T.C.
İSTANBUL MEDİPOL ÜNİVERSİTESİ
SOSYAL BİLİMLER ENSTİTÜSÜ
YÜKSEK LİSANS TEZİ

VERİ KORUMA GÖREVLİSİ

Gamze Nur KESKİNKILIÇ

ÖZEL HUKUK YÜKSEK LİSANS PROGRAMI

DANIŞMAN
Doç. Dr. Harun DEMİRBAŞ

İSTANBUL – 2021

İÇİNDEKİLER

KISALTMALAR

AB : Avrupa Birliği

ABD **:** Amerika Birleşik Devletleri

AİHM **:** Avrupa İnsan Hakları Mahkemesi

AİHS **:** Avrupa İnsan Hakları Sözleşmesi

bkz. **:** bakınız

C. **:** Cilt

CNIL **:**Commission Nationale de l'Informatique et des Libertés (France)

DPO **:** Data Protection Officer

EDPB **:** European Data Protection Board

EDPS **:** European Data Protection Supervisor

f. **:** fıkra

GDPR **:** General Data Protection Regulation

IAPP **:** International Association of Privacy Professionals

ICO **:** Information Commissioner's Office

ISO **:** International Standards Organization

KURUL **:** Kişisel Verileri Koruma Kurulu

KURUM **:** Kişisel Verileri Koruma Kurumu

KVKKT **:** Kişisel Verilerin Korunması Kanun Tasarısı

m. **:** madde

OECD **:** The Organisation for Economic Co-operation and Development

OEEC **:** The Organisation for European Economic Co-operation

par. **:** paragraf

s.	**:** sayfa
S.	**:** Sayı
TBK	**:** 6098 sayılı Türk Borçlar Kanunu
TCK	**:** 2537 sayılı Türk Ceza Kanunu
TDK	**:** Türk Dil Kurumu
TMK	**:** 4721 sayılı Türk Medeni Kanunu
Tüzük	**:** Regulation 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC
vd.	**:** ve devamı
Yönerge	**:** Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the Protection of Individuals with egard to the Processing of Personal Data and on the Free Movement of Such Data

ÖZET

Bilgi ve iletişim teknolojilerindeki gelişmeler kişisel verilerin korunmasına duyulan ihtiyacın artmasına sebep olmuş ve bu durum mevcut veri koruma kurallarının güncellenmesini ve veri koruma hukukunda birtakım yenilikler yapılmasını zorunlu kılmıştır. Bu ihtiyacın sonucu olarak Avrupa Birliği Genel Veri Koruma Tüzüğü kabul edilmiş ve bu yasal düzenleme ile birtakım yenilikler veri koruma hukukunda yer edinmiştir. Tüzük ile veri koruma hukukunda yer verilen kavramlardan birisi de Tüzük'te "Data Protection Officer" (DPO) olarak anılan "Veri Koruma Görevlisi" dir.

Bu çalışma kapsamında Avrupa Birliği mevzuatında yer alan ancak henüz ülkemiz veri koruma mevzuatında hakkında açık bir düzenleme bulunmayan ve veri koruma aktörlerinden biri olan "Veri Koruma Görevlisi" incelenmiş ve Türkiye'de "Veri Koruma Görevlisi" kurumuna ilişkin yapılacak muhtemel düzenlemelere ilişkin değerlendirmelerde bulunulmuştur. Çalışma üç ana bölümden oluşmaktadır. İlk bölümde, kişisel verilere ilişkin temel kavramlara, kişisel verilerin hukuki niteliğine ve kişisel verilerin korunması alanındaki ulusal ve uluslararası düzenlemelere yer verilmiştir. İkinci bölümde ise veri koruma hukukuna ilişkin temel ilkeler ile özellikle hesap verilebilirlik ilkesi çerçevesinde uyumluluğu artırmaya ilişkin kurallar incelenmiştir. Üçüncü ve son bölümde, veri koruma görevlisinin belirlenmesi, konumu ve görevleri açıklanmış; Türkiye'deki veri koruma hukuku düzenlemeleri açısından veri koruma görevlisi değerlendirilmiştir.

Anahtar Kelimeler: Veri Koruma Görevlisi, Hesap Verilebilirlik, Risk Temelli Yaklaşım, Teknik ve İdari Tedbirler, Uyumluluğu Artırmaya İlişkin Kurallar

ABSTRACT

Developments in information and communication technologies caused an increase in the need of protection of personal data. This situation required an update in current data protection rules and some reforms in data protection law. As a result, General Data Protection Regulation (Regulation) is enacted; and with this regulation some reforms entered in data protection law. Data Protection Officer (DPO) is one of the terms mentioned in the Regulation regarding data protection law.

This thesis examines one of the data protection actors which is mentioned in the EU legislation which is not yet regulated in our country the 'Data Protection Officer'. Writer evaluates prospective legal regulations related to 'Data Protection Officer' in Turkish law. This thesis comprises of three main chapters. Under the first chapter, writer aims to evaluate fundamental terms, legal nature and characteristic of personal data followed by comparison of national and international regulations. Under the second chapter, fundamental concepts of data protection law and rules on promoting compliance within the scope of accountability principle are specifically analysed. The third and final section, examines designation process, position and tasks of data protection officer. Also this chapter evaluates data protection officer in regards to data protection regulations in Turkey.

Keywords: Data Protection Officer (DPO), Accountability Principle, Risk Based Approach, Technical and Organisational Measures, Rules on Promoting Compliance

GİRİŞ

Kişisel verilerin korunması, her ne kadar ülkemizde son yıllarda tartışılmaya başlanmış ve veri koruma hukukuna ilişkin yasal düzenlemeler son yıllarda ulusal mevzuatımızda yer edinmiş olsa da bilgi ve iletişim teknolojilerindeki büyüme ve gelişmeye paralel olarak uluslararası alanda uzun yıllardır tartışılmaktadır ve uluslararası hukuk metinlerine konu edilmiştir. 1970'li yıllardan günümüze, özellikle Avrupa Birliği'nde olmak üzere, veri koruma alanında pek çok yasal düzenleme yapılmış; ancak teknolojideki gelişmeler ile kişisel verilerin elektronik ortamda toplanması ve aktarımının kolaylaşması kişisel verilere ve mahremiyete yönelik tehditlerin artmasına sebep olmuştur. Avrupa Birliği Genel Veri Koruma Tüzüğü, gelişen teknoloji dikkate alınarak bu tehditleri bertaraf etmek amacıyla hazırlanmış ve 2016'da kabul edilmiş; veri koruma hukuku alanında en kapsamlı ve güncel yasal metindir. Muhakkak ki gelecek yıllarda yeni teknoloji faaliyetlerine bağlı olarak veri koruma alanında yeni düzenlemeler yapma ihtiyacı duyulacak ve Tüzük'ün de güncellenmesi gündeme gelecektir.

Tüzük ile unutulma hakkı, tasarımla veri korunması, varsayılan ayarlarla veri korunması, veri koruma etki değerlendirmesi, veri koruma görevlisi gibi birçok yeni kavram veri koruma hukukuna dâhil edilmiştir. Veri koruma hukukunun belirli tanımlamaları AB Genel Veri Koruma Tüzüğü ile geliştirilmiş ve kişisel verilerin korunmasına duyulan ihtiyacın artmasına bağlı olarak kapsamı genişletilmiştir. Tüzük ile kabul edilen en önemli yeniliklerden birisi de veri sorumlusu ve veri işleyen açısından yaptırıma dayalı bir anlayış yerine riskleri tespit ederek kendisini denetleme yükümlülüğü getirilmiş olmasıdır.

Veri sorumlusu ve veri işleyen, veri koruma ilkelerine uygun şekilde veri işleme faaliyetinde bulunmalı, mevcut ve olası riskler gözetmeli ve bu kapsamda gerekli teknik ve idari tedbirler almalıdır. Bu çerçevede risk temelli yaklaşım ile kendilerini denetleme, veri koruma ilkelerine uyma, bu konuda gerekli teknik ve idari tedbirleri alma ve bu ilkelere uyulduğunun kanıtlanması yükümlülüğünün bir sonucu olarak belirli veri sorumluları ve veri işleyenler hakkında veri koruma görevlisi belirleme yükümlülüğü kabul edilmiştir. Çalışmamızın konusunu oluşturan "Veri Koruma

Görevlisi", veri sorumlusu ve veri işleyenin kişisel verilerin korunmasına ilişkin hukuki düzenlemelere uyumluluğunun sağlanmasında ve yeni veri koruma rejiminin anlaşılmasında ve uygulanmasında aktif rol alacak veri koruma aktörleridir. Bu çerçevede belirtmek gerekir ki veri koruma görevlisi, veri koruma ilkelerinden hesap verilebilirlik ilkesinin bir sonucu ve bu doğrultuda uyumluluğu artırmaya ilişkin kurallardan birisi olarak karşımıza çıkmaktadır.

Çalışmamızda öncelikle kişisel verilerin korunması hukukuna ilişkin temel kavramlar açıklanacak ve kişisel verilerin korunmasının tarihçesi anlatılacaktır. Ardından veri koruma hukukunun temel ilkeleri ve özellikle Tüzük'te yer verilen hesap verilebilirlik ilkesi açıklanacaktır. Burada belirtmek gerekir ki daha güncel olması ve ülkemiz kişisel verilerin korunması hukukunda kabul edilen 6698 sayılı Kişisel Verilerin Korunması Kanunu'nda yer alan ilkeleri de kapsıyor olması sebebiyle Tüzük'te yer verilen ilkeler açıklanmış; ancak bu ilkelerin 6698 sayılı Kanun'daki görünümleri de ifade edilmiştir. Tüzük'ün getirmiş olduğu sorumluluk rejimi olan risk temelli yaklaşım ile hesap verilebilirlik ilkesinin bağlantısı incelenecek ve hesap verilebilirlik ilkesinin bir gereği olarak veri sorumlusu ve veri işleyen açısından alınması gereken teknik ve idari tedbirler ile uyumluluğu artırmaya ilişkin kurallara yer verilecektir. Hesap verilebilirlik ilkesinin ve bu doğrultuda uyumluluğu artırmaya ilişkin kuralların belirtilmesinin akabinde; uyumluluğu artırmaya ilişkin kurallardan biri olarak karşımıza çıkan "Veri Koruma Görevlisi" açıklanacaktır. Tüzük m.37-39 hükümlerinde yer verilen veri koruma görevlisi, Tüzük'ün düzenlemesine paralel olarak sırasıyla; "Veri Koruma Görevlisinin Belirlenmesi", "Veri Koruma Görevlisinin Konumu" ve "Veri Koruma Görevlisinin Görevleri" olmak üzere üç ana başlık altında anlatılacak ve nihayet Türkiye'deki mevcut ve olası veri koruma hukuku düzenlemeleri açısından veri koruma görevlisi kurumuna ilişkin değerlendirmede bulunulacaktır.

BİRİNCİ BÖLÜM: KİŞİSEL VERİLERE İLİŞKİN TEMEL KAVRAMLAR, KİŞİSEL VERİLERİN HUKUKİ NİTELİĞİ VE TARİHSEL SÜRECİ

1.1. KİŞİSEL VERİLERE İLİŞKİN TEMEL KAVRAMLAR

1.1.1. Kişisel Veri Kavramı ve Unsurları

Kişisel veri kavramı, ulusal ve uluslararası[1] pek çok normatif metinde yer alan genel tanımıyla kimliği belirli veya belirlenebilir olmak şartıyla kişiye ilişkin her türlü bilgiyi ifade etmektedir. Ülkemizde 7 Nisan 2016 tarihinde yürürlüğe giren 6698 sayılı Kişisel Verilerin Korunması Kanunu'nun m.3/f.1 (d) bendi hükmünde uluslararası normatif metinlerle örtüşür şekilde *"kimliği belirli veya belirlenebilir gerçek kişiye ilişkin her türlü bilgi"* olarak tanımlanmıştır[2]. Kanun tanımında oldukça genel bir

[1] OECD'nin 23 Eylül 1980 yılında yayınlamış olduğu Özel Yaşamın Korunması ve Kişisel Verilerin Sınır Ötesi Akışına İlişkin Rehber İlkeleri'nin 1(b) maddesinde *''Kimliği belirli veya belirlenebilir bir gerçek kişi hakkındaki tüm bilgileri ifade eder''* şeklinde tanımlanmıştır, bkz. OECD, **"Guidelines on the Protection of Privacy and Transborder Flows of Personal Data",** (Bundan sonra "OECD Rehber İlkeler" olarak anılacaktır.), http://www.oecd.org/internet/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm (Erişim:24.03.2020); 108 sayılı Kişisel Verilerin Otomatik İşleme Tabi Tutulması Karşısında Bireylerin Korunması Sözleşmesi'nin 2(a) maddesinde *''Kimliği belirli veya belirlenebilir bir gerçek kişi hakkındaki tüm bilgileri ifade eder''* şeklinde tanımlanmıştır, bkz. Avrupa Konseyi, **"Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data",** (Bundan sonra "108 Sayılı Sözleşme" olarak anılacaktır.), https://www.coe.int/en/web/conventions/full-list/-/conventions/rms/0900001680078b37, Türkçe metni için bkz. https://www.resmigazete.gov.tr/eskiler/2016/03/20160317-2.pdf (Erişim:24.03.2020); Avrupa Birliği 95/46/EC sayılı Kişisel Verilerin İşlenmesi ve Serbest Dolaşımına İlişkin Yönerge'nin 2(a) maddesinde *"Kişisel veri fiziksel, fizyolojik, zihinsel, ekonomik, kültürel veya sosyal kimliğine özel bir veya daha fazla faktöre veya bir kimlik numarasına atıf başta olmak üzere doğrudan veya dolaylı olarak tespit edilebilen bir tespit edilebilir kişi; tespit edilmiş veya tespit edilebilir gerçek kişiye (veri öznesi) ilişkin herhangi bir bilgiyi kastedecektir"* şeklinde tanımlanmıştır, bkz. **"Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data",** (Bundan sonra "Yönerge" olarak anılacaktır.) https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:31995L0046 (Erişim:24.03.2020).

[2] 6698 sayılı Kişisel Verilerin Korunması Kanunu, RG. 07.04.2016 T., 29677 S., (Bundan sonra "Kanun" olarak anılacaktır.), Kanun metni için bkz. https://www.mevzuat.gov.tr/MevzuatMetin/1.5.6698.pdf (Erişim:24.03.2020); Kişisel Verileri Koruma Kurumu, **"6698 Sayılı Kanun'da Yer Alan Temel Kavramlar"**, Ankara, 2017, s. 9 (Çevrimiçi) https://www.kvkk.gov.tr/SharedFolderServer/CMSFiles/45af208d-3718-49ed-b51a-9be9edde6ff2.pdf (Erişim:24.03.2020).

ifadeye yer verilmiş olup bir bireyin, diğer bireylerden ayırt edilmesine yardımcı olacak her türlü bilginin kişisel veri kapsamında olduğu söylenebilir. Kanun'un gerekçesine bakıldığı zaman sadece bireyin adı, soyadı, doğum tarihi ve doğum yeri gibi onun kesin teşhisini sağlayan bilgilerin değil; aynı zamanda kişinin fiziki, ailevi, ekonomik, sosyal ve sair özelliklerine ilişkin bilgilerin de kişisel veri olduğu belirtilmiştir[3]. Gerek Kanun'da gerek gerekçesinde hangi verilerin kişisel veri olduğu tahdidi olarak tanımı sınırlandırıcı mahiyette sayılmamış olup kavramın çok geniş bir tanıma karşılık geldiği ve gelişen teknoloji ile yeni veri kategorilerinin de oluşabileceği düşünüldüğünde, tanımın genel nitelikli olmasının isabetli olduğu söylenebilir[4].

Avrupa Birliği Genel Veri Koruma Tüzüğü'nün (GDPR)[5] *"Tanımlar"* başlıklı m.4/f.1 hükmünde ise Yönerge'den ve Kanun'dan daha geniş bir tanıma yer verilmek suretiyle kişisel veri *"belirli veya belirlenebilir bir gerçek kişiye ilişkin her türlü bilgi"* olarak tanımlanmıştır. Tüzük, madde metninin devamında gerçek kişinin özellikle isim, kimlik numarası, konum verileri, çevrim içi tanımlayıcı ya da söz konusu gerçek

---

[3] Kişisel Verilerin Korunması Kanunu Tasarısı (1/541) ve Adalet Komisyonu Raporu, tam metin için bkz. https://www.tbmm.gov.tr/sirasayi/donem26/yil01/ss117.pdf (Erişim:24.03.2020).

[4] İçtihat metinlerine bakıldığı zaman Anayasa Mahkemesi'nin 19.03.2015 T. 2014/180 E. 1025/30 K. sayılı kararında kişisel veri *"Kişisel veri kavramı, belirli veya kimliği belirlenebilir olmak şartıyla, bir kişiye ilişkin bütün bilgileri ifade etmektedir. Bu bağlamda adı, soyadı, doğum tarihi ve doğum yeri gibi bireyin sadece kimliğini ortaya koyan bilgiler değil; telefon numarası, motorlu taşıt plakası, sosyal güvenlik numarası, pasaport numarası, özgeçmiş, resim, görüntü ve ses kayıtları, parmak izleri, genetik bilgiler, IP adresi, e-posta adresi, hobiler, tercihler, etkileşimde bulunulan kişiler, grup üyelikleri, aile bilgileri gibi kişiyi doğrudan veya dolaylı olarak belirlenebilir kılan tüm veriler kişisel veri kapsamındadır."* şeklinde tanımlanmıştır. Karar için bkz. https://www.resmigazete.gov.tr/eskiler/2015/04/20150403-8.pdf (Erişim:24.03.2020); Yargıtay Hukuk Genel Kurulu'nun 17.06.2015 T. 2014/4-56 E. 2016/1679 K. sayılı kararında kişisel veri *"Hemen ifade edilmesi gerekir ki kişisel verinin sayısal olarak sınırlandırılması mümkün değildir. Ancak içtihatlar ve akademik yayınlar dikkate alındığında bireyin kimliğini ortaya çıkartan, bir kişiyi belirli kılan ve karakterize eden kişinin kimlik, ekonomik ve dijital bilgileri, tabiiyeti, kanaatleri, ırk, siyasî düşünce, felsefî inanç, din, mezhep veya diğer inançları, dernek, vakıf ve sendika üyeliği, sağlık bilgileri, fotoğrafları, parmak izi, sağlık verileri, telefon mesajları, telefon rehberi, sosyal paylaşım sitelerinde yazdığı veya paylaştığı yazı, fotoğraf, ses veya görüntü kayıtları kişisel verileri olarak kabul edilebilir."* şeklinde tanımlanmıştır. Karar için bkz. www.kazanci.com (Erişim:24.03.2020).

[5] "**Regulation (Eu) 2016/679 Of The European Parliament And Of The Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)",** Official Journal of the European Union, 4 Mayıs 2016 (Bundan sonra "Tüzük" olarak anılacaktır.) Tüzük metni için bkz. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679, Türkçe metni için bkz. https://www.kisiselverilerinkorunmasi.org/wp-content/uploads/2017/09/GDPR T%C3%BCrk%C3%A7e-%C3%87eviri-AB-Bakanl%C4%B1%C4%9F%C4%B1.pdf (Erişim:24.03.2020).

kişinin fiziksel, fizyolojik, genetik, ruhsal, ekonomik, kültürel veya toplumsal kimliğine özgü bir ya da daha fazla sayıda faktöre atıfta bulunularak doğrudan veya dolaylı olarak ilgili kişinin tanımlanmasına olanak sağlayan verilerin kişisel veri olduğunu belirtmiştir. Tüzük metninde konum verilerine, çevrimiçi tanımlayıcılara, genetik kimlik verilerine yer verilmiş olması Tüzük'ün güncel gelişmeler dikkate alınarak hazırlanan son metin olduğuna da işaret etmektedir. Ancak bahsedildiği üzere gelişen teknoloji ile yeni veri kategorilerinin oluşacağı düşünüldüğünde günümüz normatif metinlerinin de güncellenmesi kaçınılmaz olacaktır.

Gerek Kanun'un gerekçesinde gerek Tüzük ve Yönerge'de kişisel veri tanımı yapıldıktan sonra veri ve kişiyi belirlemeye yönelik birtakım faktörler sayılmış olup bu sayımın tahdidi olmadığını belirtmek gerekir. Yüksek Mahkeme kararlarında ve doktrinde kişisel verilere ilişkin örnekler çoğaltılmakta olup bu anlamda; parmak izi, kan grubu, yaş, boy, kilo, doğum tarihi, sosyal/ekonomik durum, görsel-işitsel kayıtlar, araç plakası, vergi beyannamesi, vergi numarası, banka hesap numarası, kredi kartı bilgileri, kredi kartı ekstreleri, MOBESE kayıtları, IP adresi gibi bir kimseye ilişkin çeşitli bilgiler içeren verilerin kişisel veri niteliğinde olduğu belirtilmektedir[6].

Uluslararası normatif metinlerde kişisel veriye ilişkin geniş kapsamlı tanımlara yer verilmiş olması, ülkeler arasında kişisel veri kavramı ile ilgili bazı belirsizliklerin ve farklılıkların oluşmasına sebebiyet vermiştir. Bu nedenle, Yönerge'nin 29. maddesi kapsamında kurulmuş olan Article 29 Working Party[7] tarafından 20 Haziran 2017 tarihinde kişisel veri kavramı hakkında görüş metni[8] kabul edilmiş ve bu metin ile belirsizlik ve farklılıkların bertaraf edilerek ortak bir anlayış oluşturulması ve kavramın sınırlarının belirlenmesi hedeflenmiştir.

---

[6] Mesut Serdar ÇEKİN, **Avrupa Birliği Hukukuyla Mukayeseli Olarak 6698 Sayılı Kanun Çerçevesinde Kişisel Verilerin Korunması Hukuku**, 3.Baskı, İstanbul, 2020, s. 47; Metin TURAN, **Karşılaştırmalı Hukukta Kişisel Verilerin Korunması,** 2.Baskı, Ankara, 2019, s. 57.

[7] Article 29 Working Party 95/46/EC sayılı Yönerge'nin 29. maddesi kapsamında kurulmuş, kişisel veriler alanında çalışmalar yapan Avrupa Birliği bağımsız danışma organıdır. 25 Mayıs 2018 tarihinde Avrupa Birliği Genel Veri Koruma Tüzüğü'ünün (GDPR) yürürlüğü girmesiyle Article 29 Working Party'nin yerini Avrupa Veri Koruma Kurulu (European Data Protection Board/EDPB) almıştır.

[8] Article 29 Working Party, **"Opinion 4/2007 on the Concept of Personal Data"**, WP136, 20 Haziran 2007, https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2007/wp136_en.pdf (Erişim:24.03.2020).

Yasal düzenlemelerde birbirine paralel biçimde kişisel veri kavramının bilgi, bilginin kişiye ilişkin olması ve belirli veya belirlenebilir gerçek kişi olmak üzere üç temel unsurdan oluştuğu söylenebilir[9].

1.1.1.1. Bilgi

Kişisel veri kavramının temel unsurlarından biri, belirli veya belirlenebilir olmak şartıyla kişiye ilişkin her türlü bilgidir. Gerek Avrupa Birliği mevzuatında gerek 6698 sayılı Kanun'da kişisel verinin tanımında kullanılan ve Article 29 Working Party'nin hazırladığı görüş metninde ilk açıklanan unsur bilgidir. Burada bilgi unsuruna ilişkin açıklama yapmadan önce farklı anlamlara sahip olmakla beraber kişisel verileri koruma alanında sıkça birbirinin yerine kullanılan bilgi (information) ve veri (data) kavramları arasındaki ilişki ve farklılığı anlamak adına bu kavramların açıklanması gerekir.

Veri, *"bilgi işleme sürecinin temel hammaddesi olarak ve çeşitli sembol, harf, rakam ve işaretlerle temsil edilen, ham, işlenmeye hazır işlenmemiş gerçekler ya da izlenimler"*[10] olarak tanımlanmaktadır veya TDK'daki tanımı ile veri, *"olgu, kavram ya da komutların, iletişim, yorum ve işlem için elverişli biçimsel ve uzlaşımsal bir gösterimi"*[11] ifade etmektedir. Bilgi ise *"verilerin, karar alma sürecine destek sunacak şekilde anlamlı bir biçime getirilmek üzere, analiz edilerek işlenmesiyle ulaşılan sonuçlar"*[12] olarak tanımlanmaktadır veya TDK'daki anlamı ile *"kurallardan yararlanarak kişinin veriye yönelttiği anlamı"*[13] ifade etmektedir[14]. Veri kavramı, genellikle bilgisayar sistemi tarafından üzerinde işlem yapılabilen her türlü değeri

[9] Article 29 Working Party tarafından kişisel veri kavramının unsurları 4 başlık altında açıklanmış olup bunlar; herhangi bir bilgi, bilginin bir kişiye ilişkin olması, belirli veya belirlenebilir kişi ve gerçek kişidir. bkz. Art. 29 Working Party, WP136, s. 6.

[10] Türksel Kaya BENGSHIR, **Bilgi Teknolojileri ve Örgütsel Değişim**, Türkiye ve Ortadoğu Amme İdaresi Enstitüsü, Ankara, 1996, s. 14; Hüseyin Can AKSOY, **Medeni Hukuk ve Özellikle Kişilik Hakkı Yönünden Kişisel Verilerin Korunması**, Ankara, 2010, s. 11.

[11] Türk Dil Kurumu (TDK), Güncel Türkçe Sözlük için bkz. https://sozluk.gov.tr/ (Erişim:26.03.2020).

[12] AKSOY, s.11; BENGSHIR, s. 14.

[13] Türk Dil Kurumu(TDK), Güncel Türkçe Sözlük için bkz. https://sozluk.gov.tr/ (Erişim:26.03.2020).

