temsilcisi[222] ve irtibat kişisinin[223] görevleri ve yükümlülükleri anlatılmıştır. Bu kapsamda organizasyonel süreçlerin yönetilmesi konusunda veri sorumlusu temsilcisi ve irtibat kişisine verilmiş bir görev şu an için bulunmamaktadır.

Veri Koruma Görevlisi, Regülasyon kapsamında veri sorumlusunun denetim makamı ile olan iletişimini de sağlamakla görevlendirilmiştir. Aynı zamanda denetim makamı ile iş birliğini de yine Veri Koruma Görevlisi sağlayacaktır. İlgili kişiler de iletişim bilgilerinin yayınlanması ile birlikte taleplerini Veri Koruma Görevlisi'ne iletebileceklerdir. Görüleceği üzere; Veri Koruma Görevlisinin iletişim kaynağı olarak da veri sorumlusu kapsamında önemli bir konumu vardır. Veri Koruma Görevlisi'nin iletişim bilgilerinin aleni hale getirilmesi, veri sorumlusunun uyması gereken temel prensiplerden "şeffaflık ilkesi"nin sağlandığını gösterir ve ilgili kişilerin veri koruma hukuku kapsamında haklarını kullanabilmeleri açısından da kolaylık sağlar.

Kanun'da Kurum ve Kurul ile veri sorumlusunun iletişim halinde olmasına aracılık edecek iki kişi öngörülmüştür. Çalışmanın üçüncü bölümünde anlatılan bu kişiler "veri sorumlusu temsilcisi" ve "irtibat kişisi"dir. Veri sorumlusu temsilcisi; Kurum'un veri sorumlusuna yapacağı tebligat ve yazışmalarda, ileteceği talepler, ilgili kişilerin başvurularını veri sorumlusuna ve veri sorumlusunun cevaplarını ilgili kişilere iletme, sicile ilişkin işlemleri yapma görevleri ile görevlendirilmiştir. Kurum ile iletişimde net bir şekilde görevlendirilen veri sorumlusu temsilcisi, Regülasyon'da yer alan Veri Koruma Görevlisi'nin denetim makamı ile olan iletişimine benzer bir nitelik taşımaktadır. İrtibat kişisi ise; veri sorumlusunun Sicil'e kaydolurken belirleyeceği kişidir ama aynı zamanda Yönetmelik'te ilgili kişilerin veri sorumlularına yönelteceği taleplerin cevaplandırılması konusunda da

[221] Bkz: s. 31.
[222] Bkz: s. 109.
[223] Bkz: s. 119.

iletişim ile görevlendirilmiştir. Her iki kişinin görevleri değerlendirildiğinde, ilgili kişilerin veri sorumlularına iletecekleri taleplerin karşılanması konusunda birbirlerinin görevlerinin çakıştığı görülmektedir. İrtibat kişisi'nin oluşturulma amacının Sicil'de yer alması gerekliliği ve çıkarılacak ikincil düzenlemeler kapsamında veri sorumlusu ile Kurum arasındaki iletişimin sağlanması olduğu düşünüldüğünde, irtibat kişisine yüklenen ilgili kişilerle iletişim kapsamında yüklenen bu sorumluluğun yerinde olmadığı düşünülebilir. Regülasyon, irtibat kişisi kavramına yer vermemiş, aksine iletişimin sağlanması için gerekli hususları Veri Koruma Görevlisi ve atanması öngörülen hallerde atanan temsilciye bu görevleri vermiştir. Görüleceği üzere; Kanun, ilgili kişilerin iletişimi için Regülasyon'daki gibi net bir kurum belirlememiştir. İlgili kişiler taleplerini veri sorumlusu temsilcisine mi yoksa irtibat kişisine mi yönlendirecekleri konusunda net bir hüküm bulamamaktadırlar. İlgili kişiler, uygulamada direkt olarak veri sorumlusuna herhangi bir iletişim kanalıyla ulaşma yolunu seçerek bu ikilemi ortadan kaldırma yoluna gitmektedirler, bu durum da belirlenen bu iki kişinin görevlerinin etkin bir şekilde yerine getirilmesinde engel teşkil edecektir.