[14] 5651 sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun'un *"Tanımlar"* başlıklı 2. maddesinde bilgi *"Verilerin anlam kazanmış biçimi"*, veri ise *"Bilgisayar tarafından üzerinde işlem yapılabilen her türlü değer."* olarak tanımlanmıştır. Kanun metni için bkz. https://www.mevzuat.gov.tr/MevzuatMetin/1.5.5651.pdf (Erişim:26.03.2020).

veya elektronik olarak depolanmış işaretleri nitelendirmek için kullanılsa da verinin yalnızca bilgisayar sistemine veya elektronik sisteme has bir kavram olarak anlaşılması kişisel verilerin korunma alanını daraltacaktır ve kişisel verilerin korunması hukukunun amacına uymayan hukuksal sonuçlara sebep olacaktır[15]. Bu sebeple veri kavramının kişisel verilerin korunması alanında yalnızca bilgisayar verisi veya elektronik veri olarak anlaşılmaması gerekir. Dolayısıyla yapılan tanımlamalara göre verinin anlam bulmuş hâlinin bilgi olduğu ve içeriğinden bağımsız olarak bir kişiye ilişkin her türlü bilginin kişisel veri olduğu söylenebilir[16]. Yine bu bağlamda veri, bilginin belirlenmiş veya belirlenebilir bir kişiye ait olması durumunda kişisel kabul edilir[17].

Kişisel veri kavramı bir kişiye ilişkin her türlü bilgiyi içerdiğinden, bilginin kişisel veri olarak kabul edilip edilmemesi bakımından öznel veya nesnel niteliğe sahip olup olmaması önem arz etmemektedir[18]. Bir kişinin belirli bir hastalık geçirmesi veya kanında bir madde tespit edilmesi gibi objektif olgular içeren nesnel nitelikteki bilgiler kişisel veri kabul edildiği gibi; bir kişinin bankalar tarafından oluşturulan sicili veya iş hayatındaki performansı gibi sübjektif görüş veya değerlendirmeler içeren öznel nitelikteki bilgiler de kişisel veri kabul edilir[19]. Zira öznel nitelikteki bilgiler sübjektif görüş veya değerlendirmeler içermekle beraber örneğin, bir kişinin bankalar nezdindeki sicili, bankacılık sektöründe yapacağı iş ve işlemlerde; yine bir kişinin iş hayatındaki performansı, iş yerindeki pozisyonunun belirlenmesinde yahut gelecekte başvuracağı bir işte kişi hakkında belirleyici bir rol oynayacağından nihayetinde kişisel veri kabul edilmesi gerekir.

Kişiye ilişkin bilgilerin kişisel veri kabul edilebilmesi için gizli olması aranmaz[20]. Kişisel verilerin korunması, temelde her ne kadar özel hayatın gizliliği ile kişinin özel yaşam ve aile yaşamının korunmasına ilişkin temel hakkına dayanmakta

[15] Elif KÜZECİ, **Kişisel Verilerin Korunması**, 3.Baskı, Ankara, 2019, s. 10.
[16] AKSOY, s. 13.
[17] Paul VOIGT / Axel von dem BUSSCHE, **The EU General Data Protection Regulation (GDPR) A Practical Guide**, Springer, 2017, s. 11.
[18] Art. 29 Working Party, WP136, s. 6.
[19] Dilek YÜKSEL CİVELEK, **Kişisel Verilerin Korunması ve Bir Kurumsal Yapılanma Önerisi,** Ankara, 2011, s.16; AKSOY, s. 14.
[20] AKSOY, s. 13.

ise de kişinin kamuya açık alandaki davranışları da koruma alanına dâhil edilmiştir[21]. Aksi bir düşünce kişinin yalnızca mahrem bilgilerinin kişisel verilerin korunması hukuku kapsamında olduğu ve kişinin kamuya açık alanda korumasız bırakılacağı anlamına gelir. Ancak bu durum da yine kişisel verilerin korunması hukukunun amacına uymayan hukuksal sonuçların doğmasına sebebiyet verecektir.

Bir bilginin kişisel veri olarak değerlendirilmesinde ve kişisel verilerin korunması kapsamına girip girmediğinin belirlenmesinde, bilginin hangi biçimde ortaya çıktığı veya hangi ortamda saklandığı önem arz etmemektedir[22]. Kişisel veri kavramındaki diğer unsurların sağlanması koşuluyla verinin formu (örneğin fotografik veya akustik olması) o verinin kişisel veri olması özelliğine etki etmeyecektir[23]. Aynı şekilde bir bilginin kağıda geçirilmiş olması yahut bilgisayar veya elektronik ortamda saklanması, o verinin kişisel veri olması özelliğini değiştirmeyecektir. Bu bağlamda belirlenmiş veya belirlenebilir bir kişiye ait olması durumunda özellikle ses ve görüntü verilerinin de kişisel veri niteliğinde olduğu tartışmasızdır. Zira kişisel verilerin korunmasına ilişkin hem Türk hukukunda[24] hem AB düzenlemelerinden 95/46/EC sayılı Yönerge'de[25] ses ve görüntü verilerine özellikle ve ayrıca atıfta bulunulmuş olup koruma kapsamında olduğu düzenlenmiştir. Buna göre bir konservatuar öğrencisinin akustik hâlde tutulmuş ses kaydı, telefon bankacılığı hizmetlerinde müşterinin

---

[21] Kişiye ilişkin kamuya açık alanda kaydedilen verinin özel hayat kapsamına girdiği ve kişisel veri sayıldığına ilişkin Avrupa İnsan Hakları Mahkemesi (AİHM) ilgili kararları: Rotaru/Romanya 28341/95 sayılı karar, Aman/İsviçre 27798/95 sayılı karar. Kararlar için bkz. https://hudoc.echr.coe.int/tur (Erişim:27.03.2020).

[22] Art. 29 Working Party, WP136, s. 7.

[23] Mine KAYA, **Elektronik Ortamda Kişilik Hakkının Korunması**, Ankara, 2015, s. 38.

[24] Kişisel Verilerin Korunması Kanunu Tasarısı (1/541) ve Adalet Komisyonu Raporu, m.3 gerekçesi: *"…İsim, telefon numarası, motorlu taşıt plakası, sosyal güvenlik numarası, pasaport numarası, özgeçmiş, resim, görüntü ve ses kayıtları, parmak izleri, genetik bilgiler gibi veriler dolaylı da olsa kişiyi belirlenebilir kılabilme özellikleri nedeniyle kişisel verilerdir."*, s. 7, https://www.tbmm.gov.tr/sirasayi/donem26/yil01/ss117.pdf (Erişim:27.03.2020).

[25] 95/46/EC sayılı Yönerge giriş bölümü 14. paragraf *"Gerçek kişilere ilişkin ses ve görüntü verilerini yakalamak, iletmek, değiştirmek, kaydetmek, saklamak veya nakletmek için kullanılan teknolojilerin, bilgi toplumu çerçevesinde devam eden gelişmelerinin önemi dikkate alındığında, bu Direktif bu tür verileri gerektiren işlemeye uygulanmalıdır."*, 17.paragraf *"Başta görsel işitsel alan olmak üzere, ilgili edebi ve sanatsal ifade amaçlarının yanı sıra gazetecilik amaçları için ses ve görüntü verilerinin işlenmesinde; Direktifin esasları, m.9'da öngörülen hükümlere göre, sınırlı bir şekilde uygulanacaktır."*, 33. madde *"...Komisyon, özellikle, gerçek kişilere ilişkin ses ve görüntü verilerinin işlenmesinde bu Direktifin uygulanmasını inceleyecektir ve bilgi toplumundaki ilerleme durumunun ışığında ve bilgi teknolojisindeki gelişmeleri dikkate alarak gerekeceği kanıtlanan herhangi uygun önerileri sunacaktır."* düzenlemelerini içermektedir. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:31995L0046 (Erişim:27.03.2020).

bankaya talimat verdiği ses kaydı, bir kimsenin psikiyatrik analiz amacıyla yaptığı resim, güvenlik kamerası görüntüleri, anonimleştirme işlemine tabi tutulmamış grafik ve şekiller, kişinin belirlenmesini veya belirlenebilir olmasını sağlıyor ise kişisel veri olarak kabul edilir[26].

Son olarak belirtelim ki bilginin, kişisel verilerin korunması kapsamına dâhil edilmesi için muhakkak doğru olması aranmaz. Gerçek veya doğruluğu kanıtlanmamış ve hatta yanlış bilgiler de kişisel veri olarak kabul edilir[27]. Kişisel verilerin korunmasına ilişkin yasal düzenlemelerde, veri sahibine hakkında işlenmiş yanlış bilgilerin düzeltilmesini talep etme hakkının tanınmış olması da bu durumun bir göstergesidir.

1.1.1.2 Bilginin Kişiye İlişkin Olması

Bilgininin kişiye "ilişkin" olması unsuru, bilginin kimliği belirli veya belirlenebilir bir kişi "hakkında" olmasını ve o kişiyle "bağlantılı" olmasını ifade eder. Bir verinin kişiye ilişkin olduğunu belirlemenin birkaç yolu vardır. Bilgi ile kişiyi ilişkilendirebilmek için verinin içerik, amaç veya sonuç unsurlarından en az birinin kişi ile alakalı olması gerekmektedir.

İçerik, amaç ve sonuç unsurlarına ilişkin açıklama yapmadan önce, bazı durumlarda bilginin doğrudan kişiye ilişkin değil de nesneye ilişkin olması ihtimaline dikkat çekmekte fayda bulunmaktadır. Bilgi ilk aşamada her ne kadar nesne hakkında olabilse de bir nesne hakkındaki bilgi, kişi ile ilişkilendirilebildiği ölçüde kişisel veri sayılabilir. Kısaca, bir nesneye ilişkin bilgi dolaylı yoldan bir kimse ile ilişkilendirilebilir ve bu durumda kişisel veri mahiyetine bürünebilir. Bu duruma örnek vermek gerekirse, bir bölgedeki konut fiyatlarının değerlendirilmesi hususu kişisel veri sayılmazken, konut fiyatlarının o bölgede yaşayan bir kişi ile ilişkilendirilmesi ve o kişinin vergi yükümlülüğü ile bağlantı kurulması durumunda kişisel veri olarak kabul edilecektir[28].

---

[26] YÜKSEL CİVELEK, s. 17; AKSOY, s. 15.
[27] Art. 29 Working Party, WP136, s.6; AKSOY, s. 14.
[28] Douwe KORFF, **New Challenges to Data Protection Study - Working Paper No. 2: Data Protection Laws in the EU: The Difficulties in Meeting the Challenges Posed by Global Social and**

Bir bilginin içerik yönünden bir kişiye ilişkin olması, amaç ve sonuçtan bağımsız olarak bilginin ilgili kişi hakkında olmasını ifade eder. Bilginin içeriğinin kişiye ilişkin yahut kişiyle ilgili olduğuna ilişkin birçok örnek vermek mümkündür. Bir hastanın kan tahliline ilişkin veri, kişinin sabıka kaydına ilişkin veri, çalışanın işyerinde performans değerlendirmesinin kaydına ilişkin veri, sporcunun sportif faaliyetlerinin başarısı yahut başarısızlığının kaydına ilişkin veri içerik itibariyle doğrudan kişiye ilişkin verilere örnektir. Yine bilginin içerik itibariyle doğrudan kişinin kendisine değil de faaliyetlerine ilişkin olan ve içerik itibariyle kişiyle ilişkilendirilebilen veriler de olabilir. Kişinin banka yahut kredi kartı hesap özetleri, ayrıntılı telefon faturaları bu duruma örnek olarak verilebilir[29].

Bir bilginin amaç yönünden kişiye ilişkin olması, bir bilginin kişinin durumunu ve davranışlarını değerlendirmek, kişi hakkında bilgi sahibi olmak ve kişiyi etki altında bırakmak amacıyla toplanması veya işlenmesini ifade eder. Örneğin, bisküvi fabrikasında bisküvi üretim makinasının çalışmasına ilişkin toplanan veri, makinanın verimliliğini izlemek için kaydedilirse kişisel veri sayılmaz. Ancak makinayı kullanan çalışanın performansını izlemek ve değerlendirmek amacıyla kaydedilmesi durumunda kişisel veri sayılacaktır[30]. Esasen, bir bilginin amaç yönünden kişi ile ilişkilendirilmesi dar yorumlanmamalıdır. Bir bilgiyi toplamaktaki veya işlemekteki birincil amaç bir kimse hakkında bilgi sahibi olmak, bir kimsenin durumunu ve davranışlarını değerlendirmek veya kişiyi etki altına almak olmasa bile nihayetinde elde edilen bilginin kişi ile ilişkilendirilebilme ve kişi hakkında çıkarım yapabilme olasılığı doğacaktır. Bu olasılığın var olduğu durumda elde edilen verinin kişisel veri kabul edilmesi kaçınılmaz olacaktır.

Bir bilginin sonuç yönünden bir kişiye ilişkin olması, içerik ve amaç unsurundan bağımsız olarak değerlendirilmeli ve bir bilginin kullanımı bir kimsenin hak ve çıkarları üzerinde etki edecek ise sonuç itibariyle kişisel veri kabul edilmelidir. Burada

---

Technical Developments, European Commission DG Justice, Freedom and Security Report, Haziran 2010, s.43; Art. 29 Working Party, WP136, s. 9.

[29] Information Commissioner's Office (ICO), "**What is personel data? Key definitions",** 24 Mayıs 2018, s. 18, (Çevrimiçi), https://ico.org.uk/media/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/what-is-personal-data-1-0.pdf (Erişim:28.03.2020); KORFF, **New Challenges to Data Protection,** s. 42; Art. 29 Working Party, WP136, s.10.

[30] Information Commissioner's Office (ICO), "**What is personel data? Key definitions",** s. 20.

kişinin hak ve menfaatleri üzerindeki potansiyel sonucun etkisinin önemi yoktur; önem arz eden husus verinin işlenmesinin kişinin diğer kişilerden farklı muamele görmesine yol açmasıdır. Örneğin, bir taksi durağının müşterilerine daha iyi hizmet verebilmek ve yakıt tasarrufu sağlamak amacıyla taksilerin lokasyonunu belirleyen bir sistem kullanmaları durumunda; amaç her ne kadar taksi şoförlerinin performansını izlemek olmasa da elde edilen veriler sonuç itibariyle şoförlerin performansı, hız sınırına uyup uymadıkları gibi menfaatlerini etkileyecek bilgilerin elde edilmesine hizmet edeceğinden dolayı el edilen bu veriler kişisel veri sayılacaktır[31].

1.1.1.3. Belirli Veya Belirlenebilir Gerçek Kişi

Kişisel veri kavramının tanımına ilişkin incelenecek son unsur belirli veya belirlenebilir gerçek kişidir.[32] Burada tek bir unsur varmış gibi gözükse de "kişi" ve "kimliği belirli veya belirlenebilir" ifadeleri birbirinden farklı manalara gelmekte olup her iki kavramın ayrı ayrı açıklanması gerekir. Bu çerçevede öncelikle kişi ile nitelendirilmek istenenin ne olduğu açıklanacak, ardından kişinin belirli veya belirlenebilir olmasının ne anlama geldiği izah edilecektir.

Kişisel veri kavramı belirli veya belirlenebilir bir gerçek kişiye ilişkin her türlü bilgi olarak tanımlanmıştır. Kişi, haklara sahip olabilen ve borç altına girebilen varlıkları ifade eder[33]. Bir başka ifadeyle hak ehliyetine sahip varlıklara kişi denmektedir[34]. Hukuk sisteminde gerçek kişiler ve tüzel kişiler olmak üzere iki tür kişi kabul edilmiştir. Gerçek kişiler, insanlardır[35]. Tüzel kişiler ise, kendilerine kişilik

---

[31] Art. 29 Working Party, WP136, s. 11; KORFF, s. 44.

[32] Avrupa Birliği mevzuatında Tüzük ve Yönerge'de kişisel verisi işlenen gerçek kişileri nitelemek için "data subjet" ("veri sahibi" veya "veri öznesi") deyimi kullanılmakta iken 6698 sayılı Kanun'da kişisel verileri işlenen gerçek kişileri nitelemek için "ilgili kişi" deyimi tercih edilmiştir. Çalışmamızda kişisel verileri işlenen kişiyi ifade etmek için "veri sahibi", "veri öznesi", "ilgili kişi" deyimleri kullanılmış/kullanılacak olup tüm bu deyimler birbiriyle eş anlamlıdır.

[33] Serap HELVACI, **Gerçek Kişiler**, 5.Bası, İstanbul, 2013, s. 23; Hüseyin HATEMİ, **Kişiler Hukuku**, 8.Baskı, İstanbul, 2020, s. 2; Kemal OĞUZMAN / Özer SELİÇİ / Saibe OKTAY ÖZDEMİR, **Kişiler Hukuku Gerçek ve Tüzel Kişiler,** İstanbul, 2016, s. 2; Jale AKİPEK/ Turgut AKINTÜRK/Derya ATEŞ, **Türk Medeni Hukuku Başlangıç Hükümleri Kişiler Hukuku,** 15.Baskı, İstanbul, 2019, s. 341; Mustafa DURAL/ Tufan ÖĞÜZ, **Türk Özel Hukuku Cilt II Kişiler Hukuku, 18.Baskı,** İstanbul, 2017, s. 5.

[34] Mehmet AYAN / Nurşen AYAN, **Kişiler Hukuku**, 8.Baskı, Ankara, 2016, s. 29.

[35] HELVACI, s. 24; AYAN / AYAN, s. 31.

tanınmış, belirli niteliklere sahip, belirli bir amaca yönelmiş kişi ya da mal topluluklarıdır[36].

Kişisel verilerin korunması hukukunda kişi kavramının kapsamına kimlerin girmesi gerektiğine ilişkin uluslararası doktrin ve mevzuatta görüş birliği bulunmamaktadır. Burada görüş ayrılığı tüzel kişilerin verilerinin kişisel verilerin korunması kapsamında olup olmadığı, ölen kişilerin verilerinin korunması ve cenine ilişkin verilerin korunması konularından kaynaklanmaktadır.

Tüzel kişilere ait verilerin korunma kapsamında olması gerektiğini savunan görüş[37] olduğu gibi, öğretide çoğunlukla kişisel verilerin korunması kapsamının yalnızca gerçek kişiler ile sınırlı olduğu görüşü[38] savunulmaktadır. Ancak burada kişisel verinin bir gerçek kişiyi belirlenebilir kılan her türlü bilgi olduğu dikkate alındığında, tüzel kişilere ait verilerden gerçek kişiye ulaşmak mümkünse, bu durumda söz konusu gerçek kişiye ilişkin bir korumanın sağlanması gerekeceği unutulmamalıdır.

Avrupa Birliği düzenlemelerine bakıldığı zaman; Avrupa Birliği Genel Veri Koruma Tüzüğü'nün giriş bölümünün 14. paragrafında açıkça Tüzük'ün uygulama alanının gerçek kişilere ait bilgilerin işlenmesi ile sınırlı olduğu, tüzel kişilere ait

---

[36] HELVACI, s. 24; AYAN / AYAN, s. 31.

[37] KORFF'a göre; kişisel verilerin korunmasına ilişkin gerçek kişiler ve tüzel kişiler arasında ayrım yapmak veri koruma amacıyla örtüşmeyebilmektedir. Esnaf veya gerçek kişi tacir gibi bazı gerçek kişiler tüketiciler gibi diğer gerçek kişilerden daha az koruma gerektirebileceği gibi; dini, siyasi ve sendikal örgüt gibi bazı tüzel kişiler büyük şirketler gibi tüzel kişilerden daha fazla koruma gerektirebilir. Hatta kimi durumlarda bazı gerçek kişiler bazı tüzel kişilerden daha az koruma gerektirebilir ve nitekim tüzel kişiler için herhangi bir korumanın olmaması menfaatlerinin olumsuz anlamda etkilenmesine sebebiyet verebilir. Ayrıntılı bilgi için bkz. Douwe KORFF, **Study on the Protection of the Rights and the Interests of Legal Persons of Personal Data Relating to Such Persons,** Commission of the European Communities Report, Ekim 2008, s.43; Nilgün BAŞALP, **Kişisel Verilerin Korunması ve Saklanması,** Ankara, 2004, s. 35.

[38] Kişisel verilerin korunması kapsamına tüzel kişilerin dâhil edilmemesinin yerinde bir düzenleme olduğu, kişisel verilerin korunmasındaki amacın temel hak ve özgürlüklerin korunması, kaynağının ise özel yaşamın gizliliği hakkı olduğu, kişisel verilerin korunması kapsamına tüzel kişilerin dâhil edilmesinin kişisel verilerin korunmasının temel felsefesine aykırı olacağı gibi korumanın zayıflaması tehlikesini de beraberinde getirebileceği, tüzel kişilerin verilerin korunmasının hukukumuzda başka bir alan olan ticari sırların konusunu oluşturduğuna ilişkin bkz. KÜZECİ, s. 317-318; Özel hayatın esas itibariyle gerçek kişilere ilişkin bir kavram olduğu, tüzel kişiler için ticari gizliliğin korunmasının söz konusu olabileceğine ilişkin bkz. Durmuş TEZCAN, **"Bilgisayar Karşısında Özel Hayatın Korunması",** Anayasa Yargısı, 1991, s. 389; Tüzel kişilere ait verilerin veri koruma hükümleri kapsamında korunamasa bile sözleşmeler hukuku, haksız fiil, fikri mülkiyet hukuku gibi alternatif yasal koruma sistemleri ile korunabileceğine ilişkin bkz. Jerry KANG, **"Information Privacy in Cyberspace Transactions",** Stanford Law Review, C.50, 1998, s. 1211.

bilgilerin işlenmesinin Tüzük kapsamında yer almadığı belirtilmiştir. Oysaki Tüzük'ten önce yürüklükte bulunan 95/46/EC sayılı Yönerge'de yer alan kişisel veri tanımında, gerçek kişilerin kişisel verilerin korunması kapsamında yer aldığı belirtilmişse de Yönerge'nin giriş bölümünün 24. paragrafında taraf devletlerin tüzel kişilerin de kişisel verilerin korunması kapsamına dâhil edilmesine ilişkin yasal düzenleme yapmalarına engel bir durumun olmadığı kararlaştırılmıştır. Bu kapsamda Avrupa Birliği üye ülkelerinden Avusturya, Danimarka, İtalya ve Lüksemburg'da tüzel kişilere ait kişisel veriler korunmaktadır[39]. Aynı yaklaşım Avrupa Birliği üye ülkesi olmayan İzlanda, Norveç ve İsviçre'de kabul edilmekte ve tüzel kişilere ait kişisel veriler koruma kapsamında yer almaktadır[40]. Avrupa Birliği üye ülkelerinden Belçika, Finlandiya, Fransa, Almanya, Yunanistan, İrlanda, Hollanda, Portekiz, İspanya, İsveç ve 31 Ocak 2020 tarihinde Avrupa Birliği'nden ayrılan İngiltere'de ise yalnızca gerçek kişilere ait kişisel veriler kişisel verilerin korunması kapsamına dâhil edilmiştir[41].

Her ne kadar Tüzük'te ve Yönerge'de tüzel kişilere ait veriler kişisel verilerin korunması kapsamına dâhil edilmemiş olsa da elektronik haberleşme sektöründe kişisel verilerin korunmasına ilişkin ilkeleri belirleyen Avrupa Birliği düzenlemesi olan 2002/58/EC sayılı Elektronik Haberleşme Sektöründe Kişisel Verilerin İşlenmesi Ve Özel Hayatın Gizliliğinin Korunmasına İlişkin Direktif'in 1. maddesinin 2. fıkrasında tüzel kişi abonelerin korumadan yararlanacağı düzenlenmiştir[42]. Ancak anılan Direktif'in giriş bölümünün 12. paragrafında elektronik haberleşme hizmetine gerçek kişilerin ve tüzel kişilerin abone olabileceği, Direktif'in 94/46/EC sayılı Yönerge'ye ek olarak gerçek kişilerin temel hakları ile tüzel kişilerin menfaatlerini

[39] KORFF, **Study on the Protection** s. 23-37.
[40] KORFF, **Study on the Protection,** s. 37-38.
[41] KORFF, **Study on the Protection,** s. 39-41; Almanya, Yunanistan ve daha az ölçüde Fransa'da kabul edildiği üzere veri koruması kişilik hakkı ve insan kimliğinden kaynaklanmaktadır ve amaç gerçek kişilerin mahremiyetine ilişkin özel hayatının ve özel alanının korunmasıdır. Benzer biçimde İspanya ve Finlandiya gibi ülkelerde ise veri koruması mahremiyet, özel yaşam, kişisel veya ailevi nitelikler, onur, haysiyet gibi daha geleneksel değerler ile bağlantılıdır. Buna göre insan kişiliği, haysiyet, ailevi nitelikler gibi değerlere sahip olmayan tüzel kişilerin gizlilik veya korunmaya tabi bir özel alanları da söz konusu olmayacaktır. KORFF, **Study on the Protection**, s. 42.
[42] **"Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications)"** Official Journal of the European Communities, 31 Temmuz 2002. Direktif metni için bkz. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:32002L0058 (Erşim:04.04.2020).

korumayı amaçladığı, Direktif'in uygulanmasının 95/46/EC sayılı Yönerge'nin uygulama alanında tüzel kişilerin meşru menfaatlerinin korunmasını genişletme yükümlülüğü getirmediği ve istisnai bir düzenleme olduğu açıklanmıştır.

6698 sayılı Kanun'da da yalnızca gerçek kişilerin kişisel verilerinin koruma kapsamına alındığı hem Kanun'un kapsamının düzenlendiği 2. maddeden hem de kişisel verinin tanımının yapıldığı 3. maddeden anlaşılmaktadır[43]. 2008 tarihli Kişisel Verilerin Korunması Kanun Tasarısı'nda (KVKKT) tüzel kişilerin verileri kişisel verilerin korunması kapsamına alınmış; ancak daha sonra bu yaklaşımdan vazgeçilerek 2014 tarihli KVKKT'de ve nihayet yürürlüğe giren Kanun'da tüzel kişiler, kişisel verilerin korunması kapsamı dışında bırakılmıştır[44]. Kanun her ne kadar tüzel kişileri kişisel verilerin korunması kapsamına dâhil etmemiş olsa da AB düzenlemesi olan 2002/58/EC sayılı Direktif ile benzer şekilde ulusal mevzuatta elektronik haberleşme sektöründe faaliyet gösteren işletmecilerin uyacakları usul ve esasları düzenleyen Elektronik Haberleşme Sektöründe Kişisel Verilerin İşlenmesi Ve Gizliliğinin Korunması Hakkında Yönetmelik'te[45] kişisel veri tanımına *tüzel kişilere ilişkin bütün bilgiler*[46] de dâhil edilmiştir.