5. SONUÇ

Veri korumasına ilişkin günümüze dek atılan tüm adımlar, bir sonraki adım için bir katkı olarak düşünülmelidir. Veri korumasına ilişkin bu çalışmada anlatılan tüm çalışmalar ister Avrupa ülkeleri ister AB ister Türkiye'de olsun aslında tüm dünya vatandaşlarını etkisi altına alacaktır. Regülasyon ile getirilen sınır ötesi işleme kavramı da bunun bir göstergesidir. Günümüzde verinin toplanma ve işlenme alanı yalnızca ülkelerle sınırlı kalmamakta, veriler tüm dünyada hızla yayılmaktadır.

Çalışmanın önceki bölümlerinde de bahsedildiği üzere; kişisel verilerin korunması, sahip olduğumuz temel hak ve özgürlüklerimize dayanmaktadır. Özünde insan hakları ile yakından bağlantısı vardır. Her bir bireyin, kişisel

verilerinin korunmasını istemesi temel bir hak olarak düşünüldüğünde, dünya üzerindeki her bireyin de eşit haklara sahip olması gündeme gelecektir. Bu eşitliğin sağlanabilmesi adına benzer düzenlemeler üzerinden veri koruması sağlanmaya çalışılmalıdır. Çalışmanın önceki bölümlerinde detaylı olarak üzerinde durulan konulardan biri de Regülasyon ile tüm AB üye ülkelerinin aynı düzenlemeye sahip hale geldiğidir[224]. Ülkemiz de yine bir AB düzenlemesi olan Yönerge'yi temel alarak oluşturduğu Kanun ile güncel düzenlemeleri yakalamaya çalışmıştır. Ancak veri korumasına ilişkin yasal düzenlemeler yapılmasında deyim yerindeyse geç kalındığı için Kanun'da bazı eksiklikler görülmektedir. Bu eksikliklerin net bir şekilde görülebilmesi adına bu çalışmada AB kapsamında oluşturulan Regülasyon ile ülkemizde oluşturulan Kanun'un belli başlı konularda karşılaştırması yoluna gidilmiştir. Çalışmanın önceki bölümlerinde de görüleceği üzere; her iki hukuk düzeni veri sorumlularına çeşitli yükümlülükler yüklemektedir. Bu yükümlülükler, Regülasyon ve Yönerge arasındaki farklılıktan ve Kanun'un Yönerge'yi esas almasından kaynaklı olarak benzerlik gösterse de detaylandırma ve günün koşullarına uygunluğu oluşturma bakımından çeşitli farklılıklar göstermektedir. Her iki hukuk düzeninde veri sorumlusunun durumunu inceleyen bu çalışma aynı zamanda Veri Koruma Görevlisi kurumunun veri sorumlusu temsilcisi ve irtibat kişisi karşısındaki durumunu da karşılaştırmıştır. Kanun'da, Regülasyon kapsamında Veri Koruma Görevlisi gibi iletişim, organizasyonel süreçlerin oluşturulması gibi konularda yetkilendirilmiş tek bir kurum yer almamaktadır. Veri sorumlusuna yüklenen yükümlülüklerin hayata geçirilmesi konusunda yetkilendirilen bir kurumun olmaması eksikliğinin daha net bir şekilde anlatılabilmesi adına her iki hukuk düzeninde de veri sorumlularına yüklenen sorumluluklar üzerinde durulmuştur.

Veri koruma hususunda, üzerinde durulması gereken en önemli noktalar yasal düzenlemelere ve teknolojiye uyumluluktur. Veri koruması öyle bir alandır ki; teknoloji ile gelişir ve kolaylıklar sağlar, yasal düzenlemelerle kurallar altına alınır

[224] Bkz: s. 6.

ve kişileri korur. Bu nedenle bu iki ana faktörün birbiriyle uyumu oldukça önemlidir. Bu noktada Veri Koruma Görevlisi'nin görevlerinin aslında ne kadar hayati olduğu ortaya çıkmaktadır.

AB, sağlanması amaçlanan uyumun kim eliyle yapılacağını Regülasyon ile düzenleme altına almıştır. Veri Koruma Görevlisi'nin sahip olması gereken özellikleri, görevlerini hatta bağımsızlığını dahi hüküm altına alarak söz konusu uyumun sağlanmasının ne kadar önemli bir husus olduğunu gözler önüne sermiştir. Ülkemiz de bu uyumun sağlanması gerekliliğinden bahisle veri sorumlularına yükümlülükler yüklemiş ancak belirtildiği üzere; bu uyumun kimin eliyle yapılacağı konusunda açık bir kapı bırakmıştır. Çalışmanın önceki bölümlerinde anlatıldığı üzere veri sorumlusu temsilcisi e irtibat kişisi kurumları Veri Koruma Görevlisi'nin yükümlülüklerine benzer yükümlülüklerle donatılmışlarsa da bu kurumlar arasında net bir karşılaştırma yapmak çok adil olmayacaktır. Her ne kadar Veri Koruma Görevlisi, veri sorumlusu temsilcisi ve irtibat kişisinin yasal düzenlemelere uyum konusunda kişisel sorumlulukları bulunmasa da veri sorumlularının yükümlülükleri ve sorumlulukları devam etse de, benzer görevler her iki hukuk düzeninde bu kurumlara verilse de aralarında çok önemli farklılıklar da yer almaktadır. Öncelikli olarak bağımsız olma konusu ele alınabilir. Veri Koruma Görevlisi başlığında[225] detaylı olarak anlatıldığı üzere; Veri Koruma Görevlisi'nin bağımsızlığının sağlanması, kurumun görevlerini yerine getirmesi bakımından sağlanması gereken ilk şartlardandır. Veri sorumlusu temsilcisi ve irtibat kişisi için ise bağımsız olarak görev yerine getirmeden bahsedilmemekte, keza uygulama için de bu durumun gerçekleşmesi zor görünmektedir. Veri sorumlusu temsilcisi Kurum'a, irtibat kişisi ise Sicil'e bildirilmesi öngörülmüş kurumlardır. Görevleri sınırlı olarak belirlenmiş, sorumluluk almaktan çok veri sorumlusunun iletişim kanadı olarak görevlendirilmişlerdir. Bu noktada Veri Koruma Görevlisi, veri sorumlusu temsilcisi ve irtibat kişisi arasında yer alan önemli farklılıklardan bir diğeri de

[225] Bkz: s. 31.

görev tanımlarının farklılıklarıdır. Veri Koruma Görevlisi oldukça fazla görevle görevlendirilmişken, veri sorumlusu temsilcisi ve irtibat kişisi Veri Koruma Görevlisi'ne göre oldukça dar bir görev tanımıyla görevlendirilmiştir. Veri Koruma Görevlisi'nin her hukuk düzeninde gerekliliği şüphe gerektirmeyen bir gerçektir. Ancak Veri Koruma Görevlisi'nin düzenlenmesi ve yasal düzenlemelere dahil edilmesi için uygun zamanın belirlenmesi de önem arz etmektedir. Kanun, Veri Koruma Görevlisi kavramına çok yabancı olmasa da net bir hükümle var olan bir düzenleme yoktur. Ancak veri güvenliğine ilişkin yükümlülüklerin uygunluğu amacıyla gerekli denetimlerin yapılması gerekliliği gibi hükümlere dayanılarak dahi veri sorumlularının Veri Koruma Görevlisi atamaları mümkündür. Kanun kapsamında, veri sorumlularının Veri Koruma Görevlisi ataması önünde herhangi bir engel yoktur. Aksine bu şekilde yapılacak bir çalışma ile Regülasyon'a uyum konusunda da önemli bir adım atılmış sayılacaktır.

Türkiye, önceden ayrı ayrı birkaç düzenlemeye sahip olsa da veri koruma alanında Kanun ile 2016 yılında tanışmıştır. Hemen hemen herkes için yeni olan bu Kanun'a uyumun net bir şekilde gerçekleştirilmesi beklenemeyebilir. Henüz Kanun'a adapte olunmamış iken bir Veri Koruma Görevlisi'nden uyumun en üst düzeyde beklenmesi mümkün olmayabilir. Bu nedenle Kanun ile Veri Koruma Görevlisi kurumunun düzenlenmemiş olması geri dönülmez bir eksiklik olarak düşünülmemelidir. Kanun, Kanun'un yayım tarihinden önce işlenen kişisel verilerin Kanun ile uyumlu hale getirilmesi adına iki yıllık bir uyum öngörmüştür (Geçici Madde 1). İşletmelerin, kamu kurumlarının, ilgili kişilerin "veri koruması hukuku"nun ne olduğunu, neler vadettiğini, neleri kısıtladığını bilebilecek konuma gelmesi, uyumun sağlanması adına bir yetkilinin atanması sürecini de hızlandırmalıdır. AB, Veri Koruma Görevlisi atanmasını öngörerek, çalışmanın önceki bölümlerinde detaylı olarak anlatıldığı üzere; veri sorumlularının AB hukukuna uyumlu hale gelmesi konusunda yüksek derecede verimli çalışmaların gerçekleştirilmesini sağlayama yoluna gitmiştir. Ülkemizde de Kanun içerisinde düzenlenen Veri Koruma Görevlisi benzeri bir kurum, veri sorumlularının