Ölen kişilerin kişisel verilerine ilişkin; Tüzük giriş bölümü 27. paragrafta, Tüzük'ün uygulama alanının ölen kişilerin kişisel verilerini kapsamadığı açıkça belirtilmiş ve yine giriş bölümü 158. paragraf ve 160. paragrafta bu hususa atıfta bulunulmuştur[47]. Ancak bununla birlikte Tüzük, ölen kişilerin kişisel verilerinin işlenmesine ilişkin AB üye devletlerinin kurallar koyabileceğini belirtmiş; üye

[43] İbrahim KORKMAZ, "**Kişisel Verilerin Korunması Kanunu Hakkında Bir Değerlendirme"**, TBB Dergisi, C.29, S.124, 2016, s. 90.
[44] Nafiye YÜCEDAĞ, **"Medeni Hukuk Açısından Kişisel Verilerin Korunması Kanununun Uygulama Alanı ve Genel Hukuka Uygunluk Sebepleri"**, İÜHFM, C.75, S.2, 2017, s. 766.
[45] Elektronik Haberleşme Sektöründe Kişisel Verilerin İşlenmesi Ve Gizliliğinin Korunması Hakkında Yönetmelik, RG. 24.07.2012 T. 28363 S. Yönetmelik metni için bkz. https://www.mevzuat.gov.tr/Metin.Aspx?MevzuatKod=7.5.16405&MevzuatIliski=0&sourceXmlSearch=ki%C5%9Fisel%20verilerin (Erişim:04.04.2020).
[46] Elektronik Haberleşme Sektöründe Kişisel Verilerin İşlenmesi Ve Gizliliğinin Korunması Hakkında Yönetmelik m.37/f.1 (h) bendi.
[47] VOIGT / von dem BUSSCHE, s. 11.

devletlere ölen kişilerin kişisel verilerinin işlenmesine ilişkin düzenleme yapma imkânı tanımıştır[48].

6698 sayılı Kanun'da ise ölen kişilerin kişisel verileri kapsam dışı bırakılmıştır. Türk Medeni Kanunu (TMK) m.28'e göre kişilik ölümle sona erer. Ölüm olayıyla birlikte hak ehliyeti ve kişiye sıkı sıkıya bağlı olan, kişiliği sebebiyle tanınmış kişilik hakları da sona erer[49]. Türk-İsviçre Hukuku'nda kabul edilen hatırayı koruma görüşüne[50] göre, ölüm ile birlikte bir kimsenin kişiliği koruma hakkı sona ermiştir. Ölen kimse hakkın süjesi olma vasfını kaybedeceğinden ve dolayısıyla süjesi olmayan hak da hukuk düzenince korunmayacağından kural olarak ölen kişinin kişisel verilerinin korunması mümkün değildir. Ancak istisnai olarak ölen kişinin verileri hayatta olan kişiler bakımından kişisel veri niteliği taşıyor veyahut bir başka deyişle ölen kişinin verileri hayatta kalanları etkiliyorsa burada ölen kişilerin verilerinin dolaylı olarak veri koruma kurallarından yararlanması gerekecektir[51]. Örneğin, ölen bir kişinin kalıtsal hastalığına ilişkin sağlık verileri, hayatta kalan yakınları bakımından kişisel veri niteliğinde sayılacaktır. Ayrıca ölen bir kimsenin kişisel verilerinin ihlali yakınlarının saygı duygusunu zedeleyebilir ve böylelikle kişilik alanına dâhil olabilir. Dolayısıyla kişisel verileri ihlal edilen ölen kimsenin yakınları, genel hükümler uyarınca kendi kişilik hakkı değerlerinin korunması çerçevesinde haklarının ihlalini ileri sürebileceklerdir[52].

Ayrıca ölmüş kişilerin verileri hakkında kişisel verilerin korunmasına ilişkin mevzuatta koruyucu bir hükme yer verilmemiş olmasına rağmen diğer hukuki düzenlemelerde ölen kişilerin verileri hakkında düzenleme yer alabilir. Örneğin

[48] İtalya ve Fransa, kişisel verilerin korunmasına ilişkin yasal düzenlemelerinde kişisel verilerin korunması kapsamına ölen kişileri de dâhil eden ülkeler arasında yer almaktadır. Serge GUTWIRTH vd., **European Data Protection; In Good Health?,** Springer, 2012, s. 274.
[49] HELVACI, s. 33; DURAL/ÖĞÜZ, s.23; AYAN / AYAN, s. 176.
[50] Ümit GEZDER, **"Ölüm Sonrası Hatırayı Koruma Doktrini ve Ölüm Sonrası Kişiliğin Korunması Teorisi",** İÜHFM, C.65, S.1, 2007, s. 212; Hasan PETEK, **Kişilik Değerlerinin Ölümden Sonra Korunması,** Ankara, 2015, s. 219.
[51] Art. 29 Working Party, WP136, s. 22.
[52] GEZDER, s. 212; Nafiye YÜCEDAĞ, **"Medeni Hukuk Açısından Kişisel Verilerin Korunması Kanununun Uygulama Alanı ve Genel Hukuka Uygunluk Sebepleri",** İÜHFM, C.75, S.2, 2017, s. 767.

hekimlerin, hastaların sağlık durumuna ilişkin verileri hastanın ölümünden sonra dahi koruması gerektiğine ilişkin hukuki düzenlemeler bulunmaktadır[53].

Ceninin kişisel verilerine ilişkin Tüzük'te herhangi bir düzenlemeye yer verilmemiştir. Tüzük, giriş bölümü 27. paragrafta ölmüş kişilerin verilerini açıkça kişisel veriler kapsamından çıkarmış olmasına rağmen doğmamış çocuğun verilerini dışlayıcı bir düzenlemeye yer vermemiştir. Avrupa Konseyi Bakanlar Komitesi, Tıbbi Verilerin Korunması Hakkında R (97) 5 sayılı, 13 Şubat 1997 tarihli tavsiye kararında, doğmamış çocuklarla ilgili tıbbi verilerin kişisel veri olarak kabul edilmesi gerektiği belirtilmiştir. Ancak belirttiğimiz üzere karar tavsiye niteliğinde olup bağlayıcılığı yoktur. Nitekim Tüzük'ün kabul edilmesinden çok önce tartışılmış bir konu olmasına rağmen nihayetinde Tüzük'te ceninin verilerine ilişkin düzenleme yer almamaktadır.

Burada mesele ülkelerin ulusal hukuklarında, gerçek kişilerde hak ehliyetinin ve kişiliğin ne zaman başladığı sorusuna cevap vermekle çözüme kavuşturulabilir[54]. Türk Hukuku'nda gerçek kişiler açısından kişilik, TMK m.28/f.1 hükmüne göre çocuğun sağ olarak tamamıyla doğduğu anda başlar. Hak ehliyetini ise TMK m.28/f.2 hükmüne göre çocuk, sağ doğmak koşuluyla, anne rahmine düştüğü andan başlayarak elde eder. Dolayısıyla hak ehliyeti kişinin, sağ ve tam olarak doğmak koşuluyla, ana rahmine düştüğü andan itibaren kazanılırken hukuki anlamda kişilik, doğumun tamamlanması ile kazanılmaktadır[55]. Bu bağlamda cenin kişi olarak kabul edilmemesine rağmen ceninin hak ehliyetine sahip olduğu sonucuna varıldığından, ceninin Türk Hukuku'nda kişisel verilerinin sağ doğmak şartıyla anne rahmine düştüğü andan itibaren korunma kapsamında olduğu kabul edilmelidir[56].

---

[53] Hastanın ölümünden sonra sağlık durumuna ilişkin kişisel verilerinin korunmasına ilişkin bkz. Avrupa Hasta Haklarının Geliştirilmesi Bildirgesi m.4/f.1: *"Hastanın sağlık durumu, tıbbi durumu, tanısı, prognozu, tedavisi hakkındaki ve kişiye özel diğer tüm bilgiler, ölümden sonra bile gizil olarak korunmalıdır."*, Dünya Tabipler Birliği Bali Bildirgesi m.8/f.1: *"Hastanın sağlık durumu, tıbbi durumu, tanısı, prognozu, tedavisi ve kişiye özel diğer tüm bilgiler ölümden sonra bile gizli olarak korunmalıdır. İstisna olarak hasta yakınlarının kendileri ilgili sağlık risklerini öğrenmeleri açısından bu bilgilere ulaşabilme hakkı olabilir."*, Türk Tabipler Birliği Hekimlik Meslek Etik Kuralları m.9/f.1: *"Hekim, hastasından mesleğini uygularken öğrendiği sırları açıklayamaz. Hastanın ölmesi ya da o hekimle ilişkisinin sona ermesi, hekimin bu yükümlülüğünü ortadan kaldırmaz."*, Hasta Hakları Yönetmeliği m.21/f.3:*"Ölüm olayı, mahremiyetin bozulması hakkını vermez."*.

[54] Art. 29 Working Party, WP136, s. 22.

[55] HELVACI, s. 31; DURAL / ÖĞÜZ, s. 17; AYAN / AYAN, s. 44.

[56] Hüseyin Murat DEVELİOĞLU, **6698 sayılı Kişisel Verilerin Korunması Kanunu ile Karşılaştırmalı Olarak Avrupa Birliği Genel Veri Koruma Tüzüğü Uyarınca Kişisel Verilerin Korunması Hukuku,** İstanbul, 2017, s. 31.

Bir bilginin hangi durumda kişiyi belirli veya belirlenebilir kıldığı izah edilecek olursa; kişisel veriler yalnızca bir isim etiketi değil aynı zamanda bir bilmecenin parçaları olarak düşünülebilir[57]. Bir kişinin belirli olması, başka bir vasıtaya ihtiyaç duymaksızın o kişiyi tespit edebilmeyi ve bir grup insandan ayırt edebilmeyi ifade eder. Örneğin, kişinin TC kimlik numarası ve DNA kesiti gibi veriler başka bir vasıtaya ihtiyaç duyulmaksızın kişiyi tespite yarar verilerdir. Bunun yanı sıra bir bilmecenin parçaları benzetmesinden de yola çıkarak, yardımcı vasıtalar aracılığıyla bir kişiyi diğer kişilerden ayırt etmenin mümkün olduğu durumlarda belirlenebilir bir kişinin varlığından söz edilebilir. Kişiyi nitelemeye yardımcı olacak nitelikte kişinin yaşı, mesleği, fiziksel özellikleri gibi veriler ile IP adresi, çerezler gibi veriler kişiyi belirlenebilir kılan verilere örnek olarak verilebilir[58].

Bir kişinin tanımlanabilir olup olmadığını belirlemek için tespit etme faaliyetinin kim tarafından ve hangi ölçüde göstereceği çaba sonucunda gerçekleştirilebileceği ve belirlenebilirlik kıstası tartışma konusudur[59]. Belirlenebilirlik kıstasına ilişkin Tüzük giriş bölümü 26. paragrafta, kişinin kimliğinin belirlenebilir olup olmadığının tespitinde veri sorumlusu veya herhangi bir diğer kişi tarafından kişiyi doğrudan veya dolaylı yoldan belirlemek için kullanması makul olan tüm vasıtaların dikkate alınması gerektiği belirtilmiştir. Diğer bir deyişle veri sorumlusu veya herhangi bir kişi tarafından kişinin kimliğini tespite yarar tüm vasıta ve yöntemlere başvurulacağı varsayılmalıdır. Bu çerçevede vasıtaların makul kabul edilmesinin değerlendirilmesinde ise her bir olay kendi koşullarına göre değerlendirilmeli ve burada her bir olayda tüm şartlar dikkate alınmalıdır. Belirtmek gerekir ki teknolojik imkânlar ve gelişmeler, belirlenebilirlik için gereken maliyet ve zaman, veri işlemenin amacı, veri sorumlusunun veya veri işleyenin elde etmeyi beklediği menfaat, ilgili kişinin menfaatleri belirlenebilirlik kıstasının tespitinde dikkate alınmalıdır[60].

Burada IP adresleri konuya örnek olarak verilebilir. IP adresi internet sağlayıcıları tarafından verilmektedir ve dinamik IP adresleri kullanıldığında kişinin

[57] Sanjay SHARMA, **Data Privacy and GDPR Handbook**, John Wiley & Sons, 2019, s. 47.
[58] SHARMA, s. 47.
[59] Belirlenebilirlik kıstasına ilişkin mutlak belirlenebilirlik ve nisbi belirlenebilirlik görüşü için bkz. ÇEKİN, s. 35; AKSOY, s. 26-27.
[60] SHARMA, s. 48.

her internete girişinde yeni bir IP adresi atanmaktadır. Dinamik IP adresleri kişinin kimliğine ilişkin herhangi bir bilgi içermiyor olmasına rağmen internet sağlayıcıları dinamik IP adreslerinin kaydını tutmaktadır ve internet sağlayıcıları dinamik IP adreslerinin kime ait olduğunu belirlemek açısından makul araçlara sahiptir[61]. Dolayısıyla dinamik IP adresleri, internet sağlayıcıları açısından kişisel veri niteliğindedir[62].

6698 sayılı Kanun'da belirlenebilirlik kıstasına ilişkin bir düzenlemeye yer verilmemiş olmakla birlikte Kanun'un gerekçesinde; bir kişinin belirli veya belirlenebilir olmasının, mevcut verilerin herhangi bir şekilde bir gerçek kişiyle ilişkilendirilmesi suretiyle, o kişinin tanımlanabilir hâle getirilmesini ifade ettiği belirtilmiştir. Yine Kanun gerekçesinde isim, telefon numarası, motorlu taşıt plakası, sosyal güvenlik numarası, pasaport numarası, özgeçmiş, resim, görüntü ve ses kayıtları, parmak izleri, genetik bilgiler gibi verilerin dolaylı da olsa kişiyi belirlenebilir kılma özelliği olduğu belirtilerek kişisel veri olduğu ifade edilmiştir.

Son olarak belirtelim ki belirli veya belirlenebilir bir gerçek kişi ile ilgisi olmayan veya ilgili kişinin belirlenemeyeceği şekilde bir forma dönüştürülmüş anonim veriler[63] hem Tüzük'ün[64] hem de Kişisel Verilerin Korunması Kanunu'nun kapsamı dışında bırakılmıştır. Ancak özellikle günümüz teknolojik gelişmeleri sayesinde anonim verilerin geri döndürülme imkânı söz konusu ise ve veri sorumlusu anonimleştirilmiş verileri makul bir yöntem ile geri yükleyebiliyorsa, bu durumda artık anonim verinin değil kişisel verinin varlığı kabul edilecektir[65].

Anonimleştirme, genellikle istatistik veya araştırma amacı ile kullanılmaktadır. Örneğin bir eğitim kurumu, öğrencilerinin kaç tanesinin üniversiteye gittiğine ve üniversiteye giden kişilerin hangi bölümü okuduğuna ilişkin istatistik çalışması

---

[61] Hayrunnisa ÖZDEMİR, **"Haberleşmenin Gizliliği ve Kişisel Veriler"**, EÜHFD, C.13, S.1-2, 2009, s. 290.
[62] DEVELİOĞLU, s. 34.
[63] Kişisel verilerin anonim hale getirilmesi, 6698 sayılı Kanun'un *"Tanımlar"* başlıklı 3. maddesinin 1.fıkrasının (b) bendinde ve Kişisel Verilerin Silinmesi, Yok Edilmesi Veya Anonim Hale Getirilmesi Hakkında Yönetmelik'in *"Kişisel Verilerin Anonim Hale Getirilmesi"* başlıklı 10. maddesinde *"kişisel verilerin başka verilerle eşleştirilse dahi hiçbir surette kimliği belirli veya belirlenebilir bir gerçek kişiyle ilişkilendirilemeyecek hale getirilmesi"* şeklinde tanımlanmıştır.
[64] Tüzük, Giriş Bölümü, par. 26.
[65] VOIGT / von dem BUSSCHE, s. 14.

yapmak amacıyla geçmişteki öğrencileri ile çevrimiçi bir anket yolu ile iletişim kurar. Ancak bu ankette verileri anonimleştirmek amacı ile e-posta adresi, ad-soyad, mezuniyet yılı, doğum tarihi ile ilgili sorular yer almamakta ve katılımcıların IP adresleri kaydedilmemektedir. Ayrıca daha az tercih edilen üniversite ve bölümlere giden kişileri anlaşılmaması amacıyla bu üniversite ve bölümler ayrıca gruplandırılmaktadır. Bu örnekte eğitim kurumu, kişilerin belirlenmesine olanak sağlayacak verileri toplamaktan kaçınarak ve toplanan verilerin miktarını anketin gerçekleştirilmesi için gerekli olan en aza indirerek başarılı bir anonimleştirme faaliyetinde bulunduğundan, ankette yer alan bilgiler anonim veri olarak kabul edilebilir[66].

Açıklığa kavuşturulması gereken bir kavram daha vardır ki o da psödonim verilerdir. Anonim verilerin aksine psödonim veriler Tüzük kapsamında kişisel veri olarak kabul edilmiştir[67]. Psödonimleştirme, bir başka deyişle "takma adlandırma", kişisel verilerin ek bilgi kullanılmadan belirli bir veri öznesi ile ilişkilendirilmeyecek şekilde işlenmesidir. Psödonim veriler, ek bilgilerle birlikte kullanılmaları hâlinde kişilerin dolaylı olarak belirlenebilmesini sağlar. Dolayısıyla kişiyi yeniden tanımlama riski, anonim verilere göre daha fazladır.

Psödonimleştirme, ek teknik ve organizasyonel önlemler ile sağlanmaktadır. Genellikle kişiyi belirlemeye imkân veren ek bilgiler ayrı tutulmakta ve bu bilgiler kodlama, şifreleme, kriptografik algoritma kullanma gibi bilgilerin gerçek kişiye atfedilmesini önleyecek yöntemlerle yapılmaktadır[68]. Örneğin, A ve B işletmelerini de barındıran bir grup teşebbüste A, grup müşterilerinin kişisel verilerini toplar ve B müşteri tercihlerine ilişkin profil oluşturmak için toplanan verileri alır. Ancak veriler B'ye verilmeden önce müşterilerin kişisel verilerini içeren müşteri bilgileri kaldırılarak yerine kod verilir ve takma isimlendirilir. Mevcut durumda B, kodu ilgili müşteri ile ilişkilendirecek anahtara sahip değildir. Ancak veriler anonim değildir ve A'da kodun hangi müşteriye ait olduğunun tespitini sağlayan anahtar vardır.

[66] VOIGT / von dem BUSSCHE, s. 14.
[67] Sophie STALLA-BOURDILLON / Alison KNIGHT, **Anonymous Data V. Personal Data-A False Debate: An EU Perspective on Anonymization, Pseudonymization and Personal Data**, Wisconsin International Law Journal, 34 (2), 2017, s. 286.
[68] Art. 29 Working Party, WP136, s. 18.

Dolayısıyla B'nin A aracılığıyla müşteri kimliğini tanımlama imkânı olduğundan psödonim verinin var olduğunu söyleyebiliriz[69].

1.1.2. Kişisel Veri Türleri

1.1.2.1. Özel Nitelikli Kişisel Veriler

Kişisel verilerin korunmasına ilişkin ulusal ve uluslararası yasal düzenlemelerde verilerin bir kısmı özel nitelikli veri, bir başka deyişle hassas veri olarak nitelendirilmiştir. Bazı verilerin işlenmesi, verisi işlenen kişinin temel hak ve özgürlükleri bakımından önemli riskler yatabileceğinden daha özenli korumayı hak eder. Genel nitelikli kişisel verilerden daha etkin koruma altına alınmış bu verilere, özel nitelikli kişisel veriler denmektedir. Böyle bir ayrıma gidilmesinde, söz konusu verilerin kötüye kullanılması ihtimalinde veri sahibi üzerinde doğabilecek zararın ve mağduriyetin daha büyük olması endişesi yer almaktadır[70]. Ayrıca özel nitelikli kişisel verilerin genel nitelikli kişisel verilere kıyasla ayrımcılık gibi sorunlara neden olma ihtimali daha yüksektir.

Özel nitelikli veriler, kişisel verilerin korunmasına ilişkin mevzuatta diğer verilere kıyasla daha çok koruma altına alınmıştır; ancak bu ifadenin kişisel verilerin korunmasına ilişkin bütün yasal düzenlemeleri kapsadığı söylenemez. Avrupa Birliği Genel Veri Koruma Tüzüğü, 95/46/EC sayılı Yönerge, 108 sayılı Sözleşme, BM Rehber İlkeler, 6698 sayılı Kanun belirli türdeki verilere özel koruyucu hükümler getirirken, OECD Rehber İlkeler ve APEC (Asya-Pasifik Ekonomik İşbirliği Forumu) Çerçeve Belgesi'nde özel koruyucu hükümler bulunmamaktadır[71].

---

[69] VOIGT / von dem BUSSCHE, s. 15.
[70] Murat Volkan DÜLGER, "**İnsan Hakları ve Temel Hak ve Özgürlükler Bağlamında Kişisel Verilerin Korunması",** İMÜHFD, C.5, S.1, 2018, s. 73.
[71] KORKMAZ, s. 111-112; Çiğdem AYÖZER, **Kişisel Verilerin Korunması Hukuku Elektronik Haberleşme Sektörüne İlişkin Özel Düzenlemeler Dâhil**, 2.Baskı, İstanbul, 2019, s. 18.

Bu tür verileri ifade etmek üzere çeşitli uluslararası düzenlemelerde aynı anlamı karşılayacak şekilde "hassas veri"[72], "özel kategorili kişisel veriler"[73], "özel kişisel veriler"[74], "özel korumaya layık olan veriler"[75] gibi çeşitli kavramlar kullanılmıştır.

Her ne kadar bazı verilerin mahiyetleri itibariyle, kişilerin mağduriyetine ve ayrımcılığa uğramasına sebep olması bakımından yüksek önemi haiz olduğunu belirtsek de özel nitelikli veri-genel nitelikli veri ayrımı herkes tarafından kabul edilmemektedir. Örneğin Federal Almanya Anayasa Mahkemesi 1983 tarihli Nüfus Sayımı Kararı'nda, kişisel verilerin tamamının önemli olduğunu ve bu sebeple önemliler ve daha az önemliler gibi bir ayrıma gidilemeyeceğini; başlangıçta kişi için tehlike arz etmeyecek basit bir bilginin otomatik işleme sistemleri sonucu önemli hâle gelebileceğini belirtmiştir[76]. Ancak aksi yönde; kişisel verinin işlenmesinden elde edilebilecek yarar ile oluşabilecek tehlike arasındaki dengenin sağlanabilmesi açsından bazı kişisel verilerin diğerlerine oranla daha fazla korunmasının yadırganmaması gerektiğine ilişkin görüş de mevcuttur[77].

Tüzük m.9'da özel nitelikli kişisel verilerin neler olduğu sayılmış olup numerus clauses ilkesine tabi bu sayıma göre kişinin ırksal veya etnik kökeni, siyasal görüşleri, dinsel veya felsefi inançları, sendika üyeliği, sağlık[78], cinsel yaşam ve cinsel eğilimine ilişkin veriler ile bir gerçek kişinin kimlik teşhisinin yapılması amacıyla genetik

[72] İngiliz 1998 tarihli Kişisel Verilerin Korunması Kanunu'nda "sensitive personal data" olarak tanımlanmıştır. KORKMAZ, s. 112.
[73] Örnek olarak bkz. 2001 tarihli Alman Federal Veri Koruma Kanunu, 2003 tarihli Litvanya Kişisel Verilerin Hukuki Korunması Hakkında Kanun, 2002 tarihli Slovakya Kişisel Verileri Koruma Hakkında Kanun. Cemil KAYA, **"Avrupa Birliği Veri Koruma Direktifi Ekseninde Hassas (Kişisel) Veriler ve İşlenmesi",** İÜHFM, C.LXIX, S.1-2, 2011, s.318.; AK Sözleşmesi, AB Yönergesi gibi metinlerde de bu veriler "özel kategorideki veriler" olarak isimlendirilmiştir. KÜZECİ, s. 242.
[74] Örnek olarak bkz. 2000 tarihli Hollanda Veri Koruma Kanunu. KAYA, s. 318; KORKMAZ, s. 112; AYÖZER, s. 18.
[75] Örnek olarak bkz. 2000 tarihli Avusturya Federal Kişisel Verilerin Korunması İle İlgili Kanun. KAYA, s. 318.
[76] KÜZECİ, s. 245.
[77] KORKMAZ, s. 113.
[78] Sağlık verileri, Tüzük m.4/f.15'te tanımlanmıştır: *" 'sağlıkla ilgili veri' sağlık hizmetlerinin sağlanması da dahil olmak üzere bir gerçek kişinin sağlık durumuyla ilgili bilgilerin açıklandığı, söz konusu gerçek kişinin fiziksel veya ruhsal sağlığına ilişkin kişisel verilerdir."*.

verileri[79] ile biyometrik verileri[80] özel nitelikli kişisel veridir. Ayrıca mahkûmiyet kararları ve ceza gerektiren suçlara ilişkin ya da ilgili güvenlik tedbirlerine ilişkin kişisel veriler de Tüzük m.10 uyarınca özel bir korumaya tabi tutulmuştur.

95/46/EC sayılı Yönerge'den farklı olarak; Tüzük'te bir gerçek kişinin kimliğini belirlemek amacıyla işlenen genetik verilerin ve biyometrik verilerin özel nitelikli veri olduğu belirtilmiştir. Yine Yönerge'de yer alan kişinin cinsel yaşamına ilişkin veriler kategorisinin yanında cinsel eğilimine ilişkin verilerin de özel nitelikli veri kapsamında olduğu açıkça düzenlenmiştir.

Tüzük'ün özel nitelikli verilere ilişkin getirdiği yeni düzenlemeler, yeni veri kategorilerinin eklenmesi ile sınırlı değildir. Çalışmamızın konusunu bizzat ilgilendiren önemli bir yenilik söz konusudur ki bu da özel nitelikli kişisel verilerin işlenmesi bakımından Tüzük m.37 kapsamında zorunlu olarak veri koruma görevlisinin belirlenmesidir. Veri sorumlusunun veya veri işleyenin temel faaliyetlerinin Tüzük m.9'da sayılan özel nitelikli kişisel verilerin geniş çapta işlenmesinden meydana gelmesi hâlinde, ilgili veri sorumlusunun veya veri işleyenin veri koruma görevlisi belirlemesi zorunludur.

Yine özel nitelikli kişisel verilere ilişkin Tüzük ile getirilen bir başka yeni düzenleme ise Tüzük m.35 uyarınca getirilen riskli veri işleme faaliyetleri bakımından zorunlu veri koruma etki değerlendirmesi yapılmasıdır. Bu düzenlemeye göre; özellikle yeni teknolojik veri işleme yöntemlerinin kullanıldığı ve veri işleme faaliyetlerinin gerçek kişilerin hakları ve özgürlükleri açısından yüksek bir riske sebebiyet vermesinin muhtemel olduğu hâllerde veri sorumlusu, işlemenin kapsamı, niteliği, bağlamı ve amacını da dikkate alarak işleme faaliyetinden önce, öngörülen işleme faaliyetlerinin kişisel verilerin korunmasına olan etkisine ilişkin bir değerlendirme yapar. Tüzük m.35/f.2'de, özellikle hangi durumlarda veri koruma etki

[79] Genetik veri, Tüzük m.4/f.13'te tanımlanmıştır: *" 'genetik veri' bir gerçek kişinin fizyoloji veya sağlığı ile ilgili eşsiz bilgiler sağlayan ve özellikle söz konusu gerçek kişiden alınan bir biyolojik numunenin analizinden kaynaklanan ve söz konusu kişinin kalıtım yoluyla alınan veya kazanılan özelliklerine ilişkin kişisel verilerdir."*.

[80] Biyometrik veri, Tüzük m.4/f.14'te tanımlanmıştır: *" 'biyometrik veri' yüz görüntüleri veya daktiloskopik veriler gibi bir gerçek kişinin özgün bir şekilde teşhis edilmesini sağlayan veya teyit eden fiziksel, fizyolojik veya davranışsal özelliklerine ilişkin olarak spesifik teknik işlemeden kaynaklanan kişisel verilerdir."*.

değerlendirmesi yapılması gerektiği sayılmış olup özel nitelikli kişisel verilerin işlenmesi de bu sayıma dâhil edilmiştir. Ayrıca maddede, veri sorumlusunun veri koruma etki değerlendirmesini gerçekleştirirken, belirlenmiş olması durumunda veri koruma görevlisinin tavsiyesine başvuracağı açıklanmıştır. 6698 sayılı Kanun'da bu kapsamda ayrıca tanımlanmış hükümler bulunmamaktadır; ancak veri sorumlularının ve veri işleyenlerin sorumluluklarının artırılması eğilimi doğrultusunda Tüzük'teki yenilikler uyarınca 6698 sayılı Kanun'da da bu yönde hükümlere yer verilmesi uluslararası güncel yasal düzenlemelere uyum açısından faydalı olacaktır.

6698 sayılı Kanun'da özel nitelikli kişisel veri kavramı tanımlanmamakla birlikte, hangi verilerin özel nitelikte olduğu numerus clauses ilkesine tabi olarak sayılmıştır. Bu sınırlı sayım ilkesi uyarınca sayılan veriler haricinde herhangi bir verinin özel nitelikli kabul edilip buna göre hareket edilmesi mümkün değildir[81]. Kanun'un 6. maddesine göre; kişilerin ırkı, etnik kökeni, siyasi düşüncesi, felsefi inancı, dini, mezhebi veya diğer inançları, kılık ve kıyafeti, dernek, vakıf ya da sendika üyeliği, sağlığı, cinsel hayatı, ceza mahkûmiyeti ve güvenlik tedbirleriyle ilgili verileri ile biyometrik ve genetik verileri özel nitelikli kişisel veridir. Tüzük ile karşılaştırıldığı zaman 6698 sayılı Kanun'da, Tüzükten farklı olarak kişinin mezhep ve diğer inançları, kılık ve kıyafeti, dernek ve vakıf üyeliği de hassas veri grubuna dâhil edilmişken kişinin cinsel eğilimi hassas veri grubuna dâhil edilmemiştir.

Belirttiğimiz üzere 6698 sayılı Kanun'da özel nitelikli kişisel veri kavramı tanımlanmamıştır. Fakat öte yandan Kanun'un gerekçesinde özel nitelikli verilerin, başkaları tarafından öğrenildiği takdirde ilgili kişinin mağdur olabilmesine veya ayrımcılığa maruz kalabilmesine neden olabilecek nitelikte veriler oldukları belirtilmiştir[82]. Böylelikle, bu verilerin belirlenmesinde hangi ölçütlerin kullanıldığı da açıklanmıştır.

[81] DÜLGER, **İnsan Hakları Bağlamında Koruma**, s. 74.
[82] Kişisel Verilerin Korunması Kanunu Tasarısı (1/541) ve Adalet Komisyonu Raporu, m.6 gerekçesi, s.9.

1.1.2.2. Genel Nitelikli Kişisel Veriler

Özel nitelikli kişisel veri grubunun dışında kalan tüm veriler, genel nitelikli kişisel veri olarak değerlendirilir[83]. Genel nitelikli kişisel verilere ilişkin özel bir tanımlama bulunmamakta olup özel nitelikleri verilerden ayırt edebilmek adına hassas veriler haricinde kalan veri grubu genel nitelikli olarak adlandırılmaktadır. Kişisel veri kavramı başlığı altında yapılan açıklamalar genel nitelikli kişisel veriler açısından da aynen geçerlidir.

1.1.3. Veri Sorumlusu

Veri sorumlusu, veri koruma hukuku bakımından merkezi bir konuma sahiptir. Tüzük'te "data controller" olarak yer alan ve kişisel verilerin işlenmesinin amaçlarını ve vasıtalarını belirleyen kişiye karşılık Türkçe'de veri kontrolörü, veri sorumlusu, veri denetçisi gibi deyimler kullanılmaktadır.

Tüzük m.4/f.7'de yer alan tanıma göre veri sorumlusu, yalnız başına veya başkalarıyla birlikte kişisel verilerin işlenmesine ilişkin amaçlar ve yöntemleri belirleyen gerçek veya tüzel kişidir. Veri sorumlusu, kamu kurum ve kuruluşları veya diğer herhangi bir organı, dernekler, vakıflar, şirketler, veri üzerinde hâkimiyet kurabilecek her türlü çalışan ve tedarikçi olabilir[84].

Veri sorumlusu, 6698 sayılı Kanun'da da Tüzük ile benzer şekilde "*kişisel verilerin işleme amaçlarını ve vasıtalarını belirleyen, veri kayıt sisteminin kurulmasından ve yönetilmesinden sorumlu olan gerçek veya tüzel kişi"*[85] şeklinde tanımlanmıştır[86]. Tüzük'te kamu kurum ve kuruluşlarının da veri sorumlusu olabileceği tanımda açıkça belirtilmişken Kanun'un tanımında kamu kurum ve kuruluşlarına yer verilmemiştir. Ancak Kanun'da yer alan hükümler kamu hukuku

[83] Furkan Güven TAŞTAN, **Türk Sözleşme Hukukunda Kişisel Verilerin Korunması**, 2.Baskı, İstanbul, 2017, s. 45.
[84] ÇEKİN, s. 42.
[85] 6698 sayılı Kanun m.3/f.1 (ı) bendi.
[86] Kanun'daki tanımın kişilik şartı öngörmesine ilişkin değerlendirme için bkz. ÇEKİN, s.61.

tüzel kişileri bakımından da bağlayıcı olduğundan Avrupa Birliği mevzuatında olduğu gibi Türk hukukunda da kamu hukuku tüzel kişileri veri sorumlusu sıfatını haizdir[87].

Tüzel kişilerin, kişisel verilerin işlenmesine ilişkin gerçekleştirdikleri faaliyet itibariyle veri sorumlusu bizatihi tüzel kişiliğin kendisidir[88]. Tüzel kişinin belirli bir organının veya veri işleme konusunda tüzel kişilik nezdinde görevlendirilen çalışanın eylemlerinden doğacak hukuki sorumluluk, veri sorumlusu olan ilgili tüzel kişiliğin şahsında olacaktır[89]. Nihayetinde tüzel kişiliğin veri sorumlusu olarak sorumlu olmasının ilgili kişiye güvenilir bir başvuru mekanizması sağladığı söylenebilir. Ancak bu durum bir tüzel kişilik bünyesinde yer alan gerçek kişinin hukuki sorumluluğunu her zaman ortadan kaldırmaz. Tüzel kişilik bünyesinde yer alan ancak tüzel kişinin denetim ve amaçları dışında kendi menfaatleri uyarınca veri işleyen bir gerçek kişinin bulunması hâlinde; o kişinin veri sorumlusu sıfatını haiz olacağı söylenebilir. Örneğin, bir yönetim kurulu üyesinin görev aldığı şirkette işlenen kişisel verileri kendi amaçları doğrultusunda kullanması durumunda tüzel kişiden bağımsız olarak ayrıca veri sorumlusu sıfatıyla sorumluluğu doğacaktır[90].

Tüzük m.26'da "ortak veri sorumluları" kavramına yer verilmiş olup Tüzük tanımına göre; iki ya da daha fazla sayıda veri sorumlusunun "işleme amaçları ve yöntemlerini" ortak bir şekilde belirlediği hâllerde bu veri sorumlularının ortak veri sorumlusu olduğu kabul edilir. Bu tanıma göre veri işleme amaç ve yönteminin tek bir veri sorumlusu tarafından belirlenmediği durumda ortak veri sorumlularının olduğu ve sorumluluklarının da ortak olduğu söylenebilir[91]. Ancak burada dikkat edilmesi gereken husus; paylaşılan bir işleme amaç ve aracı olmaksızın taraflar arasındaki veri alışverişi, onları ortak veri sorumluları hâline getirmez. Buradaki faaliyet bir veri

[87] KÜZECİ, s. 319.
[88] Article 29 Working Party, **"Opinion 1/2010 on the concepts of "controller" and "processor"",** WP 169, 16 Şubat 2010, s. 15.
[89] Veri sorumlusunun bir çalışanı tarafından verilerin hukuka aykırı bir biçimde işlenmesi durumunda, ilgili kişi 6698 sayılı Kanun'un yanı sıra Borçlar Hukuku uyarınca Türk Borçlar Kanunu (TBK) m.66'da yer alan adam çalıştıranın sorumluluğu hükümlerine de başvurabilecektir. TAŞTAN, s. 72.
[90] Elif KÜZECİ / Şebnem KILIÇ, **"6698 Sayılı Kişisel Verilerin Korunması Kanunu'nun İş Sözleşmesi Çerçevesinde Değerlendirilmesi: Veri Sorumlusu, Veri İşleyen Ve Diğer Aktörler"**, Legal İş Hukuku ve Sosyal Güvenlik Hukuku Dergisi, C.16, S.63, 2019, s. 12.
[91] SHARMA, s. 65.

aktarımı olduğundan dolayı burada ortak veri sorumlularından değil bağımsız veri sorumlularından bahsedilebilecektir[92].

Ortak veri sorumluları veri işleme faaliyetine başlamadan önce Tüzük'ten doğan sorumlulukların aralarında ne şekilde paylaşılacağını ve veri konularına ilişkin rolleri belirlemelidir. Bu belirlemenin yer aldığı düzenleme şeffaflık ve bilgi yükümlülükleri doğrultusunda ilgili kişinin erişimine açık olmalıdır[93]. Ayrıca ilgili kişi, taraflar aralarındaki sorumluluğu ne şekilde belirlemiş olurlarsa olsun, haklarını veri sorumlularından her birine karşı yöneltebilecektir[94].

Ortak veri sorumlularına örnek vermek gerekirse, bir havayolu şirketinin bir konaklama rezervasyon internet sitesi ile işbirliği yaptığı ve belirli bir bölgede konaklama yeri arayan kişilere havayolu şirketinin ilgili bölgeye olan uçuş seçeneklerinin sunulması durumunda, kişinin konaklama yerini ve uçuşu birlikte rezerve edebilmesi için hangi verilerin ne kadar süre saklanacağı, verilere kimlerin erişebileceği vb. veri işleme amaç ve araçlarına ortaklaşa karar vermeleri hâlinde bu iki veri sorumlusunun ortak veri sorumlusu olduğu söylenebilir[95].

Son olarak belirtelim ki 6698 sayılı Kanun'da ortak veri sorumlularına ilişkin özel bir düzenleme yer almamaktadır.

1.1.4. Veri İşleyen

Veri koruma aktörlerinden bir başkası ise Tüzük'te "data processor" olarak yer alan veri işleyendir. Veri işleyen, 6698 sayılı Kanun'un *"Tanımlar"* başlıklı 3. maddesinde *"Veri sorumlusunun verdiği yetkiye dayanarak onun adına kişisel verileri işleyen gerçek veya tüzel kişi"* şeklinde tanımlanmıştır. Bu tanımlamaya göre veri işleyen, veri sorumlusunun verdiği yetkiye dayanarak ve onun adına işleme faaliyetini gerçekleştirecektir. Bu bağlamda veri işleme faaliyetine ilişkin işlemenin amacı, işleme araçları, işlenen verilerin hangi süreler ile saklanacağı, bir başka deyişle veri

[92] VOIGT / von dem BUSSCHE, s. 34.
[93] SHARMA, s. 66.
[94] Paul LAMBERT, **Understanding the New European Data Protection Rules**, CRC Press Taylor&Francis Group, 2017, s. 105.
[95] VOIGT / von dem BUSSCHE, s. 35.

işlemenin "neden" ve "nasıl" yapılacağına yanıt veren veri sorumlusu iken bu yanıta istinaden veri işleyen kişiye ise veri işleyen denir[96].

Sorumluluğa ilişkin düzenlemeye ise Kanun'un 12. maddesinde yer verilmiştir. Buna göre Kanun, veri işleyenin veri sorumlusu ile müştereken sorumlu olacağını kararlaştırmış ve ayrıca veri işleyenin öğrendiği kişisel verileri Kanun hükümlerine aykırı olarak başkasına açıklayamayacağını ve işleme amacı dışında kullanamayacağını hüküm altına almıştır.

Veri sorumlusu ile veri işleyen arasındaki ilişki iki farklı şekilde karşımıza çıkabilir. Bunlardan biri veri işleyen kişinin veri sorumlusunun talimatları doğrultusunda çalışanı olması iken diğeri ise veri sorumlusu ile arasında sözleşme ilişkisi bulunan üçüncü bir kişinin veri işleyen olmasıdır[97]. Ayrıca bir gerçek veya tüzel kişi hem veri sorumlusu hem veri işleyen sıfatını bir arada haiz olabilir. Konuya ilişkin 6698 sayılı Kanun'un 3. maddesinin gerekçesinde verilen örneğe göre; "*bir muhasebe şirketi kendi personeliyle ilgili tuttuğu verilere ilişkin olarak veri sorumlusu sayılırken, müşterisi olan şirketlere ilişkin tuttuğu veriler bakımından ise veri işleyen olarak kabul edilecektir.*".

Tüzük'te veri işleyen, Kanun ile benzer şekilde *"veri sorumlusu adına kişisel verileri işleyen bir gerçek ya da tüzel kişi, kamu kuruluşu, kurumu veya diğer herhangi bir organ"* olarak tanımlanmıştır. Kanun'da veri işleyen ile veri sorumlusu arasındaki ilişkiye tek bir hükümde yer verilmesi ve veri işleyene ilişkin detaylı düzenlemelerin yer almamasının aksine, Tüzük'te bu her iki aktör arasındaki sorumluluk paylaşımına ilişkin özel düzenlemelere yer verilmiş ve ayrıca Yönerge'den ve Kanun'dan farklı olarak veri işleyenin yükümlülükleri genişletilerek veri sorumlusuna yaklaştırılmıştır. Veri güvenliğine ilişkin gerekli teknik ve yapısal tedbirleri alma[98], kişisel veri ihlalinden haberdar olduktan sonra herhangi bir gecikmeye mahal vermeden veri sorumlusuna bildirimde bulunma[99], işleme faaliyetlerinin kaydını tutma[100] gibi

[96] KÜZECİ / KILIÇ, **İş Sözleşmesi Çerçevesinde Değerlendirme,** s. 15; TAŞTAN, s. 71.
[97] Tekin MEMİŞ, **"Veri Sorumlusu ve Veri İşleyen Arasındaki İlişkiler ve Sorumluluk Düzeni",** Beykent Üniversitesi Hukuk Fakültesi Dergisi, C.3, S.6, 2017, s. 15.
[98] Tüzük m.32.
[99] Tüzük m.33/f.2.
[100] Tüzük m.30/f.2.

yükümlülükler Yönerge'den farklı olarak Tüzük'te düzenlenmiştir. Çalışmamızın üçüncü bölümünde ayrıntılı şekilde izah edileceği üzere; Tüzük ile veri işleyene getirilen yükümlülüklerden birisi de veri koruma görevlisi belirleme yükümlülüğüdür. Belirli şartlar altında veri koruma görevlisi belirlenmesi veri sorumlusu ile birlikte veri işleyen bakımından da kararlaştırılmıştır.

Tüzük, kişisel verilerin veri işleyen tarafından işlenmesi durumunda veri sorumlusu ile veri işleyen arasında, veri sorumlusunun talimatlarının detaylı bir şekilde belirlendiği bir sözleşmenin veya hukuki işlemin yapılması gerektiğini hüküm altına almıştır[101]. Ayrıca kişisel verilerin, veri işleyen tarafından veri sorumlusunun talimatları haricinde işlenmesi açıkça yasaklanmıştır[102].

1.2. KİŞİSEL VERİLERİN HUKUKİ NİTELİĞİ

Kişisel verilerin kamu kuruluşları ve şirketler tarafından geniş çaplı olarak toplanması, biriktirilmesi ve saklanması gibi verinin işlenmesine ilişkin faaliyetlerin artması, gizlilik ve korumaya ilişkin rejimin belirlenmesi noktasında tartışmaların da artmasına sebep olmuştur. Bu tartışmalar temelinde, Anglo-Amerikan hukuk sistemi ile Kıta Avrupası hukuk sisteminin kişiye ait veriye bakış açısının farklılığından kaynaklanmaktadır[103]. Koruma rejimine ilişkin tartışmalar iki büyük başlık altında incelenmekte olup bunlar; Anglo-Amerikan yaklaşımı olan ve veriyi kişisinden soyutlayarak üzerinde tasarrufta bulunulabilen bir mal olarak değerlendiren *ekonomik hak yaklaşımı* ile Kıta Avrupası yaklaşımı olan ve kişisel verilerin korunmasını kişilik hakkının korunması olarak değerlendiren *insan hakkı yaklaşımıdır*[104]. Gerçekten de kişisel veriler AB'de temel bir insan hakkı ve sosyal değer olarak kabul edilip katı bir düzenleme rejimi ile korunmakta iken ABD'de kişisel verilerin korunmasına ilişkin çözümler sektörel düzenlemelere bırakılmıştır[105].

---

[101] Tüzük m.28/f.3; TAŞTAN, s. 118.
[102] Tüzük m.29.
[103] Sinan Sami AKKURT, **"Kişisel Veri Kavramının Hukuki Niteliğine İlişkin Yaklaşımlara Mukayeseli Bir Bakış"**, Kişisel Verileri Koruma Dergisi, C.2, S.1, 2020, s. 21.
[104] KÜZECİ, s. 59.
[105] Serpil KARLIDAĞ, **"Ekonomi Politik Açıdan Kişisel Verilerin Korunması"**, Amme İdaresi Dergisi, C.46, S.1, 2013, s. 128.

Kişisel verilerin korunması rejiminde ekonomik hak yaklaşımını benimseyen; kişisel verinin bir mülkiyet türü olduğu teorisi ile kişisel verinin özünde fikri hakkın olduğu teorisi olmak üzere iki farklı görüş bulunmaktadır[106].

Mülkiyet hakkı teorisine göre kişisel veriler, kişiliğin bir uzantısı olmasının yanı sıra kişiliğin bir ürünüdür ve kişi malik sıfatıyla kişisel verileri üzerinde kullanma, yararlanma ve tasarrufta bulunma hakkına sahiptir[107]. Amaçsal yönden aralarında bir benzerlik olduğu gerekçesiyle[108] kişisel verilerin korunması hakkı ile fikri mülkiyet kavramını özdeşleştiren ve kişisel verilerin fikri mülkiyet hakkı kapsamında korunmasını savunan teoriye göre ise eser sahibinin eser üzerindeki manevi haklarından olan umuma arz hakkı ve eserde değişiklik yapılmasını yasaklama hakkı ile kişinin verileri üzerindeki hak ve yetkileri benzetilmekte, kişisel verilerin telif benzeri bir yaklaşımla korunması gerektiği ifade edilmektedir[109].

Daha çok Kıta Avrupası ülkelerinde kabul gören ve Türk hukukunda da benimsenen kişilik hakkı görüşüne göre ise kişisel veriler başta özel yaşamın gizliliği olmak üzere kişi temel hak ve özgürlükleri ile yakından ilişkilidir[110]. Bu sebeple kişi, verileri üzerinde denetim hak ve yetkisine sahip olmalıdır; bu da esasında kişisel verilerin korunmasını temel hak ve özgürlük kapsamında kabul etmekle mümkün olacaktır. Her ne kadar kişisel verilerin temel bir insan hakkı olduğundan hareketle korumaya ilişkin aşırı korumacı bir yaklaşımın benimsendiği kabul edilse de devlet-birey arasındaki dikey ilişkide devletin menfaatlerinin ağır bastığı durumlarda; birey-birey arasındaki yatay ilişkide ise veri sorumlularının kişisel verilerden elde ettiği hukuki, iktisadi ya da bireysel menfaatleri söz konusu olduğunda kişisel verilerin korunması hakkı sınırlandırılabilmektedir[111]. Burada veri sahibinin menfaatine üstünlük tanımak adına kişisel verilerin korunması hukukuna ilişkin düzenlemelerde kural olarak kişisel verilerin işlenmesinin yasak olduğu kaidesine yer verilebilir; ancak menfaatler arasında denge kurabilmek için bu kural istisnalar ile sınırlandırılabilir[112].

[106] Diğer teoriler için bkz. KÜZECİ, s. 63-64.
[107] AKSOY, s. 57; AYÖZER, s. 16; KÜZECİ, s. 60; TAŞTAN, s. 55.
[108] AKKURT, **Kişisel Veri,** s. 24.
[109] AKSOY, s. 61; AYÖZER, s. 17; KÜZECİ, s. 62; TAŞTAN; s. 58.
[110] AKSOY, s. 54; AYÖZER, s. 15; KÜZECİ, s. 65; TAŞTAN; s. 59.
[111] ÇEKİN, s. 15-16.
[112] ÇEKİN, s. 16-17.

Gerek Tüzük'te gerek Türk hukukunda gerekse mukayeseli hukukta bu menfaat dengesi kanun koyucu tarafından gözetilmiştir[113].

1.3. KİŞİSEL VERİLERİN KORUNMASI HUKUKUNA İLİŞKİN HUKUKSAL DÜZENLEMELERİN TARİHSEL SÜRECİ

1.3.1. Uluslararası Düzenlemeler

1.3.1.1. Avrupa İnsan Hakları Sözleşmesi Kapsamında Kişisel Verilerin Korunması

Kişisel verilerin korunması Avrupa İnsan Hakları Sözleşmesi'nde ayrıca ve özel olarak düzenlenmemiş olup "Özel Yaşama ve Aile Yaşamına Saygı Hakkı" başlığı taşıyan Sözleşme'nin 8. maddesi kapsamına girmektedir. Kişisel verilerin korunması temelde özel hayatın gizliliği hakkına dayanmaktadır ve özel hayat birçok hukuk metninde temel insan haklarından biri olarak kabul edilmiştir. Kişisel verilerin AİHS'nin 8. maddesi kapsamında ele alınması, kişisel verilerin mahremiyete ilişkin olan insan özel yaşamının bir parçasını teşkil ettiğini de göstermektedir. Sözleşme'nin 8. maddesi;

> *"1.Herkes, özel yaşamına ve aile yaşamına, konutuna ve haberleşmesine saygı gösterilmesi hakkına sahiptir.*
>
> *2. Bu hakkın kullanılmasına bir kamu makamı tarafından, ulusal güvenliğin, kamu emniyetinin ya da ülkenin ekonomik refahının yararı, suçun ya da düzensizliğin önlenmesi, sağlığın ya da ahlakın korunması için yahut başkalarının haklarının ve özgürlüklerinin korunması için, hukuka uygun olarak yapılan ve bir demokratik toplumda gerekli bulunanlar hariç, hiçbir müdahale olmayacaktır.*" şeklinde düzenlenmiştir.

Madde metninde özellikle kişisel verilerin korunmasına ilişkin bir ibare yer almayıp bireyin "özel yaşamı", "aile yaşamı", "konutu" ve "haberleşmesi" güvence altına alınmıştır. Kişisel verilerin 8. madde kapsamında ele alınmasını Avrupa İnsan

[113] ÇEKİN, s. 16.

Hakları Mahkemesi kararları ile tespit etmek mümkündür. AİHM, Sözleşme'nin uygulanmasında denetleyici mekanizma olarak var olup Sözleşme'de yer alan hakların ihlali iddiasını incelemek ile görevlidir ve uygulamada koruyucu ve yol gösterici mekanizma konumundadır. AİHM verdiği kararlarında kişisel verilerin özel yaşamın içinde olduğunu kabul etmekte ve kişisel verilerin ihlaline ilişkin başvuruları Sözleşme'nin 8. maddesi kapsamında incelemektedir.