Kanun'a uyumluluğunu hızlandırmakla kalmayacak, AB veri koruma mevzuatına da uyumluluk için sayısız fayda sağlayacaktır. Özellikle Regülasyon ile gelen sınır ötesi veri işlenmesinin hüküm altına alınması ile, veri sorumlularının Regülasyon'a uyumluluğunun da öneminin arttığı düşünüldüğünde, Veri Koruma Görevlisi'nin hayati önem taşıdığı yadsınamaz bir gerçek olarak karşımıza çıkacaktır. Tarafların Kanun'a uyumu sonrası atılacak bir sonraki adım da uyumun sürekliliğinin sağlanması olmalıdır. Günümüzde Kanun'un işlerliğini artırmak için öncelikle Veri Koruma Görevlisi kurumunun, en azından Regülasyon'da düzenlendiği gibi belirli sektörler adına zorunlu hale getirilmesi gerekmektedir. Bu gerekliliğin beraberinde Kanun'un veri sorumluları için sistematik bir halde işlemesine katkıda bulunacağı açıktır.

KAYNAKÇA

AKKURT, Sinan Sami — Türk Özel Hukukunda İş Sözleşmesi ile Eser Sözleşmesinden Kaynaklanan Başlıca Yükümlülükler ve Anılan Sözleşmelerin Ayırt Edilmesi, 2008

ANTALYA, Gökhan — Borçlar Hukuku Genel Hükümler Cilt 1., 1. Baskı, İstanbul, 2012

AŞIKOĞLU, Şehriban İpek — Avrupa Birliği ve Türk Hukukunda Kişisel Verilerin Korunması ve Büyük Veri, 1. Baskı, İstanbul, 2018

ATASOY, Kemal — Kişilik Hakkı Kapsamında Sosyal Medyada Kişisel Verilerin Korunması ve Veri Sahibinin Rızası, T.C. Marmara Üniversitesi Hukuk Araştırmaları Dergisi Prof. Dr. Cevdet Yavuz'a Armağan 1. Cilt 22 (3), İstanbul, 2016

ATİKCAN, Ece Özlem — Choosing lobbying sides: The General

CHALMERS, Adam William — Data Protection Regulation of the European Union. Journal of Public Policy, 1-22

ARTICLE 29 WORKİNG PARTY Guidelines on Data Protection Officers ("DPOs"), Adopted on 13 December 2016 As last Revised and Adopted on 5 April 2017 https://www.dsb.gv.at/documents/22758/112500/Guidelines_on_Data_Protection_Officers_(DPOs).pdf/21b32ade-ed56-4046-b555-a8a7788a2dc7

BHAIMIA, Sahar The General Data Protection Regulation: The Next Generation of EU Data Protection. Legal Information Management, 18(1), 21-28

BEYTAR, Erdi İşçinin Kişiliğinin ve Kişisel Verilerinin Korunması, 2. Baskı, İstanbul, 2018

BIEKER, Felix
FRIEDEWALD, Michael
HANSEN,Marit
OBERSTELLER,Hannah
ROST,Martin A Process for Data Protection Impact Assesment Under the European General Data Protection Regulation, Privacy Technologies and Policy,4th Annual Privacy Forum, APF 2016, Frankfurt/Main, Germany, September 7-8, 2016

CHIRICA, Simona The Main Novelties and Implications of the New General Data Protection Regulation. " Perspectives of Business Law" Journal, 2017, 6.1: 159-176.

CİVELEK, Dilek Yüksek — Kişisel Verilerin Korunması ve Bir Kurumsal Yapılanma Önerisi, Ankara, 2011

CLIZA, Marta-Claudia
SPATARU-NEGURA, Laura-Cristiana — The General Protection Regulation: What Does the Public Authorities and Bodes Need to Know and to Do. *Juridical Trib.*, 2018, 8: 489

CULIK, Nicolai
DOPKE, Christian — About Forgetting and Being Forgotten, in: ed. Thomas Hoeren/ ed. Barbara Kolany-Raiser, Big Data in Context Legal, Social and Technological Insights, Cham 2017, Springer, s. 21 – 26

ÇEKİN, Mesut Serdar — AB Hukukuyla Mukayeseli Olarak 6698 Sayılı Kişisel Verilerin Korunması Kanunu, 1. Baskı, İstanbul 2018