Sözleşme'nin 8. maddesinin 1. fıkrasında düzenlenen hak, mutlak olmayıp yine aynı maddenin 2. fıkrasında bu hakkın sınırları sayılmıştır. Buna göre müdahale 2. fıkrada sayılan amaçlara yönelik ise, yasal bir temeli var ise ve demokratik toplum için gerekli ise meşru kabul edilmelidir. Ancak AİHM kararlarına göre müdahaleyi meşru gören hâller dar yorumlanmalı ve suiistimale sebebiyet vermemek adına yasada müdahalenin usul ve şartları belirlenmeli; müdahale bağımsız bir denetim organının denetimine tabi olmalı ve her koşulda müdahalenin demokratik bir toplum için gerekli olup olmadığı sorusuna cevap aranmalıdır[114].

Mahkeme'nin kişisel verilerin korunmasına ilişkin verdiği ilk kararı olması ve iletişimin denetlenmesine yönelik önemli değerlendirmeler içermesi nedeniyle *"Klass ve Diğerleri"* kararı önem arz etmektedir. 6 Eylül 1978 tarihli kararda başvuru sahipleri başsavcı Gerhard Klass, avukat Peter Lübberger, yargıç Jürgen Nussbruch, avukat Hans-Jürgen Pahl ve avukat Dieter Selb, Federal Almanya'da kabul edilen ve posta, mektup ve telekomünikasyon yoluyla yapılan iletişimin ilgililere haber vermeksizin gizli bir biçimde denetlenmesine olanak sağlayan 1968 tarihli yasanın, Sözleşme'nin 6., 8. ve 13. maddesine aykırı olduğu gerekçesiyle başvuruda bulunmuşlardır[115]. Başvuru öncelikle Avrupa İnsan Hakları Komisyonu'nca incelenmiş ve Komisyon başvuruya ilişkin gerek "adil yargılanma hakkı"nın düzenlendiği 6. madde, gerek "özel ve aile hayatına saygı hakkı"nın düzenlendiği 8. madde, gerekse "etkili başvurma hakkı"nın düzenlendiği 13. madde bakımından ihlalin söz konusu olmadığı kanaatine varmıştır. Komisyon daha sonra başvuruyu incelemesi için Avrupa İnsan Hakları Divanı'na sunmuştur. Divan kararında

[114] KÜZECİ, s. 142.
[115] Mehmet Aydoğan ÖZMAN, **"Avrupa İnsan Hakları Divanı'nın 1978 Yılında Verdiği Kararlar"**, AÜHFD, C.35, 1978, s. 209.

başvuruya konu yasa ile kişinin özel yaşamı, aile yaşamı ve haberleşmesine saygısı gösterilmesi haklarına müdahale edildiğini kabul etmekle beraber esas olarak bu müdahalenin 8. maddenin 2. fıkrası kapsamında gerekli olup olmadığı hususunda incelemesini yürütmüştür. Divan, başvuruya konu kişiler arasındaki telekomünikasyon yoluyla sağlanan iletişimin devlet tarafından denetlenmesine imkân veren yasanın; devletlerin ulusal güvenliğin temini, kamu düzeninin sağlanması ve suçla mücadele kapsamında ancak demokratik toplum düzeninin korunması amacıyla meşru sayılabileceğine karar vermiştir. İletişimin denetlenmesinin ilgiliye bildirilmemesi bakımından ise bu uygulamanın yasanın korumayı amaçladığı ulusal güvenlik, kamu düzeni ve suçla mücadele bakımından bir gereklilik olduğu ve gözetlemede gizliliğin önemli bir husus olup aksi takdirde gözetleme sistemi ile hedeflenen amacın riske gireceği belirtilmiştir.

AİHM kişisel verilerin korunması bağlamında taraf devletlere Sözleşmeye aykırı olarak kişilerin özel yaşamına keyfi müdahale etmemek, kişisel verileri Sözleşmeye uygun olarak toplamak, saklamak ve işlemek negatif yükümlülüğünün yanında; devletlere kişisel verilen gizliliğini ve güvenliğini koruma altına alacak düzenlemeler yapmak ve ihlali önleyecek önlemler almak pozitif yükümlülüğünü de getirmektedir.

I. v. Finlandiya kararı kişisel verilerin korunması hakkında devletin pozitif yükümlülüğüne ilişkin önemli bir karardır. Karara konu olayda HIV virüsü taşıyan bir kimsenin bilgilerine yalnızca ilgili birimde çalışan hastane çalışanlarının değil ilgili birim haricindeki diğer çalışanların da erişebilmesi, tıbbi verilerin gizliliğinin ihlali sonucunu doğurmuştur. Mahkeme bu kararında devletlerin, kişilerin tıbbi verilerinin gizliliğine saygı göstermek zorunda olduğunu vurgulamıştır. Özellikle bulaşıcı hastalıklar konusunda tıbbi verilerin gizliliğinin ihlali hâlinde bulaşıcı hastalığa sahip kimseler, kişisel bilgilerini vermek istemeyeceği için tıbbi yardım yoluna başvurmaktan da kaçınacaktır. Bu husus hem bulaşıcı hastalık sahibi kimselerin sağlığı hem de toplum sağlığı yönünden tehlike arz edeceğinden önemli sonuçlar doğuracağı muhakkaktır[116]. Mahkeme bu karar ile kişisel verilerin korunması ve muhtemel

[116] Anayasa Mahkemesi, 28.09.2017 Tarih ve E.2016/125, K.2017/143 sayılı Kararı: *"AİHM'nin kararlarında da kişisel sağlık verilerine izinsiz erişilmesine karşı etkin ve somut bir korumanın önemi vurgulanarak kamu kurumları ve devletin bu verilerin gizliliğini güvence altına alabilmek için kişisel verileri koruyacak kuralları yürürlüğe koyma ve gerekli güvenceleri sağlama yükümlülüğü altında*

zararların önlenmesi bakımından Finlandiya mevzuatında yeterli güvencenin sağlanmadığı ve gerekli önlemlerin alınmadığı gerekçesiyle devletin pozitif yükümlülüğünün ihlal edildiğine karar vermiştir.

1.3.1.2. OECD Rehber İlkeler

II. Dünya Savaşı'nda zarar gören Avrupa ekonomisini yeniden canlandırmak amacıyla ABD ile Kanada'nın ortaya koydukları Marshall Planı kapsamında 1948 yılında OEEC (Avrupa Ekonomik İşbirliği Örgütü) kurulmuştur. 1961 yılında ise 14 Aralık 1960 tarihinde imzalanan Paris Sözleşmesi'ne dayanılarak OEEC'nin devamı niteliğinde küresel ticaretin refahını sağlamak için çalışmalar yapmak üzere OECD (Ekonomik İşbirliği ve Kalkınma Örgütü) kurulmuştur. Kişisel verilerin korunması konusunda uluslararası kuruluşlar tarafından ilk hukuki belgeyi de OECD yürürlüğe koymuştur. OECD bu anlamda "Özel Yaşamın Gizliliğinin ve Sınır Ötesi Kişisel Veri Dolaşımının Korunmasına İlişkin Rehber İlkeler"i 23.09.1980 tarihinde kabul etmiştir. OECD Rehber İlkeleri üye devletler bakımından bir tavsiye niteliğinde olup bağlayıcılığı yoktur; ilkeleri iç hukuk düzenlerine aktarıp aktarmamak konusu ülkelerin kendi inisiyatiflerine bırakılmıştır[117].

OECD üye devletlere belirlediği ilkeleri iç hukuklarına aktarıp aktarmama konusunda serbesti tanıdığı gibi; ülkelere kendi iç hukuklarında kişisel verileri koruma altına alan düzenlemeler hazırlarken içeriğin oluşturulmasında bu ilkelerin en azından benimsenmiş olmasını ve bundan daha kapsamlı bir koruma mekanizması ortaya konması gerektiğini belirtmektedir[118]. Bir başka ifade ile ilkeler adında geçtiği üzere gerçek anlamda "rehber" niteliğinde olup ülkelere kendi mevzuatlarını oluşturmada yol gösterici bir misyon konumundadır.

---

olduğu ifade edilmiş ve kişisel sağlık verilerini saklamakta başarısız olunması veya bu bilgilere erişime engel olacak güvenli ve sağlam bir sistem kurulamamasının AİHS'nin ihlali olarak değerlendirildiği görülmektedir." http://kararlaryeni.anayasa.gov.tr/Karar/Content/0556eb9f-017d-4dc4-9060-0e95c999ccd0?excludeGerekce=False&wordsOnly=False (Erişim:07.08.2019).

[117] Hayrunnisa ÖZDEMİR, **Elektronik Haberleşme Alanında Kişisel Verilerin Özel Hukuk Hükümlerine Göre Korunması**, Ankara, 2009, s. 23.

[118] KÜZECİ, s. 114.

Rehber ilkeler sekiz adettir ve şunlardır:[119]

1. Veri toplamanın sınırlı olması ilkesi (Collection limitation principle): Kişisel verilerin toplanması sınırlamaya tabi olmalıdır. Kişisel veriler yasal olarak ve dürüst araçlarla toplanmalı ve gerektiğinde veri öznesinin bilgisi veya rızası ile toplanmalıdır.

2. Veri kalitesi ilkesi (Data quality principle): Kişisel veriler amacına uygun olmalı ve bu amaç için gerekli ölçüde, tam ve güncel olmalıdır.

3. Amacın belirliliği ilkesi (Purpose specification principle): Kişisel veriler toplanırken ne amaç ile toplandığı belirli olmalıdır ve bu amaç haricinde kullanılmamalıdır. Verilerin toplanma amacı değiştirilecek ise bu değişiklik eskisi ile uyumlu olmalı ve muhakkak veri öznesine haber verilmelidir.

4. Kullanımın sınırlı olması ilkesi (Use limitation principle): Kişisel veriler, veri öznesinin rızası olmadıkça veya kanun izin vermedikçe açıklanamamalı, erişime sunulmamalı ve 9. paragrafta belirtilen (Amacın belirliliği ilkesi) amaç haricinde kullanılmamalıdır.

5. Veri güvenliği ilkesi (Security safeguards principle): Kişisel veriler kaybolma, yetkisiz erişim, imha, kullanılma, değiştirilme veya ifşa edilme gibi risklere karşı gerekli güvenlik önlemleriyle korunmalıdır.

6. Açıklık ilkesi (Openness principle): Kişisel veriler hususundaki gelişmeler, uygulamalar ve politikalar hakkında genel açıklık politikası olmalıdır. Kişisel verilerin toplanmasında, kullanımlarının asıl amaçları belirtilmeli ve veri sorumlusunun kimliği ve mutat meskeniyle birlikte kolaylıkla bilinebilir olmalıdır.

7. Bireyin katılımı ilkesi (Individual participation principle): Veri öznesi, veri sorumlusunda kendisi ile ilgili verilerin mevcut olup olmadığının teyit edilmesini isteme hakkına sahip olmalıdır. Veri öznesi, hakkındaki verileri makul bir sürede, gerekirse aşırı olmayan bir ücret ile makul bir şekilde ve kolayca anlaşılabilir bir formda öğrenebilme hakkına sahiptir. Bu hakkın kullanımının reddedilmesi hâlinde veri öznesi, talebinin red gerekçesinin açıklanmasını isteme ve bu karara karşı hukuki yollara başvurabilme hakkına da sahiptir. Ayrıca itirazda bulunup da başarılı olması

[119]Recommendation of the Council concerning Guidelines governing the Protection of Privacy and Transborder Flows of Personal Data (2013), (Çevrimiçi) https://www.oecd.org/sti/ieconomy/2013-oecd-privacy-guidelines.pdf (Erişim:08.09.2019).

hâlinde; hakkındaki verilerin silinmesini, düzeltilmesini, eksikliklerin tamamlanmasını veya değişiklik yapılmasını isteyebilir.

8. Hesap verilebilirlik ilkesi (Accountability principle): Veri sorumlusu belirtilen ilkelere etki eden tedbirlere uymak bakımından hesap verebilir durumda olmalıdır.

Türkiye'de de 6698 sayılı Kişisel Verilerin Korunması Kanunu'nun gerekçesinde OECD Rehber İlkeler'e atıfta bulunulmuştur[120].

1.3.1.3. 108 Sayılı "Kişisel Verilerin Otomatik İşleme Tabi Tutulması Karşısında Bireylerin Korunması Sözleşmesi" ve 181 Sayılı Ek Protokol

Kişisel verilerin korunmasına ilişkin uluslararası alanda ilk ve bağlayıcı olan 108 sayılı "Kişisel Verilerin Otomatik İşleme Tabi Tutulması Karşısında Bireylerin Korunması Sözleşmesi", Avrupa Konseyi tarafından 28 Ocak 1981 tarihinde kabul edilmiş ve imzaya açılmış; Sözleşmenin yürürlüğe girebilmesi için beş devlet tarafından onaylanma şartının yerine getirilmesiyle 1 Ekim 1985 tarihinde yürürlüğe girmiştir[121]. Sözleşme yalnızca Konsey üyesi ülkelerin değil, Konsey üyesi olmayan ülkelerin de katılımına açıktır[122].

Türkiye 108 sayılı Sözleşme'yi 1981 yılında imzalamış olmasına karşın 31.01.2016 tarihinde kabul edilen 6669 sayılı Kişisel Verilerin Otomatik İşleme Tabi Tutulması Karşısında Bireylerin Korunması Sözleşmesinin Onaylanmasının Uygun Bulunduğuna Dair Kanun ile onaylanmasını uygun bulmuş ve 108 sayılı Sözleşme 18.02.2016 tarih ve 29628 sayılı Resmi Gazete'de yayınlanarak yürürlüğe girmiştir[123]. Sözleşme'nin 4. maddesiyle Sözleşme'ye taraf devletlere metinde yer alan ilkelere kendi iç hukuklarında işlerlik kazandırmak amacıyla gerekli önlemleri alma

---

[120] Kişisel Verilerin Korunması Kanunu Tasarısı (1/541) ve Adalet Komisyonu Raporu, s. 6.

[121] Songül ATAK, "**Avrupa Konseyi'nin Kişisel Veriler Açısından Sağladığı Temel Güvenceler"**, TBB Dergisi, S.87, 2010, s.92; Aydın AKGÜL, **Danıştay ve Avrupa İnsan Hakları Mahkemesi Kararları Işığında Kişisel Verilerin Korunması,** İstanbul, 2014, s. 187.

[122] 108 sayılı Sözleşme'yi imzalayan ve onaylayan ülkeler listesi için bkz. https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/108/signatures (Erişim:10.10.2020) .

[123] 6669 sayılı Kanun metni için bkz. https://www.resmigazete.gov.tr/eskiler/2016/02/20160218-2.pdf (Erişim:10.10.2020).

yükümlülüğü getirilmiştir[124]. Türkiye'de, Sözleşme'nin imzalanmasından uzun bir süre sonra onaylanmasının sebebi kişisel verilerin korunmasına ilişkin yasanın 108 sayılı Sözleşme'den çok sonra yürürlüğe girmiş olmasıdır[125].

108 sayılı Sözleşme'de kişisel verilerin korunması alanında denetleyici veri koruma otoritelerinin belirlenmesine ve uluslararası veri aktarımına ilişkin bazı düzenleyici eklemeler yapılarak Sözleşme'nin uygulama alanı 181 sayılı Ek Protokol ile genişletilmiştir[126]. 2001 yılında imzaya açılarak beş taraf devletin onaylaması ile 2004 yılında yürürlüğe giren Protokol, Türkiye'de 5 Mayıs 2016 tarih ve 29703 sayılı Resmî Gazete'de yayınlanan 6705 sayılı Kanun ile onaylanması uygun bulunarak iç hukuka dâhil edilmiştir[127]. Türkiye'nin Protokolü 2001 yılında imzalamasına rağmen 2016 yılında onaylayarak iç hukuka dâhil etmesinin nedeni ise uzunca bir süre denetleyici otoritenin kurulamamış olmasıdır.

1.3.1.4. Avrupa Birliği Veri Koruma Yönergesi

Avrupa Birliği nezdinde veri koruma hukukuna yönelik birleştirici ve uyumlaştırıcı bir yasal düzenlemeye olan ihtiyacın sonucu olarak Avrupa Parlamentosu ve Avrupa Konseyi, 24 Ekim 1995 tarihinde 95/46 sayılı Kişisel Verilerin İşlenmesi ve Serbest Dolaşımı Bakımından Bireylerin Korunmasına İlişkin Yönerge'yi kabul etmiştir.

Avrupa Birliği Veri Koruma Yönergesi'nin kabul edilmesindeki amaç, kişisel verilerin korunmasına ilişkin üye ülkelerdeki ulusal mevzuatların birbiriyle uyumlu hâle getirilerek kişisel verilerin üye devletlerde aynı düzeyde ve temel ilkeler çerçevesinde korunması ve böylelikle herhangi bir güvenlik riski bulunmaksızın verilerin serbest dolaşımının sağlanmasıdır[128]. Bu doğrultuda AB'de kişisel verilerin

[124] ATAK, s. 94.
[125] 108 sayılı Sözleşme'yi yenileyen 18 Mayıs 2018 tarihli Değişiklik Protokolü için bkz. https://rm.coe.int/convention-108-convention-for-the-protection-of-individuals-with-regar/16808b36f1(Erişim:10.10.2020).
[126] ATAK, s. 120; TAŞTAN, s. 14.
[127] 6705 sayılı Kanun metni için bkz. https://www.resmigazete.gov.tr/eskiler/2016/05/20160505-1.htm (Erişim:10.10.2020).
[128] Yönerge m.1.

korunmasına ve verilerin sınırlar ötesinde serbest dolaşımına yönelik asgari veri koruma ölçütleri belirlenmiştir.

AB yasal sistemine göre yönergeler üye devletler açısından uyumlaştırma aracı niteliğindedir ve üye devletler açısından doğrudan geçerli kurallar getirmemektedir. Yönergeler üye devletler açısından ulaşılması gereken sonuç bakımından bağlayıcı olup buna ilişkin şekil ve yöntem seçimi ise ulusal otoritelere bırakılmıştır[129]. Üye devletlerin yönergelerde yer alan temel ilkeleri ulusal veri koruma düzenlemelerine derç etmeleri gerekmektedir[130]. Bu bağlamda üye devletler Yönerge'de belirtilen amaçlar doğrultusunda iç hukuklarında düzenleme yapma yetkisine sahip olmakla birlikte bu yetki üye devletlerin takdirine bırakılmıştır[131]. Esasında Yönerge'nin kabulü ile üye devletlere kendi ulusal veri koruma düzenlemelerini Yönerge ile uyumlu hâle getirme görevi verilmiş olmaktadır. Yönerge'nin üye devletlerin iç hukuklarında doğrudan geçerli olmaması ve üye devletlerin ulusal yasalarına Yönerge hükümlerini aktarım konusunda şekil ve yöntem bakımından takdir yetkisine sahip olması, uygulamada veri koruma hukukunda yeknesaklığın sağlanamamasına ve birbirinden farklı veri koruma kurallarının oluşturulmasına yol açmıştır[132].

1.3.1.5. Avrupa Birliği Genel Veri Koruma Tüzüğü

Avrupa Birliğinde yeknesak bir veri koruma kültürünün oluşturulması amacıyla her ne kadar Avrupa Birliği Veri Koruma Yönerge'si kabul edilmiş olsa da, zaman içerisinde bu hedefe tam anlamıyla ulaşılamadığı ve üye ülkelerin Yönerge'ye istinaden hazırladıkları ulusal veri koruma yasalarının birbiriyle örtüşmediği anlaşılmıştır[133]. Bu durum hukuk güvenliği açısından olumsuz sonuçlar doğmasına

---

[129] Sanem BAYKAL / İlke GÖÇMEN**, "Avrupa Birliği Hukukunun Kaynakları Bakımından Normlar Hiyerarşisi",** Prof.Dr.Erdal Onar'a Armağan, Ankara, 2013, s. 325.

[130] **Handbook on European Data Protection Law,** Publications Office of the European Union, Lüksemburg, Nisan 2018, s. 30.

[131] Yönergenin ulusal hukuka aktarılmasının şekil ve yöntemini seçmede üye devletlere serbestiyet tanınmış olup üye devletlerin yönergeleri iç hukuka aktarmalarında tamamen serbest olduklarından bahsedilemez. Üye devletlerin birtakım şartlara uymaları gerekmektedir. Ayrıntılı bilgi için bkz. Mehmet Hanifi BAYRAM, **Avrupa Birliği Hukuku Dersleri**, 4.Baskı, Ankara, 2019, s. 166.

[132] Nilgün BAŞALP, "**Avrupa Birliği Veri Koruması Genel Regülasyonu'nun Temel Yenilikleri",** MÜHF-HAD, C.21, S.1, 2015, s. 82.

[133] AB üye ülkelerinde veri koruma alanında yeknesak bir hukuk düzeni oluşturulamadığına Google Street View örnek verilebilir. Google, Street View uygulamasından ötürü AB üyesi ülkelerde birçok soruşturmaya uğramış ancak üye ülkelerin ulusal veri koruma mevzuatları uyarınca aynı konuya ilişkin

sebebiyet vermiş; veri koruma düzeyinin ülkeden ülkeye farklılık göstermesi özellikle veri transferi konusunda veri koruma düzeyi daha düşük üye devletlerin tercih edilmesine neden olmuştur.

Öte yandan teknolojinin azami ölçüde kullanılır hâle gelmesi, bu kullanım ile beraber kişisel verilerin işlendiği ve kullanıldığı mecraların artması ve nihayetinde elde edilen kişisel verilerin depolanması ve analizi yoluyla yaratılan kullanıcı profillerinin davranışsal reklamcılık faaliyetlerinin en önemli kaynağı hâline gelmesi, kişisel verileri dijital çağın modern para birimine dönüştürmüştür. Bilgi ve iletişim teknolojilerinin kullanımının yaygınlaşması kişisel verilere atfedilen maddi ve manevi değerin artmasına sebep olmuş; bu durum ise mevcut veri koruma kurallarının güncellenmesini ve veri koruma hukukunda birtakım yenilikler yapılmasını zorunlu kılmıştır.

Veri koruma hukukunda yapılacak yeni düzenlemeye ilişkin AB yasama süreçleri dâhilinde iki ihtimal gündeme gelmiştir. Bunlardan ilki 95/46 sayılı Yönerge gibi yeni bir yönergenin hazırlanması iken diğer seçenek ise yeni bir AB Tüzüğü hazırlanması ihtimalidir[134]. AB Komisyonu bu ihtimallerden ikincisi olarak belirttiğimiz veri koruma hukuku alanında yeni bir tüzük hazırlanması ihtimaline yatkın olduğunu belirtmiş; nihayetinde kabul edilecek metnin hukuki tasarruf türü olarak da tüzük belirlenmiştir[135]. Yukarıda izah ettiğimiz üzere 95/46 sayılı Yönerge'nin eleştirilme sebeplerinden birisi de hukukun yeknesaklaştırılması amacına hizmet etmediğidir[136]. Bu husus gözetilerek kabul edilecek yeni düzenlemenin bütünüyle bağlayıcı ve üye devletler açısından doğrudan uygulanabilir bir hukuki tasarruf türü[137] olan tüzük şeklinde kabul edilmesi isabetli bir tercihtir.

---

birbirinden farklı kararlar verilmiştir. Bkz. https://www.theguardian.com/technology/2009/apr/23/google-street-view-data-protection-cleared; https://www.bbc.com/news/technology-11595495 (Erişim:31.10.2020).

[134] BAŞALP, **Regülasyonun Temel Yenilikleri,** s. 83.

[135] Francoise GILBERT, **"European Data Protection 2.0: New Compliance Requirements in Sight - What the Proposed EU Data Protection Regulation Means for U.S. Companies",** Santa Clara High Tech. L.J., C.28, S.4, 2012, s. 823.

[136] BAŞALP, **Regülasyonun Temel Yenilikleri,** s. 85.

[137] BAYKAL / GÖÇMEN, s. 325.

Birlik tarafından kişisel verilerin korunmasında yeknesak bir veri koruma kültürü geliştirilerek hukuk güvenliğinin sağlanması, Yönerge'den farklı olarak çok daha fazla detaylandırılmış ve Yönerge'nin kabul edilmesinden sonra gelişen bilgi ve iletişim teknolojileri de düşünülerek güncel ve kapsayıcı bir çalışma yapılması amacıyla 2012 yılının başlarında Tüzük çalışmasına başlanmıştır. Avrupa Komisyonu, Avrupa Konseyi ve Avrupa Parlamentosu tarafından 4 yıl boyunca yapılan Tüzük görüşmeleri nihayet tamamlanmış[138] ve "2016/679 Sayılı Avrupa Birliği Genel Veri Koruma Tüzük'ü" 4 Mayıs 2016 tarihinde AB Resmi Gazetesi'nde yayınlanmış; 25 Mayıs 2018 tarihinden itibaren ise Yönerge'yi ilga etmek suretiyle uygulanmaya başlanmıştır.

Tüzük'ün yer bakımından uygulama alanı Yönerge'ye göre genişletilmiştir. Tüzük'ün yer bakımından uygulama alanı 3. maddede düzenlenmiş olup m.3/f.1 hükmüne göre; *"Tüzük, işleme faaliyeti Birlik içerisinde gerçekleşip gerçekleşmediğine bakılmaksızın, Birlik içerisindeki bir veri sorumlusu veya veri işleyenin işletmesinin faaliyetleri bağlamında kişisel verilerin işlenmesine uygulanır."*. Tüzük'ün AB sınırları dışında da uygulama alanı bulacağına ilişkin düzenleme ise 2. fıkrada yer almaktadır. Buna göre Tüzük'ün uygulanması iki şekilde gerçekleşecektir. İlk olarak Tüzük m.3/f.2 (a) bendine göre, şirket merkezi ve faaliyet alanı AB'de bulunmayan bir veri sorumlusu veya veri işleyenin –ilgili kişinin ödeme yapmasına gerek olup olmadığına bakılmaksızın- AB'de bulunan ilgili kişilere bir mal veya hizmet sunması hâlinde Tüzük uygulama alanı bulacaktır[139]. İkinci olarak Tüzük m.3/f.2 (b) bendine göre, işleme faaliyetinin AB'de bulunan ilgili kişilerin Birlik içerisindeki davranışlarının izlenmesine ilişkin olması hâlinde de Tüzük uygulama alanı bulacaktır. Bu bent ile Birlik dışında merkezi olan sosyal medya şirketlerinin hedef alındığı belirtilmektedir[140]. Dolayısıyla AB temelli bir düzenleme olan Tüzük'ün coğrafi olarak uygulama alanının AB sınırlarını aştığı söylenebilir[141].

[138] TAŞTAN, s. 17.
[139] DEVELİOĞLU, s. 17.
[140] Murat Volkan DÜLGER, "**Avrupa Birliği Genel Veri Koruma Tüzüğü Bağlamında Kişisel Verilerin Korunması",** Yaşar Hukuk Dergisi, C.1, S.2, 2019, s. 96.
[141] DÜLGER, **Tüzük Bağlamında Koruma,** s. 94.

1.3.2. Ulusal Düzenlemeler

1.3.2.1. Genel Olarak

Uluslararası düzenlemelerin aksine ülkemizde kişisel verilerin tarihçesinin uzun bir geçmişe sahip olduğu söylenemez[142]. Bilgi ve iletişim teknolojilerinin gelişmesiyle globalleşen dünyada bütün dünyayı saran veri ağı, beraberinde kişisel verilerin hukuk düzeninde korunmasına olan ihtiyacı da beraberinde getirmiş ve bu ihtiyacın bir sonucu olarak 1970'lerden günümüze özellikle Avrupa'da birçok hukuki düzenleme yapılmıştır[143]. Türkiye, teknolojideki gelişmeleri yakından izleyen, internet kullanımı ve bu ortamdaki Türkçe içeriklerin hızla arttığı bir ülke olmasına rağmen kişisel verilerin korunmasına ilişkin hukuki düzenlemelerin uzun bir geçmişe sahip olduğunu söylemek mümkün değildir[144]. Kişisel verilerin korunması, ülkemizde ilk kez[145] 06.02.2004 tarih ve 25365 sayılı Resmi Gazete'de yayınlanan Telekomünikasyon Sektöründe Kişisel Bilgilerin İşlenmesi Ve Gizliliğinin Korunması Hakkında Yönetmelik ile bir mevzuat hükmünde yer almıştır[146].

Türkiye'de kişisel verilerin korunması 2010 yılında 5982 sayılı Kanun'un 2. maddesi ile Anayasa'nın 20. maddesine eklenen 3. fıkra hükmü ile anayasal bir hak hâline gelmiştir[147]. Buna göre *"Herkes, kendisiyle ilgili kişisel verilerin korunmasını isteme hakkına sahiptir. Bu hak; kişinin kendisiyle ilgili kişisel veriler hakkında bilgilendirilme, bu verilere erişme, bunların düzeltilmesini veya silinmesini talep etme ve amaçları doğrultusunda kullanılıp kullanılmadığını öğrenmeyi de kapsar. Kişisel*

---

[142] Kemal ATASOY, **"Kişilik Hakkı Kapsamında Sosyal Medyada Kişisel Verilerin Korunması ve Veri Sahibinin Rızası",** Marmara Üniversitesi Hukuk Fakültesi Hukuk Araştırmaları Dergisi, C.22, S.3, 2016, s. 278.

[143] Avrupa'da kişisel verilerin korunmasına ilişkin ilk hukuki düzenleme 7 Ekim 1970 tarihli Almanya'nın Hessen Eyaleti'ne ait Kişisel Verilerin Korunması Kanunu'dur. Ayrıntılı bilgi için bkz. ÇEKİN, s. 5.

[144] KÜZECİ, s. 275.

[145] TAŞTAN, s. 23.

[146] Yönetmelik metni için bkz. https://www.resmigazete.gov.tr/eskiler/2004/02/20040206.htm#10 (Erişim:03.11.2020) Söz konusu Yönetmelik 24.07.2012 tarih ve 28363 sayılı Resmi Gazete'de yayınlanan Elektronik Haberleşme Sektöründe Kişisel Verilerin İşlenmesi Ve Gizliliğinin Korunması Hakkında Yönetmelik'in 23. maddesi ile yürürlükten kaldırılmıştır.

[147] Kişisel Verileri Koruma Kurumu, "6698 Sayılı Kişisel Verilerin Korunması Kanununun Uygulanmasına Yönelik Soru Cevaplar", Ankara, 2017, s.11 (Çevrimiçi) https://www.kvkk.gov.tr/yayinlar/6698%20SAYILI%20K%C4%B0%C5%9E%C4%B0SEL%20VER%C4%B0LER%C4%B0N%20KORUNMASI%20KANUNUNUN%20UYGULANMASINA%20Y%C3%96NEL%C4%B0K%20SORU%20VE%20CEVAPLAR.pdf (Erişim:03.11.2020).

veriler, ancak kanunda öngörülen hâllerde veya kişinin açık rızasıyla işlenebilir. Kişisel verilerin korunmasına ilişkin esas ve usuller kanunla düzenlenir.". 2010 yılında kişisel verilerin korunmasına temel hak ve özgürlükler içerisinde Anayasa'da ayrıca bir yer verilinceye kadar kişisel verilerin korunmasına dayanak olacak birtakım anayasal hükümler 2010 yılı öncesinde de mevcut idi[148]. Hukuk devleti ilkesi (m.2), kişinin maddi ve manevi varlığını koruma ve geliştirme hakkı (m.17), özel yaşamın gizliliği hakkı (m.20), konut dokunulmazlığı (m.21), haberleşmenin gizliliği (m.22), dini ve vicdani kanaatleri açıklamaya zorlanamama (m.24), düşünce ve kanaat hürriyeti (m.25) kişisel verilerin korunmasının normatif temelini oluşturan anayasal hükümlere örnek olarak verilebilir[149].

Kişisel verilerin korunmasına ilişkin kanun düzeyinde ilk düzenleme ise 2005 yılında yürürlüğe giren 5237 sayılı Türk Ceza Kanunu'nda kişisel verilere karşı suçlar ihdas edilmek suretiyle yapılmıştır[150]. 5237 sayılı TCK'nın *"Kişilere Karşı Suçlar"* başlıklı ikinci kısmının *"Özel Hayata ve Hayatın Gizli Alanına Karşı Suçlar"* başlıklı dokuzuncu bölümünde doğrudan kişisel verilerin korunmasına ilişkin birtakım suçlar düzenlenmiş ve cezai yaptırıma bağlanmıştır. Buna göre *kişisel verilerin hukuka aykırı olarak kaydedilmesi* (m.135), *hukuka aykırı olarak verilmesi veya ele geçirilmesi* (m.136) ve *kanunlarca belirlenen sürelerin geçmiş olmasına rağmen yok edilmemesi* (m.138) fiilleri suç olarak düzenlenmiştir.

Kişisel verilerin korunmasına ilişkin bu suçların karşılığı 765 sayılı mülga Türk Ceza Kanunu'nda yer almamakla beraber 1997, 2000 ve 2003 yıllarında hazırlanan TCK tasarılarında kişisel verilerin korunmasına ilişkin düzenlemelere yer verilmiştir[151]. Bu düzenlemelere ilişkin birtakım değişiklikler yapılarak nihayetinde kanun düzeyinde kişisel verilerin korunmasına ilişkin özel hükümlere 5237 sayılı TCK'da yer verilmiştir.

---

[148] KÜZECİ, s. 278.
[149] Doğan KILINÇ, "**Anayasal Bir Hak Olarak Kişisel Verilerin Korunması**", AÜHFD, C. 61, S.3, 2012, s. 1131; Ali Tarık GÜMÜŞ, **"Türk Anayasasında Kişinin Maddi ve Manevi Varlığını Koruma Ve Geliştirme Hakkı"**, SÜHFD, C. 13, S. 2, 2005, s. 137; KÜZECİ, s. 285-291.
[150] İbrahim KORKMAZ, **Kişisel Verilerin Ceza Hukuku Kapsamında Korunması**, 2.Baskı. Ankara, 2019, s. 375.
[151] KORKMAZ, s. 376.

Doğrudan kişisel verilerin korunmasına ilişkin özel hükümlere TCK m.135, m.136 ve m.138'de yer verilmiş olmakla beraber, kişisel verilere dolaylı olarak koruma sağlayan birtakım suç ve yaptırımlar da TCK'da hüküm altına alınmıştır. Bu çerçevede *haberleşmenin gizliliğini ihlal* (m.132), *kişiler arasındaki konuşmaların dinlenmesi ve kayda alınması* (m.133), *özel hayatın gizliliğini ihlal* (m.134), *ticari sır, bankacılık sırrı veya müşteri sırrı niteliğindeki bilgi veya belgelerin açıklanması* (m.239), *bilişim sistemine girme* (m.243), *sistemi engelleme, bozma, verileri yok etme veya değiştirme* (m.244), *göreve ilişkin sırrın açıklanması* (m.258) kişisel verilerin korunmasını dolaylı olarak sağlayan suçlar olarak zikredilebilir.

Belirtmek gerekir ki TCK'da her ne kadar kişisel verilerin hukuka aykırı olarak elde edilmesi, kaydedilmesi veya ifşa edilmesi fiilleri suç olarak düzenlenmiş ve yaptırıma bağlanmış olsa da kişisel verilere ilişkin teknik kavramların tanımlanmaması ve bu konuda özel bir kanunun bulunmaması, söz konusu fillerin ne zaman hukuka aykırı ne zaman hukuka uygun olduğu konusunda birtakım tereddütlerin yaşanmasına sebep olmuştur[152].

1.3.2.2. 6698 Sayılı Kişisel Verilerin Korunması Kanunu

Çalışmamızda kişisel verilerin korunması hukukunun tarihsel sürecine ilişkin "Uluslararası Düzenlemeler" başlığı altında açıklamaya çalıştığımız üzere, birçok uluslararası kuruluş ve başta AB üye ülkeleri olmak üzere birçok ülke tarafından kişisel verilerin korunmasına ilişkin hukuk metinleri yürürlüğe konulmuştur. Ancak AB üyelik süreci ile bağlantılı olarak birçok hukuk reformunun gerçekleştiği ülkemizde kişisel verilerin korunmasına ilişkin kapsayıcı bir yasal düzenlemenin olmayışı, iç hukukumuzun AB veri koruma mevzuatı ile uyumsuz hâle gelmesine sebebiyet vermiştir. Nitekim AB tarafından yayınlanan birçok Türkiye Ulusal İlerleme Raporu'nda bu hususa değinilmiş ve Türkiye'de veri korumasına ilişkin kanun boşluğuna dikkat çekilmiştir[153]. Ayrıca Avrupa Birliği'nin, üye devletler arasında veri koruması alanında uyumluluğun sağlanması amacıyla 95/46/EC sayılı Yönerge'yi

[152] Kişisel Verilerin Korunması Kanunu Tasarısı (1/541) ve Adalet Komisyonu Raporu, s. 5.
[153] BAŞALP, **Regülasyonun Temel Yenilikleri,** s. 80.

yürürlüğe koyması, Türkiye'nin de üyelik sürecinde AB ile uyumlu bir yasal düzenleme yapma gerekliliğini ortaya çıkarmıştır[154].

Ülkemizde kişisel verilerin korunmasını sağlayacak bir kanunun çıkarılmasında çeşitli sebepler etkili olmuştur. Temel olarak insan haklarının etkin bir biçimde korunması, AB üyelik süreci ve uluslararası alanda daha etkin ekonomik faaliyetlerde bulunma ihtiyacı bu sebepler arasında sayılabilir[155]. Bunun yanı sıra Kişisel Verilerin Korunması Kanunu'nun genel gerekçesinde de belirtildiği üzere, TCK'nın 135 vd. maddelerinde kişisel verilerin korunmasına yönelik birtakım suç ve yaptırımlar belirlenmiş olmasına rağmen konuya ilişkin yasal bir düzenleme bulunmaması sebebiyle bir fiilin ne zaman hukuka aykırı olduğunun belirlenmesinde güçlük yaşanması; Anayasa'nın 20. maddesi ile kişisel verilerin korunmasına ilişkin esas ve usullerin belirlendiği bir yasal düzenleme yapılması gerekliliğinin belirtilmesi; AB tam üyelik sürecinde müzakere fasıllarından dördünün doğrudan kişisel verilerle ilgili olması ve sürecin ilerleyebilmesi için ülkemizde kişisel verilerin korunmasına ilişkin temel bir kanunun yürürlüğe girmesinin gerekliliği; Avrupa Polis Teşkilatı (EUROPOL) ve AB üyesi ülkeler arasında yargısal işbirliğini sağlayan kurum olan EUROJUST ile operasyonel işbirliği ve elektronik bilgi paylaşımının yapılamaması; veri güvenliğine ilişkin kanuni dayanak olmaksızın sağlık kuruluşlarında hastalara ait özel nitelikli verilerin tutulması ve bu hususun AİHM ihlal kararlarına konu olması; Türkiye'de yaşayan yabancılar ile yurtdışında yaşayan Türk vatandaşları bakımından veri paylaşımında sorunlar yaşanması; yabancı sermayenin ülkemizde güvenle yatırım yapmasına yönelik ekonomik kaygılar kişisel verilerin korunmasına ilişkin özel bir kanun yapılmasını zorunlu kılmıştır[156].

Tüm bu sebepler ışığında uzun bir hazırlık ve yasama sürecinin ardından 18.01.2016 tarihinde TBMM Başkanlığına sunulan ''Kişisel Verilerin Korunması Kanun Tasarısı'' Adalet Komisyonu tarafından kabul edilerek 24.03.2016 tarihinde yasalaşmış; yasalaşan 6698 sayılı Kişisel Verilerin Korunması Kanunu ise 07.04.2016

---

[154] Türkay HENKOĞLU, **Bilgi Güvenliği ve Kişisel Verilerin Korunması**, Ankara, 2015, s. 82.
[155] Kişisel Verileri Koruma Kurumu, "Ulusal Ve Uluslararası Alanda Kişisel Verilerin Korunmasına Duyulan İhtiyaç", Ankara, 2017, s. 4 (Çevrimiçi) https://www.kvkk.gov.tr/SharedFolderServer/CMSFiles/8e39e0a1-6ec4-4179-a5d3-bbd8e78dce31.pdf (Erişim:08.11.2020).
[156] Kişisel Verilerin Korunması Kanunu Tasarısı (1/541) ve Adalet Komisyonu Raporu, s. 4-6.

tarih ve 29677 sayılı Resmi Gazete'de yayınlanarak yürürlüğe girmiştir. Son yıllarda kişisel verilerin korunmasının ehemmiyetinin anlaşılmasıyla ülkemizde bu alanda mevzuatta birtakım hükümlere[157] yer verilmiş olmasına rağmen temel ilkelerin benimsendiği kapsayıcı ve bütüncül ilk yasa 6698 sayılı Kanun'dur.

[157] Çeşitli mevzuat hükümlerinde yer alan kişisel verilere ilişkin düzenlemelere; 5070 sayılı Elektronik İmza Kanunu (m.12), 5809 sayılı Elektronik Haberleşme Kanunu (m.51, 55 ve 56), 6563 sayılı Elektronik Ticaretin Düzenlenmesi Hakkında Kanun (m.10), 4857 sayılı İş Kanunu (m.75), 5502 sayılı Sosyal Güvenlik Kurumu Kanunu (m.35), 6183 sayılı Amme Alacaklarının Tahsil Usulü Hakkında Kanun (m.107), 2559 sayılı Polis Vazife ve Salâhiyet Kanunu (m.5), 4982 sayılı Bilgi Edinme Hakkı Kanunu (m.21) ve benzer diğer normatif düzenlemeler örnek olarak verilebilir.

İKİNCİ BÖLÜM: VERİ KORUMA HUKUKUNUN TEMEL İLKELERİ VE UYUMLULUĞU ARTIRMAYA İLİŞKİN KURALLAR

2.1. VERİ KORUMA HUKUKUNUN TEMEL İLKELERİ

Kişisel verilerin işlenmesine ilişkin hukuki düzenlemelerde, veriler işlenirken esas alınması gereken temel ilkeler de hüküm altına alınmaktadır. Kişisel verilerin korunması hukuku temel ilkeler doğrultusunda şekillenmiş ve yapılan düzenlemeler bu ilkeler uyarınca tesis edilmiştir[158]. Bu ilkelerin varlığı tek başına bir veri işleme faaliyetini hukuka uygun hâle getirmemekle beraber ilkelere aykırı hareket edilmiş olması veri işleme faaliyetini hukuka aykırı hâle getirecektir[159]. Veri sorumluları ve veri işleyenler açısından, veri işleme faaliyetinin hukuka uygunluğunun sınırının belirlenmesinde de bu ilkeler yol gösterici olmaktadır.

6698 sayılı Kanun'da, uluslararası düzenlemeler ve 95/46/EC sayılı Yönerge ile paralel olacak şekilde genel ilkeler benimsenmiştir[160]. Çalışmamızda daha güncel olması ve Kanun'da yer alan ilkeleri kapsamakla beraber Kanun'da yer almayan yeni ilkelere de yer verilmiş olması sebebiyle Avrupa Birliği Genel Veri Koruma Tüzüğü'nde yer alan ilkelere değinilecektir. Bu ilkeler Tüzük'ün 5. maddesinde sayılmış olup bunlar, "*hukuka uygunluk, hakkaniyet ve şeffaflık", "amacın sınırlandırılması", "veri minimizasyonu", "doğruluk", "saklama süresinin sınırlandırılması", "bütünlük ve gizlilik"* ve *"hesap verilebilirlik"* ilkeleridir.

[158] TAŞTAN, s.47.
[159] ÇEKİN, s. 66.
[160] 6698 sayılı Kanun'un *"Genel İlkeler"* başlıklı 4. maddesinde, kişisel verilerin işlenmesinde uyulması gereken ilkeler sayılmıştır. Buna göre kişisel veriler hukuka ve dürüstlük kuralına uygun olarak işlenmeli, doğru ve gerektiğinde güncel olmalı, belirli, açık ve meşru amaçlar için işlenmeli, işlendikleri amaçla bağlantılı, sınırlı ve ölçülü olmalı, ilgili mevzuatta öngörülen veya işlendikleri amaç için gerekli olan süre kadar muhafaza edilmelidir.

2.1.1. Hukuka Uygunluk, Hakkaniyet ve Şeffaflık İlkesi

Veri işleme faaliyetinde hukuka uygunluğun sağlanması, kişisel verilerin veri sahibinin rızası veya Tüzük'ün 6 vd. maddelerinde sayılan hukuka uygunluk hâllerinden biri uyarınca işlenmesi hâlinde mümkün olur[161]. Tüzük m.6/f.1'de rızaya ek olarak; bir sözleşmenin ifa edilmesi, yasal yükümlülüğün yerine getirilmesi, veri sorumlusunun veya üçüncü bir kişinin meşru menfaatleri ya da gerektiğinde veri sahibinin veya başka bir kişinin hayati menfaatlerinin korunması, bir kamu otoritesinin görevini yerine getirmesi için kişisel verilerin işlenmesi durumunda meşru dayanağın var olacağı kabul edilmiştir[162].

Hakkaniyet ilkesi ise veri sahibi ile veri sorumlusu arasındaki ilişkiyi yönetmekte olup veri sorumlusunun kimliği konusunda dürüst olması, işleme faaliyetlerinin veri sahibinin makul karşılayacağı ve potansiyel risklerin farkında olacağı şekilde gizli olmaksızın gerçekleştirilmesi anlamına gelmektedir[163]. Ayrıca veri sorumlusu mümkün olduğu kadar, özellikle rızanın veri işleme için yasal dayanak oluşturduğu durumlarda, veri sahibinin isteklerine en uygun şekilde hareket etmelidir[164].

Yönerge'de ayrıca düzenlenmemiş olup Tüzük'te detaylı bir şekilde yer alan şeffaflık ilkesi ile veri sahibinin, kişisel verilerinin kim tarafından ve hangi amaçla işlendiğini her halükarda öğrenebilmesi amaçlanmıştır[165]. Tüzük'ün 12. maddesinde veri sahibine bilginin ne şekilde sağlanacağı, 13. ve 14. maddelerinde ise veri sahibine hangi bilgilerin sağlanacağı düzenlenmiştir.

Hukuka uygunluk ve hakkaniyet ilkesi 6698 sayılı Kanun'da[166] *"hukuka ve dürüstlük kurallarına uygun olma ilkesi"* olarak ifade edilmiştir. Kanun'da "*şeffalık ilkesi"* başlığıyla ayrıca düzenlenmemiş olmakla beraber Kanun'un m.4/f.2 (c) bendi

[161] Tüzük, Giriş Bölümü, par. 40; Handbook on European Data Protection Law, s. 117-118; IT Governance Privacy Team, **EU General Data Protection Regulation: An Implementation and Compliance Guide**, IT Governance Publishing, Birleşik Krallık, 2.Baskı, 2017, s. 57.
[162] Handbook on European Data Protection Law, s. 118.
[163] Handbook on European Data Protection Law, s. 118; IT Governance Privacy Team, s. 57.
[164] Handbook on European Data Protection Law, s. 118.
[165] DEVELİOĞLU, s. 44.
[166] 6698 sayılı Kanun m.4/f.2 (a) bendi.

ile m.10 ve m.11 hükümlerinde şeffaflık ilkesine ve buna bağlı koruma mekanizmasına yer verilmiştir[167].

2.1.2. Amacın Sınırlandırılması İlkesi

Amacın sınırlandırılması ilkesinin iki bileşeni olduğundan bahsedilebilir. Bunlardan ilki kişisel verilerin belirli, açık ve meşru amaçlar için toplanması iken ikincisi toplanan verilerin toplanma amacına uygun olmayan bir şekilde ve başka surette işlenemeyeceğidir[168]. Bu ilke ile veri sorumlusuna kişisel verileri nasıl kullanabileceklerinin sınırını belirleme yükümlülüğü getirilmiştir. Kişisel verilerin belirsiz ve/ya sınırsız amaçlarla işlenmesi hukuka aykırılık teşkil edecek olup[169] kişisel verilerin belirli bir amaç olmaksızın, *"bir gün gerekli olursa"*[170] düşüncesiyle işlenmesi ve depolanması[171] durumunda hukuka uygun bir veri işleme faaliyetinden bahsedilemeyecektir[172].

Amacın sınırlandırılması ilkesi, veri koruma önlemlerinin tasarlanmasında da önemli bir ilk adımdır[173]. Zira veri sorumlusu tarafından alınan güvenlik önlemlerinin yeterli olup olmadığına ilişkin değerlendirme, belirlenen amaca göre yapılacaktır[174].

Burada belirtilmesi gereken bir diğer husus ise söz konusu amacın veriler toplanırken, yani henüz veri işlenmeden, veri sahibine bildirilmesi gerektiğidir. Nitekim veri sahibinin neye onay verdiğini bilmesi gerekir[175]. Ayrıca Tüzük'te öngörülen düzenlemeler uyarınca kişisel verilerin, toplandığı amaç dışında işlenebilmesi için kural olarak veri sahibinin rızası aranmaktadır[176].

---

[167] ÇEKİN, s. 79.
[168] Article 29 Working Party, **"Opinion 03/2013 on Purpose Limitation",** WP203, 2 Nisan 2013, s. 4.
[169] Handbook on European Data Protection Law, s. 122.
[170] KÜZECİ, s. 203.
[171] Mesut Serdar ÇEKİN, **"6698 Sayılı Kişisel Verilerin Korunması Hakkında Kanun'un Big Data (Büyük Veri) ve İrade Serbestisi Açısından Değerlendirilmesi"**, İÜHFM, C. LXXIV, S.2, 2016, s. 637.
[172] Handbook on European Data Protection Law, s. 122; KÜZECİ, s. 203.
[173] Art. 29 Working Party, WP203, s. 4.
[174] ÇEKİN, s. 71.
[175] ÇEKİN, s. 71.
[176] Tüzük m.6/f.4.

Bu ilke 6698 sayılı Kanun'da[177] *"belirli, açık ve meşru amaçlar için işlenme ilkesi"* olarak ifade edilmiştir.

2.1.3. Veri Minimizasyonu İlkesi

Veri minimizasyonu ilkesi uyarınca verilerin toplanması ve/veya işlenmesi veri sorumlusunun meşru bir amacını yerine getirmek için en az seviyede, gerekli olanla sınırlandırılmalıdır ve kişisel veriler ancak işleme amacı başka yollar ile makul bir şekilde yerine getirilemediğinde işlenmelidir[178]. Bu çerçevede toplandıkları ve/veya işlendikleri amaçlarla ilgili olarak kişisel veriler yeterli, ölçülü ve gerekli olanla sınırlı olmalıdır. Dolayısıyla bu ilke, bir anlamda veri sorumlusunun meşru bir amacı yerine getirmek için gerekenden daha fazla veriyi tutmaması gerektiği anlamına gelmektedir[179]. Örneğin, bir şehirde toplu taşıma sistemini kullanmak isteyen kullanıcılara sağlanan çipli ulaşım kartında, kartın yüzeyinde ve çipte elektronik biçimde kullanıcının isminin yer alması veri minimizasyonu ilkesi ile bağdaşmamaktadır. Zira bir kişinin toplu taşıma olanaklarını kullanma izni olup olmadığı, kişilerin isminin yer almadığı ve kartın geçerli olup olmadığını teyit edecek barkod gibi özel bir elektronik görüntünün kullanılması yolu ile sağlanabilecek iken hangi taşıma aracını, kimin, hangi zamanda kullandığını kaydeden bir sistemin veri minimizasyonu ilkesine uygunluğundan bahsedilemez[180].

Çeşitli metinlerde yeterlilik ilkesi veya veri sadeleştirilmesi ilkesi olarak ifade edilen bu ilke, 6698 sayılı Kanun'da[181] *"işlendikleri amaçla bağlantılı, sınırlı ve ölçülü olma ilkesi"* olarak ifade edilmiştir.

---

[177] 6698 sayılı Kanun m.4/f.2 (c) bendi.
[178] Europen Data Protection Supervisor (EDPS), **"Opinion of the European Data Protection Supervisor on the Data Protection Reform Package"**, Brüksel, 07.03.2012, s. 20 (Çevrimiçi) https://edps.europa.eu/sites/edp/files/publication/12-03-07_edps_reform_package_en.pdf (Erişim:28.08.2020).
[179] IT Governance Privacy Team, s. 60.
[180] Handbook on European Data Protection Law, s. 126.
[181] 6698 sayılı Kanun m.4/f.2 (ç) bendi.