DEVELİOĞLU, Hüseyin Murat — 6698 sayılı Kişisel Verilerin Korunması Kanunu ile Karşılaştırmalı Olarak AB Genel Veri Koruma Tüzüğü uyarınca Kişisel Verilerin Korunması Hukuku,1. Baskı, İstanbul, Aralık 2017

DOE, Susan Practical Privacy: Report from the GDPR World. Legal Information Management, 18 (2), 76-79, 2018

DÜLGER, Murat Volkan Kişisel Verileri Koruma Kurulu'nun 2018/10 Sayılı Kararı ile Aydınlatma Yükümlülüğünün Yerine Getirilmesi Ve Veri Sorumlusuna Başvuru Konulu Tebliğlere İlişkin Değerlendirme, 2018

DÜLGER, Murat Volkan Veri Sorumluları Sicili Hakkında Yönetmelik'in Getirdikleri ve Yönetmelikte Dikkat Edilmesi Gereken Hususlar, 2018

DÜLGER, Murat Volkan Kişisel Verilerin Ceza Normlarıyla Korunması, İstanbul Medipol Üniversitesi Hukuk Fakültesi Dergisi 3 (2) Güz 2016; 101-167

DÜLGER, Murat Volkan Kişisel Verileri Koruma Kurulu'nun 2018/10 Sayılı Kararı ile Aydınlatma Yükümlüğünün Yerine Getirilmesi ve Veri Sorumlusuna Başvuru Konulu Tebliğlere İlişkin Değerlendirme, 2018

EUROPEAN DATA PROTECTION SUPERVİSOR Opinion of the European Data Protection Supervisor on the Data Protection Reform Package, March 2012

https://www.eerstekamer.nl/eu/documenteu/_opinion_of_the_european_data/f=/vixnjsqhwggb.pdf

GILBERT, Francoise European data protection 2.0: new compliance requirements in sight-what the proposed EU data protection regulation means for us companies. Santa Clara Computer & High Tech. LJ, 2011, 28: 815.

GÜRSEL, Esin
DÜĞMECİ, Fatih Yapısal Anlamda Türkiye Kişisel Verileri Koruma Kurumu'na İlişkin Bir Değerlendirme, R&S-Research Studies Anatolia Journal 1 (2), 318-329, 2018

INFORMATION COMMISSIONER'S OFFICE Guide to the General Data Protection, August 2018
https://ico.org.uk/media/for-organisations/guide-to-the-general-data-protection-regulation-gdpr-1-0.pdf

IT GOVERNANCE PRIVACY TEAM EU General Data Protection Regulation (GDPR) An Implementation and Compliance

Guide Second edition, IT Governance Publishing, İngiltere 2017

KAĞITÇIOĞLU, Mutlu Kişisel Verileri Koruma İdare Hukuku Çerçevesinden Bir Bakış, Aurum Sosyal Bilimler Dergisi 1 (2) 77-99, 2016

KARADUMAN, Ozan The General Data Protection Regulation: Achieving Compliance for EU and non-EU Companies. *Business Law International*, 2017, 18.3.

KAYA, Afra Ece Kişilik Hakkı Olarak Kişisel Veriler ve Yeni Kişisel Verilerin Korunması Kanunu, Terazi Aylık Hukuk Dergisi 12 (125), 2017

KESER, Leyla Article 29 Working Party calls fort he swift adoption of the data protection reform package, Bilişim Hukuku Günlüğü, 04.12.2013, http://www.leylakeser.org/2013/12/article-29-working-party-calls-for.html

KESER, Leyla
KAYA, Mehmet Bedii
KINIKOĞLU, Batu Türkiye'de Kişisel Verilerin Analizi (Raporun İkinci Bölümü) İstanbul Bilgi Üniversitesi, 2014

KILIÇ, Doğan Anayasal Bir Hak Olarak Kişisel Verilerin Korunması, AÜHFD 61 (3), 1089-1169, 2012

KILIÇOĞLU, Ahmet Borçlar Hukuku Genel Hükümler (Yeni Borçlar Kanunu'na Göre Hazırlanmış) 14. Baskı, Ankara, 2011

KÜZECİ, Elif Kişisel Verilerin Korunması, Yenilenmiş ve Gözden Geçirilmiş 2. Baskı, Ankara, Şubat 2018