2.1.4. Doğruluk İlkesi

Doğruluk ilkesi uyarınca işlenen kişisel veriler doğru ve gerektiğinde güncel olmalıdır. Doğruluğun sağlanabilmesi amacıyla veriler düzenli olarak kontrol edilip güncel tutulmalı ve yanlış veriler gecikmeksizin silinmelidir[182]. Kişisel verilerin doğru ve gerektiğinde güncel bir şekilde işlenebilmesi için veri sorumlusunun gerekli tedbirleri alması ve veri sahibine kişisel verileri doğrulama ve güncelleme imkânı tanıması gerekmektedir[183].

Bu ilke ile hem veri sahibinin hem de veri sorumlusunun çıkarları korunmak istenmektedir[184]. Şöyle ki verisi işlenen veri sahibinin kişisel verilerinin yanlış olması veya eski olması bireyin temel hak ve özgürlüklerini, ekonomik çıkarlarını ve manevi bütünlüğünü zedeleyecek sonuçlar meydana getirebilecektir[185]. Veri sorumlusu bakımından değerlendirildiğinde ise kişisel verileri belirli bir amaç için işleyen veri sorumlusuna amacına ulaşmak için ancak doğru ve güncel veriler fayda sağlayabilir[186].

Doğruluk ilkesinin bir yansıması olarak Tüzük m.16'da ve 6698 sayılı Kanun'un m.11/f.1 (d) bendinde ilgili kişilere doğru olmayan kişisel verilerin düzeltilmesini talep etme hakkı tanınmıştır[187]. Buna göre belirtmek gerekir ki kişisel verilerin eksik veya yanlış işlenmiş olması veya işlenen kişisel verilerde bir değişiklik meydana gelmesi hâlinde ilgili kişi tarafından bu değişikliğin güncellenmesini talep etme hakkı, eksik kişisel verilerin tamamlanması hakkı ve yanlış ve/veya güncelliğini yitirmiş kişisel verilerin silinmesini veya düzeltilmesini talep etme hakkı söz konusu olacaktır[188].

---

[182] Handbook on European Data Protection Law, s. 127; IT Governance Privacy Team, s. 61.
[183] TAŞTAN, s. 50; IT Governance Privacy Team, s.61.
[184] *"Bu ilkeler arasında yer alan kişisel verilerin doğru ve gerektiğinde güncel bir şekilde tutulması, veri sorumlusunun çıkarına uygun olduğu gibi ilgili kişinin temel hak ve özgürlüklerinin korunması açısından da gerekli olup, veri sorumlusunun eğer kişisel verilere dayalı olarak ilgili kişiye dair bir sonuç oluşturuyor ve doğuruyorsa kişisel verilerin doğru ve gerektiğinde güncel olmasının sağlanması noktasında aktif özen yükümlülüğü bulunmaktadır."* Kişisel Verileri Koruma Kurulu 22.12.2020 Tarih ve 2020/966 Sayılı İlke Kararı için bkz. https://www.resmigazete.gov.tr/eskiler/2021/01/20210115-3.pdf (Erişim:18.01.2021).
[185] KÜZECİ, s. 231; DEVELİOĞLU, s. 48.
[186] KORKMAZ, s. 101; DEVELİOĞLU, s. 48.
[187] TAŞTAN, s. 50; DEVELİOĞLU, s. 49.
[188] IT Governance Privacy Team, s. 61; AYÖZER, s. 134-135.

Bu ilke 6698 sayılı Kanun'da[189] *"doğru ve gerektiğinde güncel olma ilkesi"* olarak ifade edilmiştir.

2.1.5. Saklama Süresinin Sınırlandırılması İlkesi

Tüzük'ün m.5/f.1 (e) bendinde kişisel verilerin, işlenme amaçlarının gerektirdiğinden daha uzun süre saklanmaması gerektiği kararlaştırılmış; ancak maddenin devamında Tüzük'ün m.89/f.1 hükmünde öngörülen tedbirlerin alınmış olması şartıyla kamu yararı için arşivleme yapılması amacıyla, bilimsel veya tarihi araştırma yapmak amacıyla veya istatiksel amaçlarla kişisel verilerin daha uzun süreler saklanmasının mümkün olabileceği belirtilmiştir. Bu çerçevede kişisel verilerin, gelecekte kullanılma ihtimaline dayanılarak tutulmaması gerekir[190]. Kişisel verilerin ne kadar süre ile muhafaza edileceği ilgili mevzuat çerçevesinde belirlenebilir ve kural olarak ilgili mevzuatta kararlaştırılan süreler dikkate alınmalıdır. Mevzuatta bir sürenin belirlenmemiş olması durumunda kişisel veriler ancak işlendikleri amaç için gerekli olan süre kadar muhafaza edilmelidir. Veri sorumlusu ilgili mevzuatta öngörülen süre sona erdiğinde veya işlendikleri amaç için gerekli olan süre geçtikten sonra verileri silmeli, yok etmeli veya anonim hâle getirmelidir[191].

Bu ilke 6698 sayılı Kanun'da[192] "*ilgili mevzuatta öngörülen veya işlendikleri amaç için gerekli olan süre kadar muhafaza edilme ilkesi"* olarak ifade edilmiştir.

2.1.6. Bütünlük ve Gizlilik İlkesi

Tüzük'ün m.5/f.1 (f) bendinde yer alan bütünlük ve gizlilik ilkesi uyarınca veri sorumlusu, uygun teknik ve idari tedbirleri alarak yetkisiz ve hukuka aykırı olmayacak şekilde ve ayrıca kişisel verileri kazaen kaybolma, yasadışı erişim, imha veya hasara uğrama durumlarına karşı güvende tutarak işleme faaliyetini gerçekleştirmelidir. Bir başka ifade ile bu ilke kişisel verilerin güvende olmasını gerektirir. Bu bağlamda

[189] 6698 sayılı Kanun m.4/f.2 (b) bendi.
[190] KORKMAZ, s. 104.
[191] TAŞTAN, s. 52.
[192] 6698 sayılı Kanun m.4/f.2 (d) bendi.

kişisel verilerin, uygun güvenlik ve gizlilik sağlanacak şekilde işlenebilmesi için veri işleme faaliyetinde kullanılan ekipmana da yetkisiz erişimin önlenmesi gerekir[193].

Örnek vermek gerekirse, özel nitelikte veri olan sağlık verilerini işleyen bir sağlık kuruluşu, kişisel verilere ilişkin bir politika benimseyerek bu kapsamda kişisel verileri psödonimleştirmeyi şart koşabilir. Psödonimleştirilmiş veriye ilişkin anahtarın hastayla ilgilenen belirli sağlık personelinin erişimine açık olması organizasyonel tedbir iken belirli sağlık personelinin kendilerine özgü şifre ile kişisel verilere erişebilmesi ise teknik tedbirdir[194].

6698 sayılı Kanun'da birebir karşılığı olmayan bu ilke, veri sorumlusunun yükümlülüklerine ilişkin düzenlemeler ile temin edilmiştir[195].

2.2. SORUMLU TUTULABİLME PRENSİBİ:HESAP VERİLEBİLİRLİK İLKESİ

Hesap verilebilirlik ilkesi uyarınca veri sorumlusu, veri işleme faaliyetini veri işleme ilkelerine uygun bir şekilde gerçekleştirdiğini gösterebilmelidir. Bu ilke, veri koruma hukukunun temel ilkelerini daha iyi uygulanabilir hâle getirmenin bir aracı olarak da düşünülebilir. Hesap verilebilirlik ilkesinin "*ilkelere uyum yükümlülüğü"* ve *"gerektiğinde hesap verebilme yükümlülüğü"* olmak üzere iki unsurdan oluştuğu kabul edilmektedir[196]. Buna göre veri sorumlusu, gerçekleştirdiği veri işleme faaliyetinde veri koruma kurallarına uyulduğunu garanti edecek önlemler almalı ve denetim makamınca talep edilmesi hâlinde gerekli bütün önlemleri aldığını ispat edebilmelidir. Tüzük, veri koruma kurallarına uyumun sorumluluğunu ve söz konusu uyumun ispat yükünü açıkça veri sorumlusuna yüklemektedir[197].

Sorumlu tutulabilme prensibi her ne kadar veri sorumluları için kabul edilmiş olsa da veri işleyenlerin de hesap verilebilirliğe ilişkin birtakım yükümlülükleri olduğu

[193] Tüzük, Giriş Bölümü, par. 39.
[194] DEVELİOĞLU, s. 50.
[195] DEVELİOĞLU, s. 50.
[196] Article 29 Working Party, **"Opinion 3/2010 on the Principle of Accountability",** WP173, 13 Temmuz 2010, s. 10.
[197] VOIGT / von dem BUSSCHE, s. 31.

unutulmamalıdır[198]. Zira veri işleyenler hakkında da veri işleme güvenliğine ilişkin gerekli tüm tedbirleri almak[199], veri işleme faaliyetlerinin kaydını tutmak[200], belirli şartlarda veri koruma görevlisi belirlemek[201] gibi birtakım yükümlülükler içeren sorumlu tutulabilme ile bağlantılı hükümler vardır. Yine belirtelim ki veri sorumlusu ile veri işleyen arasında yasal olarak bağlayıcı olan sözleşmede, veri koruma etki değerlendirmesi yaparken veya herhangi bir veri ihlalini veri sorumlusuna en kısa sürede bildirirken olduğu gibi bazı uyumluluk gerekliliklerinde de veri işleyenin veri sorumlusuna yardımcı olacağı hususu özellikle yer almalıdır[202].

Tüzük'te yer alan hesap verilebilirlik ilkesinin birebir karşılığı olmamakla beraber sorumluk prensibi, 6698 sayılı Kanun'da veri sorumlusunun veri güvenliğine ilişkin yükümlülüklerinin hüküm altına alındığı 12. maddede düzenlenmiştir. Kanun'un 12. maddesinin 1. fıkrası uyarınca veri sorumlusunun veri güvenliğine ilişkin yükümlülükleri; kişisel verilerin hukuka aykırı olarak işlenmesini önlemek, kişisel verilere hukuka aykırı olarak erişilmesini önlemek, kişisel verilerin muhafazasını sağlamak amacıyla uygun güvenlik düzeyini temin etmeye yönelik gerekli her türlü teknik ve idari tedbirleri almaktır. Kanun'un 12. maddesinin 3. fıkrasında ise veri sorumlusunun, kendi kurum veya kuruluşunda Kanun hükümlerinin uygulanmasını sağlamak amacıyla gerekli denetimleri yapmak veya yaptırmak zorunda olduğu belirtilmiştir. Öte yandan Kanun, uyumdan kimin sorumlu olduğunu açıkça belirtmemiş; veri sorumlusu ile veri işleyenin müşterek sorumluluk ilişkisini düzenlemekle yetinmiştir[203]. Ancak burada belirtmek gerekir ki bu görevin yönetim organında olduğuna dair Veri Sorumluları Sicili Hakkında Yönetmelik'te düzenleme bulunmaktadır[204].

[198] VOIGT / von dem BUSSCHE, s. 32; Handbook on European Data Protection Law, s. 136.
[199] Tüzük m.28/f.3 (c).
[200] Tüzük m.30.
[201] Tüzük m.37.
[202] Tüzük m.28/f.3 (d).
[203] 6698 sayılı Kanun m.12/f.2.
[204] ÇEKİN, s. 138.

2.3.UYUMLULUĞU ARTIRMAYA İLİŞKİN KURALLAR

Genel ilkeler ışığında Tüzük'te, veri sorumlusu hakkında birtakım yükümlülükler ve sorumluluklar belirlenmiştir. Tüzük'ün getirmiş olduğu sorumluluk prensibi risk temelli bir yaklaşım benimsemektedir. Risk temelli yaklaşım, veri sorumlusunun hesap verilebilirliğine yapılan vurguyla yakından bağlantılıdır. Bu anlayışa göre veri işleme faaliyetlerindeki risk seviyesi arttıkça veri sorumlusunun hesap verilebilirliğe ilişkin yükümlülükleri de artmaktadır. Hesap verilebilirlik bir işletme içinde teknik ve idari önlemlerin uygulanmasını gerektirir[205]. Risk temelli yaklaşım ise veri sorumlusunun alınacak teknik ve idari önlemleri belirlemesine yardımcı olarak soyut yasal gerekliliklerin pratikte nasıl uygulanacağını belirlemesini sağlamak için risk kavramını kullanan bir hesap verilebilirlik yaklaşımı olarak görülebilir[206]. Güncel düzenlemelerde bu yaklaşım hesap verilebilirlik ilkesinin adeta temel unsuru olarak kabul edilmiştir[207].

Öte yandan veri sorumlusu işlemenin niteliği, kapsamı, amacı ve veri sahibi için riski ne olursa olsun, her halükarda veri işleme faaliyetinin veri koruma hukukuna uygunluğunun gösterilmesi dâhil veri koruma yükümlülüklerinden her zaman sorumludur[208].

Risk temelli yaklaşım, Tüzük ile veri koruma mevzuatında yer edinmiş yeni bir kavram değildir. 95/46/EC sayılı Yönerge'de de *"İşlemenin güvenliği"* başlıklı 17. madde ve *"Ön kontrol"* başlıklı 20. madde, risk temelli bir yaklaşımın uygulaması olarak düşünülebilir. Ancak Yönerge uyarınca veri sorumluları her zaman veri koruma yasalarına bağlı kalmakla beraber veri koruma hukuku gerekliliklerine yeterince sahip olup olmadıkları hususunda kendilerini değerlendirmekle sorumlu tutulmamışlardır. Risk temelli yaklaşım, Tüzük yürürlüğe girmeden önce veri sorumlusundan ziyade veri koruma otoritelerine yönelik bir anlam ifade etmekte olup ayrıca devletler nezdinde veri koruma hukuku alanında yapılacak düzenlemelerde bir değerlendirme

---

[205] SHARMA, s. 61.
[206] Claudia QUELLE, **The 'risk revolution' in EU data protection law: We can't have our cake and eat it, too,** Tilburg Law School Legal Studies Research Paper Series 1, No:17/2017, s. 3.
[207] Article 29 Working Party, **"Statement on the role of a risk-based approach in data protection legal frameworks",** WP218, 30 Mayıs 2014, s. 12.
[208] Art. 29 Working Party, WP218, s. 3.

ölçütü olarak riske atıfta bulunulmuştur[209]. Tüzük ile veri işlenmesinden sorumlu olanların denetiminin devlet kontrolünden ziyade, veri işlenmesinden sorumlu olanların öz denetimi ve yükümlülüklerinin artırılması yoluyla sağlanması[210] ve bu yükümlülüklerin saptanmasında da riskin değerlendirilmesi amacı güdülmüştür. Tüzük ile bu yaklaşıma daha çok önem verilmiş ve hesap verilebilirlik ilkesinin de bir yansıması olarak uyumluluğu artırmaya ilişkin birtakım yeni düzenlemelere yer verilmiştir.

Tüzük'te, uyumluluğu artırmaya ilişkin çeşitli araçlar belirlenmiştir. Bu kapsamda veri işleme faaliyetlerinin kaydının tutulması, belirli şartlarda veri koruma görevlisi belirlenmesi, veri sahiplerinin hak ve özgürlükleri için yüksek riskler oluşturması muhtemel olan işleme faaliyetlerine başlamadan önce bir veri koruma etki değerlendirmesi yapılması, veri koruma etki değerlendirmesinde veri işlemenin azaltılması mümkün olmayan riskler oluşturacağı tespit edilirse önceden ilgili denetim makamına danışılması, Tüzük'ün çeşitli sektörlerdeki kişisel veri işleme faaliyetlerine uygulanmasını belirleyen veri sorumluları ve veri işleyenler için davranış kuralları, mühür ve işaretler gibi sertifikasyon mekanizmaları uyumluluğu artırmaya ilişkin kuralların bir görünümü olarak düzenlenmiştir.

Burada uyumluluğu artırmaya ilişkin kuralları açıklamaya geçmeden önce belirtmek gerekir ki veri sorumlusunun yükümlülüğü mutlak bir neticeye bağlı değildir. Veri sorumlusunun, kişisel verilerin veri güvenliğine ilişkin saldırılara karşı korunmasının sağlanması amacıyla en azından veri koruma hukukunda kararlaştırılan gerekli önlemleri aldığını ispatlayabilmesi hâlinde sorumluluktan kurtulabilmesi mümkündür. Bu bağlamda bir özen sorumluluğunun varlığından bahsedilebilir[211]. Ancak veri sorumlusunun neticeden sorumlu tutulmaması gerekli önlemlerin alınması hususunda yükümlülük kapsamının genişlemesi anlamına da gelmektedir. Veri sorumlusu, veri güvenliğine ilişkin doğabilecek tehlikeleri tespit ederek bunları önlemeye hizmet edecek yöntemleri belirlemelidir.

[209] QUELLE, s. 17.
[210] ÇEKİN, s. 13.
[211] ÇEKİN, s. 187.

2.3.1.Veri İşleme Faaliyetinin Kayıtları

Veri sorumlusu ve veri işleyen hakkında, uyumluluğun sağlanması ile hesap verilebilirlik bakımından veri işleme faaliyetlerinin kaydının tutulması ve belgelenmesine yönelik Tüzük'te açıkça bir yükümlülüğe yer verilmiştir[212]. Veri sorumlusunun ve veri işleyenin Tüzük'e uygun hareket edildiğini ispatlamalarına yardımcı olacak kurallardan birisi veri işleme faaliyetlerinin kaydının tutulmasıdır[213]. Buna göre veri işleme faaliyetlerine ilişkin dokümantasyon ve kayıtlar muhafaza edilmeli ve talep edildiği takdirde denetim makamına sunulmalıdır. Böylece denetim makamı da veri işlemenin hukuka uygun gerçekleştirildiğini gözlemleme imkânına kavuşmuş olacaktır.

Tüzük'te kayıt tutma yükümlülüğüne istisna getirilmiştir. Buna göre veri işleme faaliyetinin ilgili kişilerin hak ve özgürlükleri açısından risk teşkil etme ihtimalinin düşük olduğu, süreklilik arz etmediği ve m.9/f.1'de belirtilen özel kategorilerdeki kişisel verilere veya m.10'da belirtilen mahkûmiyet kararı ve ceza gerektiren suçlara ilişkin olmadığı sürece, 250 kişiden az çalışanı olan işletme veya kuruluşlar kayıt tutma yükümlülüğü altında değildir[214].

2.3.2.Veri Koruma Görevlisi

Tüzük'ün 37 ila 39. maddelerinde düzenlenen veri koruma görevlisi, çalışmanın üçüncü bölümünde detaylı olarak anlatılmıştır[215]. Ancak bu başlık altında da belirtmek gerekir ki veri koruma görevlisi, Tüzük'te hesap verilebilirlik ilkesine pratik bir etki kazandırmak noktasında temel bir araç olarak görülmesi gereken önemli ve yeni bir kurumdur[216]. Dış denetim yolu ile elde edilecek uyumun iç denetim mekanizması olarak görülebilecek bir veri koruma görevlisi vasıtasıyla daha ciddi ve kapsamlı şekilde sağlanması amaçlanmıştır.

---

[212] Tüzük m.30.
[213] Handbook on European Data Protection Law, s. 179.
[214] Tüzük m.30/f.5.
[215] Bkz. s. 60 vd.
[216] Douwe KORFF / Marie GEORGES, **The DPO Handbook Guidance for data protection officers in the public and quasi-public sectors on how to ensure compliance with the European Union General Data Protection Regulation**, 2019, s. 120.

2.3.3.Veri Koruma Etki Değerlendirmesi Ve Ön İnceleme

Veri koruma etki değerlendirmesi; veri sorumlusunun gizlilik risklerini tanımasına, tanımlamasına ve en aza indirmesine yardımcı olan bir süreç olarak değerlendirilebilir[217]. Yeni teknolojilerin ortaya çıkması ve veri işleme faaliyetlerinin giderek daha karmaşık bir hâl alması karşısında veri sorumluları işleme operasyonlarına başlamadan önce işlemenin niteliği, kapsamı, bağlamı ve amacını dikkate alarak bireylerin hak ve özgürlükleri açısından oluşabilecek riskleri ele almalıdır ve yüksek risk oluşabilecek durumlarda etki değerlendirmesi yapmalıdır[218]. Böylelikle veri sorumlusunun riskleri önceden doğru bir şekilde analiz etmesi ve veri sahipleri üzerindeki olumsuz etkilerini önemli ölçüde azaltması amaçlanmıştır.

Veri koruma etki değerlendirmesi hem Avrupa Konseyi[219] hem AB hukuku uyarınca öngörülmüştür. Veri koruma etki değerlendirmesine ilişkin Tüzük m.35'te ayrıntılı bir düzenlemeye yer verilmiş olmakla beraber risk olasılığının nasıl değerlendirileceği tanımlanmamış ancak bu risklerin neler olabileceği belirtilmiştir. Yüksek riskli faaliyetlerin tanımının yapılmamış olması, uygulamada veri sorumluları bakımından veri koruma etki değerlendirmesi yapılmasına gerek olup olmadığına karar verilmesi hususunda belirsizliğe ve zorluk yaşanmasına sebebiyet verebilir. Belirsizlik söz konusu olduğunda, veri koruma kurallarına uyum konusunda veri koruma etki değerlendirmesinin yararlı bir araç olduğu göz önünde bulundurularak yapılması yönünde aksiyon alınması yerinde bir tercih olacaktır[220]. Öte yandan belirsizlik, ulusal denetim makamları tarafından açıklığa kavuşturularak çözülebilir.

---

[217] IT Governance Privacy Team, s. 70.

[218] Paul LAMBERT, **The Data Protection Officer Profession, Rules and Role**, CRC Press Taylor&Francis Group, 2017, s. 275; Tüzük, Giriş Bölümü, par. 84.

[219] Modernize Edilmiş 108 sayılı Sözleşme'nin *"Ek Yükümlülükler"* başlıklı 10. maddesinin 2. fıkrasında; "*veri sorumluları ve uygun olduğu ölçüde veri işleyenlerin, veri işleme faaliyetine başlamadan önce amaçlanan veri işlemenin veri sahiplerinin temel hak ve özgürlükleri üzerinde oluşabilecek muhtemel etkilerini değerlendirmeleri ve veri işleme faaliyetini bu temel hak ve özgürlüklere müdahale riskini önleyecek veya minimize edecek şekilde tasarlamaları gerektiği*" belirtilmiştir. https://rm.coe.int/convention-108-convention-for-the-protection-of-individuals-with-regar/16808b36f1 (Erişim:04.09.2020).

[220] Article 29 Working Party, **"Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679"**, WP248, 4 Ekim 2017, s. 8.

Tüzük'te yüksek riskli kabul edilen ve önceden veri koruma etki değerlendirmesi yapılması gereken durumlar düzenlenmiştir. Buna göre profil çıkarma da dâhil olmak üzere gerçek kişilerle ilgili özelliklerin otomatik işlemesine dayanan ve gerçek kişilerle ilgili hukuki etkiler üreten veya onları benzer şekilde etkileyen kararlara dayanak olan sistematik ve kapsamlı bir tespit yapılması hâlinde, Tüzük m.9/f.1'de atıfta bulunulan özel nitelikli veri kategorilerinin veya m.10'da atıfta bulunulan ceza mahkumiyeti veya güvenlik tedbirlerine ilişkin kişisel verilerin geniş çapta işlenmesi veya kamuya açık bir alanın büyük ölçekte sistematik olarak izlenmesi hâlinde veri koruma etki değerlendirmesi yapılmasına ihtiyaç duyulacaktır[221].

Veri koruma etki değerlendirmesi yapılmasının akabinde veri işlemenin bireylerin hak ve özgürlükleri üzerinde yüksek risk oluşturacağı ve veri sorumlusu tarafından riski azaltmak için herhangi bir tedbir alınmaması durumunda, veri sorumlusunun veri işleme faaliyetine başlamadan önce ilgili denetim makamına başvurması gerekir[222]. Öncelikle veri sorumlusu tarafından veri koruma etki değerlendirmesi yapılması, akabinde değerlendirmenin sonucuna göre denetim makamına başvurulması Tüzük ile getirilen bir yeniliktir. Yönerge'de ise kısmen veya tamamen otomatik işleme faaliyetinde bulunacak veri sorumlularının, Tüzük'ten farklı olarak, önceden denetim makamına bildirimde bulunması ve risk teşkil eden işleme faaliyetlerinin *ön kontrol* adı verilen bir mekanizma ile denetim makamı tarafından incelenmesi öngörülmüştür. Tüzük ile getirilen sistem, denetim makamına başvuruyu -gerektiğinde- yükümlü kılmakla veri sorumlusu üzerindeki ekonomik ve idari yükü azaltmaktadır.

2.3.4.Davranış Kuralları

Tüzük uyarınca, belirli sektörlerde gerçekleştirilen veri işleme faaliyetlerinin ve küçük ve orta ölçekli işletmelerin özellikleri dikkate alınarak veri işleme faaliyetlerinin hukuka uygun şekilde gerçekleştirilmesini sağlayan davranış kurallarının oluşturulması teşvik edilmiştir[223]. Sektörün özelliklerini dikkate alan kurallar ile veri

[221] Tüzük m.35/f.3; LAMBERT, **Data Protection Officer**, s. 175.
[222] Tüzük m.36/f.1.
[223] Tüzük m.40, 41.

sorumlusu ve veri işleyen açısından Tüzük'ün nasıl uygulanacağının ve hukuka uygunluğun nasıl sağlanacağının daha belirgin hâle getirilmesi; Tüzük'te yer alan soyut hükümlerin ilgili sektörlerin özellikleri dikkate alınarak somutlaştırılması amaçlanmıştır. Davranış kuralları özellikle küçük ve orta ölçekli işletmeler için hesap verilebilirlik ve veri koruma kurallarına uyumun sağlanması adına pratik bir düzenleme olarak düşünülebilir[224].