KÜZECİ, Elif Veri Sorumlusunun Yükümlülükleri, 2. Kişisel Verilerin Korunması Sempozyumu Sunum Notları, İstanbul, 2019

KULHARI, Shraddha Building-Blocks of a Data Protection Revolution\ Baden-Baden 2018 Nomos

KİŞİSEL VERİLERİ KORUMA KURUMU 6698 Sayılı Kişisel Verilerin Korunması Kanunu'nun Uygulanmasına Yönelik Soru Cevaplar
https://www.kvkk.gov.tr/yayinlar/6698%20SAYILI%20KİŞİSEL%20VERİLERİN%20KORUNMASI%20KANUNUNUN%20UYGULANMASINA%20YÖNELİK%20SORU%20VE%20CEVAPLAR.pdf

KİŞİSEL VERİLERİ KORUMA KURUMU 6698 Sayılı Kişisel Verilerin Korunması Kanunu ve Uygulaması

http://kvkk.gov.tr/yayinlar/KİŞİSEL%20VERİLERİN%20KORUNMASI%20KANUNU%20VE%20UYGULAMASI.pdf

KİŞİSEL VERİLERİ KORUMA KURUMU — 6698 Sayılı Kişisel Verilerin Korunması Kanunu'nda Yer Alan Temel Kavramlar
https://www.kvkk.gov.tr/yayinlar/6698%20SAYILI%20KANUN'DA%20YER%20ALAN%20TEMEL%20KAVRAMLAR.pdf

KİŞİSEL VERİLERİ KORUMA KURUMU — Kişisel Verilerin Silinmesi, Yok edilmesi veya Anonim Hale Getirilmesi Rehberi
https://www.kvkk.gov.tr/yayinlar/KİŞİSEL%20VERİLERİN%20SİLİNMESİ,%20YOK%20EDİLMESİ%20VEYA%20ANONİM%20HALE%20GETİRİLMESİ%20REHBERİ.pdf

KİŞİSEL VERİLERİ KORUMA KURUMU — Kişisel Veri Güvenliği Rehberi (Teknik ve İdari Tedbirler)
https://kvkk.gov.tr/SharedFolderServer/CMSFiles/7512d0d4-f345-41cb-bc5b-8d5cf125e3a1.pdf

LAMBERT, Paul — The Data Protection Officer Profession Rules and Role, CRC Press, 2016

NICOLAIDOU, Irene Loizidou
GEORGIADES, Constantinos — "The GDPR: New Horizons, EU Internet Law Regulation And Enforcement", Cham, Switzerland, January 2017

ÖZBEK, Veli Özer
KANBUR, Mehmet Nihat
DOĞAN, Koray
BACAKSIZ, Pınar
TEPE, İlker
Türk Ceza Hukuku Özel Hükümler, 6. Baskı, Ankara, 2014

RECIO, Miguel
Data Protection Officer: The Key Figure to Ensure Data Protection and Accountability. *Eur. Data Prot. L. Rev.*, 2017, 3: 114.

SOYASLAN, Doğan
Ceza Hukuku Özel Hükümler,8. Baskı, Ankara, 2010

TAŞTAN, Furkan Güven
Türk Sözleşme Hukukunda Kişisel Verilerin Korunması 2. Baskı, İstanbul 2017

YILMAZ, Sabire Sanem
Tıp Alanında Kişisel Verilerin Açıklanması Suçu, Terazi Aylık Hukuk Dergisi 11 (119), 2016

YAVUZ, Cevdet
6098 Sayılı Türk Borçlar Kanunu'na Göre Borçlar Hukuku Dersleri (Özel Hükümler), 12. Baskı, İstanbul, 2013

https://www.jdsupra.com/legalnews/austrian-data-protection-authority-45800/

https://www.insideprivacy.com/eu-data-protection/italian-court-decides-that-a-data-protection-officer-does-not-have-to-be-a-certified-iso-27001-auditor/

https://www.giustiziaamministrativa.it/cdsintra/cdsintra/AmministrazionePortale/DocumentViewer/index.html?ddocname=5LLMWH2MBE2JVPC536FUMJHNYU&q

https://www.tbmm.gov.tr/sirasayi/donem26/yil01/ss117.pdf

https://www.kvkk.gov.tr/Icerik/2032/Veri-Sorumlusu-Kimdir

https://www.kvkk.gov.tr/Icerik/5273/Istisna

http://www.resmigazete.gov.tr/eskiler/2017/10/20171028-10.htm

https://verbis.kvkk.gov.tr