Davranış kuralları hazırlamak veya değiştirmek isteyen kurum ve kuruluşların[225] hazırladıkları taslağı yetkili denetim makamına sunması gerekmektedir. Burada belirtilmesi gereken husus, davranış kuralları konusunda denetim makamının bir danışma mercii değil onay mercii olduğudur. Bununla birlikte denetim makamı onaylanmış davranış kurallarını ve onaylarının dayandığı kriterleri veya olumsuz bir sonuca ulaşmış ise bu kararının gerekçesini yayınlamalıdır[226]. Davranış kurallarının tüm Avrupa Birliği içerisinde hüküm ifade etmesi hâlinde, üye ülke otoritesi, kendisine sunulan davranış kurallarını Tüzük m.63'te açıklanan tutarlılık mekanizmasına uygun olarak Avrupa Birliği Veri Koruma Kurulu'na sunar. Tüzük m.40/f.8 hükmü uyarınca Kurul'un görüşünü Komisyona sunması durumunda Komisyon'un, ilgili davranış kurallarının Tüzük m.93/f.2'de öngörülen inceleme usulü uyarınca tüm Birlik içerisinde geçerliliğe sahip olduğuna karar vermesi de mümkündür.

Burada son olarak belirtmek gerekir ki veri sorumlularının ve veri işleyenlerin, davranış kurallarına uyumlu davranıp davranmadığını izleme noktasında Tüzük m.41 düzenlemesine göre; denetim makamı, davranış kurallarına uyumun denetlenmesi yetkisini, denetim makamı tarafından belirlenen şartları sağlayan ve yine denetim makamı tarafından akredite edilmiş özel teşebbüslere verebilir.

2.3.5.Belgelendirme

Veri sorumlusunun ve veri işleyenin Tüzük'e uyumluluğunu gösterecek bir başka araç da belgelendirme mekanizmaları ve veri koruma mühürleri ve işaretleridir. Şeffaflığı ve uyumu artırmak, veri koruma hukuku seviyesini tespit etmek amacıyla

[224] IT Governance Privacy Team, s. 65.
[225] Davranış kuralları hazırlama yetkisine ilişkin bkz. ÇEKİN, s. 236.
[226] Handbook on European Data Protection Law, s. 182.

belgelendirme mekanizmalarının, veri koruma mühürlerinin ve işaretlerinin teşvik edilmesi gerektiği Tüzük'te belirtilmiştir[227]. Bu amaçla belirli kuruluşların veya veri koruma otoritelerinin sertifika verebileceği gönüllü bir belgelendirme mekanizması kararlaştırılmıştır[228]. Belgelendirme işlemi veri koruma otoritelerince yahut veri koruma otoriteleri tarafından akredite edilmiş özel kuruluşlarca gerçekleştirilebilecektir[229].

Veri sorumlusu veya veri işleyenin, veri işleme faaliyetinden doğan yükümlülüklerini yerine yetirdiğini gösteren önemli araçlardan birisi de onaylı belgelendirme mekanizmalarına katılmak olmakla birlikte tek başına belgelendirme mekanizmaları, veri sorumlusu veya veri işleyenin işleme faaliyetlerinin Tüzük'e uyumlu olduğunu kanıtlamayacaktır[230].

[227] Tüzük, Giriş Bölümü, par. 100.
[228] Tüzük m.42.
[229] ÇEKİN, s. 241.
[230] IT Governance Privacy Team, s. 162.

ÜÇÜNCÜ BÖLÜM: VERİ KORUMA GÖREVLİSİ (DATA PROTECTION OFFICER)

3.1. VERİ KORUMA GÖREVLİSİ KAVRAMI

Avrupa Birliği'nde kişisel verilerin korunmasına ilişkin en kapsamlı düzenleme Avrupa Konseyi tarafından 1995 yılında kabul edilen 95/46/EC sayılı Kişisel Verilerin İşlenmesi ve Serbest Dolaşımı Bakımından Bireylerin Korunmasına İlişkin Yönerge iken Avrupa Birliği, 4 Mayıs 2016 tarihinde Avrupa Birliği Resmi Gazetesi'nde yayınlanarak 24 Mayıs 2016 tarihinde yürürlüğe giren ve 25 Mayıs 2018 tarihinde Yönerge'yi ilga ederek uygulanmaya başlayan Avrupa Birliği Genel Veri Koruma Tüzüğü'nü (GDPR) kabul etmiştir.

Bir bireyin kişisel verilerinin, korunması gereken değerli bir varlık olduğu ve bu değerin günümüz şartlarında ekonomik olarak da ciddi boyutta anlam ifade ettiği uzun zamandır kabul edilen bir gerçektir. Ancak kişisel verileri kullanan kuruluşlar tarafından veri koruma yükümlülükleri yeterince yerine getirilmemekte ve yine iletişim ve etkileşim teknolojisinin ilerleyişi ile paralel hızda bu korumaya ilişkin yeterli önem gösterilmemekteydi. Veri koruma rejiminin güçlendirilmesi adına bir reformun gerekli olduğu Avrupa düzeyinde tartışılagelen bir husus idi[231]. AB kanun koyucusu da günümüz gelişen teknolojisi ve kişisel verilerin her geçen gün ifade ettiği anlamın daha fazla değer kazanması karşısında hukuki düzenlemeleri revize etme ihtiyacı duymuştur. Tüzük bu ihtiyacın sonucu olarak hazırlanmış ve kabul edilmiş bir yasal düzenlemedir.

Yönerge, AB üyesi ülkeler bakımından doğrudan bağlayıcı olmayıp Yönerge'deki temel düzenlemeler doğrultusunda üye ülkelerin kanuni düzenlemelerinin hazırlanmasında "*uyumlaştırma aracı*" niteliğindedir. Yönerge, üye ülkelere kanuni düzenlemelerini hazırlarken uyulması gereken ve asgari ölçütleri belirleyen yol gösterici bir düzenleme konumunda olup netice itibariyle üye ülkelere iç hukuklarında yapacakları düzenlemelerde serbestiyet tanımıştır. AB kanun

[231] https://www.newlawjournal.co.uk/content/mind-gdpr (Erişim:20.10.2019).

koyucusu, veri koruma alanının önemini düşünerek bu konudaki bir düzenlemeyi yönerge yerine üye devletlere doğrudan uygulanabilir ve bağlayıcı nitelikte olacak, modernize edilmiş ve hesap verilebilirliğe dayalı bir tüzük ile düzenlemeyi tercih etmiştir. Tüzük'ün kabul edilmesiyle üye ülkeler arasında iç hukuk düzenlemelerinden kaynaklanan farklılıklar giderilmiş olmakla üye ülkelerdeki kişisel verilere ilişkin düzenlemelerde yeknesaklık sağlanmıştır.

AB Genel Veri Koruma Tüzüğü'nün Mayıs 2018 tarihinde uygulanmaya başlamasıyla AB sınırları içerisinde bulunan gerçek kişilere mal veya hizmet sunan veya AB'de bulunan kişilerin davranışlarının gözlemlenmesine ilişkin veri işleme faaliyetinde bulunan veri sorumlusu ve veri işleyen, AB'de bulunup bulunmadığına bakılmaksızın bu Tüzük'ün uygulama alanına dâhil edilmiştir[232].

Tüzük ile veri koruma hukukunda bugüne kadar kabul edilen *somut olay ağırlıklı bir yaklaşım*[233] yerine, kişisel verilerin korunmasına ilişkin temel ilkelerden olan hesap verilebilirlik ilkesinin bir gereği olarak *bütüncül bir yaklaşım*[234] anlayışı benimsenmiştir. Bu anlayışa göre veri sorumlularının yalnızca somut olayda veri işleme faaliyetinin hukuka uygunluğunu kanıtlaması yetmemekte, kişisel verilerin hukuka uygun şekilde işlenmesi için gerekli teknik ve idari tedbirleri alması gerekmektedir. Daha somut bir ifadeyle denetim makamı tarafından somut olay denetimi yerine, veri sorumlularının her an bir denetime tabi tutulmuşçasına özel bir organizasyon sorumluluğu geliştirmesi ve gerektiğinde kişisel verilerin veri işleme ilkelerine uygun şekilde işlenmesi adına gerekli teknik ve idari tedbirleri aldığını gösterebilmesi anlayışı kabul edilmiştir.

Tüzük'ün, veri sorumlularının teknik ve idari tedbir alma yükümlülüğüne ilişkin gerekliliklerinden ve yeniliklerinden birisi de kamu otoritelerinin ve kişisel verileri geniş çaplı olarak işleyen şirketlerin veri koruma hukukuna uyumu kolaylaştıracak bir veri koruma görevlisi belirleme yükümlülüğüdür. Tüzük'ten önce yürürlükte bulunan 95/46/EC sayılı Yönerge, veri sorumlularının zorunlu olarak bir veri koruma görevlisi belirlemesini gerektirmemekle birlikte bazı veri sorumlularının veri koruma görevlisi

[232] Tüzük m.3/f.2.
[233] ÇEKİN, s. 52.
[234] ÇEKİN, s. 52.

belirleyebileceği olasılığına yer vermiştir. Yönerge'nin 18. maddesinin 2. fıkrasında, veri sorumlularının ulusal yasalara uygun olarak bir veri koruma görevlisi belirlemesi hâlinde veri işleme faaliyetlerini denetim makamına bildirim yükümlülüğünden muaf olabileceği veya bildirimin basitleştirilmesi imkânına kavuşabileceği düzenlemesine yer verilmiştir. Yönerge'de zorunlu olarak veri koruma görevlisi belirlenmesine ilişkin bir düzenlemeye yer verilmemiş olmakla birlikte pratikte üye devletlerin -özellikle Almanya, İsveç- bu yönde organizasyon geliştirdiği görülmüştür[235]. Yönerge'nin yanı sıra Tüzük'ün kabul edilmesinden önce, AB kurumlarının kendi veri koruma kurallarını belirleyen 45/2001 sayılı Tüzüğü'nde[236] her bir AB kurumunun veya organının veri koruma görevlisi ataması yükümlülüğü getirilmiştir[237].

Tüzük'ün yayınlanması ile birlikte uluslararası kuruluşlar tarafından birtakım araştırmalar yapılmış ve International Association of Privacy Professionals-IAPP (Uluslararası Mahremiyet Uzmanları Birliği) tarafından hazırlanan Nisan 2016 tarihli araştırmada, AB üyesi devletler bakımından 28.000 veri koruma görevlisine ihtiyaç duyulacağı; Kasım 2016 tarihli araştırmada ise dünya genelinde 75.000 veri koruma görevlisine ihtiyaç duyulacağı varsayımı ortaya konmuştur[238]. Bu rakamlar resmi istatistiklere ve Avrupa İstatistik Ofisi-EUROSTAT verilerine göre hesaplanmış olmakla beraber elbette net değil tahmini rakamlardır; zira her kurum ve kuruluş hesaplamaya dâhil edilmemiş, küçük çaplı kurum ve kuruluşlar hesaplamanın dışında tutulmuştur.

Kamu kurum ve kuruluşları ile şirketlerin Tüzük kapsamındaki yükümlülüklerinin farkında olması ve işlenen verilerin geleceği konusunda ulusal ve

---

[235] Gerrit HORNUNG, "**A General Data Protection Regulation for Europe? Light and Shade in the Commission's Draft of 25 January 2012",** Scripted, C.9, S.1, Nisan 2012, s.77.; VOIGT / von dem BUSSCHE, s. 53; Miguel RECIO, **"Practitioner's Corner Data Protection Officer: The Key Figure to Ensure Data Protection and Accountability"**, European Data Protection Law Review, C.3, S.1, 2017, s. 114.

[236] REGULATION (EC) No 45/2001 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 18 December 2000, Art.24. 45/2001 sayılı Tüzük tam metni için bkz. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32001R0045 (Erişim:09.09.2020).

[237] Europen Data Protection Supervisor (EDPS), **"Position paper on the role of Data Protection Officers in ensuring effective compliance with Regulation (EC) 45/2001"**, Brüksel, 28.11.2005, s.3-4 (Çevrimiçi) https://edps.europa.eu/sites/edp/files/publication/05-11-28_dpo_paper_en.pdf (Erişim:20.10.2019).

[238] https://iapp.org/news/a/study-at-least-28000-dpos-needed-to-meet-gdpr-requirements/ (Erişim:20.10.2019), https://iapp.org/news/a/study-gdprs-global-reach-to-require-at-least-75000-dpos-worldwide/ (Erişim:20.10.2019).

uluslararası hukuk mevzuatına uygun spesifik bir politika oluşturması konusunda alanında uzman bir veri koruma görevlisi ile beraber hareket etmesi gerekmektedir. Veri koruma görevlisinin rolü, veri koruma alanında bir farkındalık yaratmak ve en önemlisi içinde bulunduğu organizasyonda bir *"veri koruma kültürü"* geliştirmektir. Veri koruma görevlisi, Tüzük'e uyumu kolaylaştıracak olup uyuma destek olduğu için *hesap verilebilirliğin temel taşı (a cornerstone of accountability)*[239] yahut bir başka ifadeyle *veri koruma uyumluluğunun temel taşı (a cornerstone of data protection compliance)*[240] niteliğindedir. *"Data Protection Officer-DPO"* olarak anılan *"Veri Koruma Görevlisi"*, Tüzük'ün 37 ila 39. maddeleri arasında düzenlenmiş olup Tüzük sırasıyla *"Veri Koruma Görevlisinin Belirlenmesi"*ni, *"Veri koruma Görevlisinin Konumu"*nu ve "*Veri Koruma Görevlisinin Görevleri"*ni hüküm altına almıştır.

3.2. VERİ KORUMA GÖREVLİSİNİN BELİRLENMESİ

Tüzük uyarınca belirli veri sorumlularının ve veri işleyenlerin veri koruma görevlisi belirlemesi zorunludur; ancak zorunluluk kapsamına girmeyen kuruluşların da pek tabii veri koruma görevlisi belirlemesi mümkündür[241]. Burada veri sorumluları ve veri işleyenler açısından ilk adım, Tüzük kapsamında bir veri koruma görevlisi rolü belirlemenin zorunlu olup olmadığının analizinin yapılmasıdır[242]. Tüzük kapsamında veri işleyen/işlenmesinden sorumlu olan her kuruluş Tüzük'ün getirdiği yükümlülüklere uymak zorundadır ve yükümlülüklerin ihlali hâlinde yine Tüzük kapsamında cezai müeyyidelere maruz kalacaktır. Kuruluşlar iş operasyonunun büyüklüğü ve çeşitliliği gibi etkenleri göz önünde bulundurarak özellikle veri ihlali riskinin yüksek olması ihtimalinde, veri sahiplerinin haklarına ve özgürlüklerine yönelik riskleri dikkate alarak değerlendirme yapmalıdır[243].

---

[239] Handbook on European Data Protection Law, s. 175.

[240] Marta-Claudia CLIZA / Laura-Cristiana SPATARU-NEGURA, **"The General Data Protection Regulation: What does the public authorities and bodies need to know and to do? The rise of the data protection officer",** Juridical Tribune, C.8, S.2, 2018, s. 492.

[241] Simona CHIRICA, **"The Main Novelties and Implications of the New General Data Protection Regulation"**, C.6, S.1, 2017, s. 163.

[242] Thomas J. SHAW, **DPO Handbook Data Protection Officers Under The GDPR**, International Association of Privacy Professionals (IAPP), 2.Baskı, 2018, s.2.

[243]Xavier Duncan L'HOIRY / Clive NORRIS, **"The Honest Data Protection Officer's Guide to Enable Citizens to exercise Their Subject Access Rights: lessons from a ten country European study",** International Data Privacy Law, C.5, S.3, 2015, s. 3.

Bu rol, yasaya göre zorunlu olabileceği gibi; zorunlu olmamakla birlikte ilgili kuruluşun veri koruma konusunda bilinçli hareket edebilmesini sağlamak için faydalı olacağı düşüncesiyle isteğe bağlı olarak da belirlenebilir. Veri koruma görevlisinin zorunlu olmaksızın belirlenmesi durumunda da yine zorunlu belirleme varmışçasına belirleme, konum ve görev gibi Tüzük m.37-39 hükümlerinde belirtilen şartlara uyulması gerekmektedir.

Kişisel verilerin işlenmesinin kural olarak yasak olması ve ancak Tüzük'ün öngördüğü istisnai durumlarda veri işlenmesine izin verilmesi, veri sahibinin haklarına ilişkin veri sorumlusu ve veri işleyenin bilgilendirme yükümlülüğünün olması, veri sahibine tanınan tazminat talep etme hakkı ve Tüzük ile uygulanacak cezai müeyyidelerin artırılması gibi hususlar göz önünde bulundurulduğunda, Tüzük'ün bir veri koruma görevlisi belirlenmesini zorunlu kılıp kılmadığına bakılmaksızın her veri sorumlusunun ve veri işleyenin Tüzük kapsamındaki yükümlülüklerini yerine getirebilmek adına veri koruma hukuku konusunda bilgili ve donanımlı yeterli personel ve kaynağa sahip olması muhakkak ki kendi menfaatlerine olacaktır.

Tüzük m.37'de veri koruma görevlisi belirlemenin zorunlu olduğu hâller düzenlenmiştir.

Buna göre;

"a) Veri işleme faaliyetinin yargı faaliyetinin yürütülmesi hariç bir kamu kurum veya kuruluşu tarafından gerçekleştirilmesi,

b) Veri sorumlusu veya veri işleyenin temel faaliyetleri veri sahiplerinin büyük ölçekte veriyi düzenli ve sistematik izlemeyi gerektiren işleme faaliyetlerinden oluşması,

c) Veri sorumlusu veya veri işleyenin temel faaliyetlerinin Tüzük m.9 uyarınca özel kategorilerdeki verilerin veya Tüzük m.10 uyarınca belirtilen mahkûmiyet kararları ve ceza gerektiren suça ilişkin kişisel verilerin büyük çaplı olarak işlenmesinden meydana gelmesi"

hâllerinde veri koruma görevlisi belirlenmesi zorunludur. Madde metninden anlaşılacağı üzere belirleme şartları veri sorumlusunun veya veri işleyenin niceliksel

özelliklerine (örneğin çalışan sayısı) değil; veri işleme faaliyetinin niteliğine bağlıdır. Veri koruma görevlisinin belirlenmesinde veri sorumlusunun veya veri işleyenin veri işleme faaliyetinin niteliklerinin dikkate alınması, Tüzük'ün risk temelli yaklaşım benimsemesinin bir sonucudur[244].

Veri koruma görevlisi, zorunlu veya isteğe bağlı olması fark etmeksizin veri sorumlusu veya veri işleyen tarafından gerçekleştirilen tüm veri işleme faaliyetleri için belirlenir. Bu sebeple belirtmek gerekir ki veri koruma görevlisinin görevlerinin kapsamının belirli veri işleme faaliyetleriyle kısıtlanması mümkün değildir[245].

Bir kuruluşun zorunlu olarak veri koruma görevlisi belirlemesi gerekip gerekmediği belirgin veya açıkça anlaşılabilir değil ise kuruluşun, veri koruma görevlisi belirlemede zorunluluk şartlarını sağlayıp sağlamadığına ilişkin ilgili faktörlerin hepsinin dikkate alındığı değerlendirmesini içerir içsel bir analiz yaptığını, gerektiğinde veri koruma otoritesine sunmak üzere, belgelemesi gerekir. Bu belgelendirme hesap verilebilirlik ilkesinin de bir gereğidir. Hemen belirtelim ki bu analiz, veri sorumlularının veya veri işleyenlerin faaliyet alanlarına yenisini eklemesi veya m.37 çerçevesinde sayılan hâllere dâhil olabilecek yeni hizmetler sağlaması durumunda güncellenmelidir.

Ayrıca, Tüzük'te her ne kadar veri koruma görevlisi belirlenmesi için gerekli şartlar belirtilmişse de bu şartlara her hâlde uyulmak şartıyla ulusal yasalar uyarınca veri koruma görevlisi belirlenmesi için ek şartlar kararlaştırılabilir.

Burada *"Tek bir kuruluş için birden fazla veri koruma görevlisi belirlenebilir mi?"* sorusu akla gelebilir. Tüzük, m.39'da sayılan görevlerin yerine getirilebilmesi için bir kuruluşun tek bir veri koruma görevlisi belirlemesi gerektiği açıkça belirtilmiştir. Bu sorunun cevabı olumsuz olmakla birlikte, çalışmamızın ilerleyen bölümlerinde açıklanacağı üzere[246] görev alınan kuruluşun faaliyet konusu, işleme operasyonlarının karmaşıklığı vb. etkenler veri koruma görevlisinin bir veri koruma

[244] VOIGT / von dem BUSSCHE, s. 53.
[245] https://www.fieldfisher.com/en/services/privacy-security-and-information/privacy-security-and-information-law-blog/everything-youve-ever-wanted-to-know-about-dpo-but-never-dared-to-ask (Erişim:25.10.2019).
[246] Bkz. s. 75 vd.

ekibi kurmasını gerektirebilir. Ancak veri koruma görevlisi olarak belirlenmiş tek bir kişi olmalıdır[247]. Bu ekibe veri koruma uzmanları da dâhil edilebilir; fakat ekipte yer alan kimselerin rol ve sorumlulukları, bu kimselerin veri koruma görevlisi ile ilişkisi açıkça belirtilmeli ve bu kimseler veri koruma görevlisi olarak anılmamalıdır.

Son olarak *"AB dışındaki kuruluşlar da Tüzük m.37 düzenlemesi uyarınca veri koruma görevlisi belirlemeli midir?"* sorusuna cevap vermek gerekirse; Tüzük'ün, uygulama alanına ilişkin *"Bölgesel Kapsam"* başlıklı m.3/f.2 hükmünde "*veri sahibine bir ödeme yapılmasına gerek olup olmadığına bakılmaksızın, Birlik içerisindeki söz konusu veri sahiplerine mal ya da hizmetlerin sunulması veya davranışları birlik içerisinde gerçekleştiği ölçüde, davranışlarının izlenmesi durumunda"* AB içerisinde bulunan veri sahiplerinin kişisel verilerinin AB içerisinde kurulu olmayan bir veri sorumlusu veya veri işleyen tarafından işlenmesinde uygulanacağı kararlaştırılmıştır. Buna göre AB dışında olan ancak Tüzük'ün uygulama kapsamına giren kuruluşların da Tüzük m.37'de belirtilen koşulları sağladığı ölçüde veri koruma görevlisi belirlemesi gerekebilir.

3.2.1. Veri Koruma Görevlisi Belirlemenin Zorunlu Olduğu Hâller

3.2.1.1. Kamu Kurum veya Kuruluşlarının Veri Koruma Görevlisi Belirleme Yükümlülüğü

Tüzük m.37 uyarınca yargı faaliyetinin yürütülmesi hariç bir kamu kurum veya kuruluşu tarafından veri işleme faaliyeti gerçekleştirilmesi hâlinde, veri koruma görevlisi tayin edilmelidir. Mahkemeler ve bağımsız yargı makamları, veri koruma görevlisi belirleme zorunluluğundan muaftır[248]. Hemen belirtelim ki Tüzük, "kamu kurum veya kuruluşu" ibaresi ile neyin ifade edildiğini tanımlamamıştır[249]. Article 29

[247] Information Commissioner's Office (ICO), "**Guide to the General Data Protection Regulation (GDPR)",** 2 Ağustos 2018 s. 197-198 (Çevrimiçi) https://ico.org.uk/media/for-organisations/guide-to-the-general-data-protection-regulation-gdpr-1-0.pdf (Erişim:25.10.2019).

[248] Tüzük, Giriş Bölümü, par. 97.

[249] AB yasa koyucusu *"public sector body"* ve *"body governed by public law"* kavramlarını 17 Kasım 2003 tarih ve 2003/98/EC sayılı Avrupa Parlamentosu ve Konseyi Direktifi'nin 2. maddesinde tanımlamıştır. Ayrıntılı bilgi için bkz. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32003L0098&from=en (Erişim:28.10.2019).

Working Party, bu kavramın ulusal yasalar çerçevesinde belirleneceği düşüncesindedir[250].

Kamu kurumu olmadığı hâlde toplu taşıma hizmetleri, enerji ve ulaşım sektörü, altyapı hizmetleri gibi kamu yararı gözeten veya kamu otoritesi tarafından kendisine verilen görevi yürüten, özel hukuk veya kamu hukuku hükümleri uyarınca faaliyet gösteren ve özel hukuk tüzel kişiliğini haiz kuruluşların veri koruma görevlisi belirlemesinin zorunlu olduğuna ilişkin Tüzük'te bir hüküm bulunmamaktadır. Ancak AB ulusal veri koruma makamları bu kuruluşların veri koruma görevlisi belirlemesini tavsiye etmektedir[251]. Gerçekten de faaliyet alanları gereği verilerin kamu kurumları ile benzer amaçlar için işlenmesi ve veri sahiplerinin verilerin işlenmesi hususunda pek az bir seçeneğe sahip olması gibi hususlar daha özenli bir koruma düzeyi gerektireceğinden, veri koruma görevlisinin bu kuruluşlar için de belirlenmesi yerinde bir uygulama olacaktır.

3.2.1.2. İşletme Temel Faaliyetinin Düzenli ve Sistematik Bir Şekilde Geniş Çaplı İzleme Gerektirmesi

Tüzük m.37 uyarınca veri sorumlusunun veya veri işleyenin temel faaliyetlerinin geniş çaplı veriyi düzenli ve sistematik izlemeyi gerektiren işleme faaliyetlerinden oluşması durumunda, o veri sorumlusu veya veri işleyenin veri koruma görevlisi belirlemesi zorunludur. Burada Tüzük maddesinde yer alan *"temel faaliyet"*, *"geniş çap"* ve *"düzenli ve sistematik izleme"* kavramları önem arz etmekte olup bu kavramlar üzerinde durulacaktır.

Sosyal medya şirketleri ve arama motorları, düzenli ve sistematik bir biçimde geniş çaplı veri işleme faaliyetinde bulunan veri sorumlusuna örnektir. Çünkü bu tarz şirketlerin iş modeli, büyük miktarda kişisel verilerin işlenmesi ile reklamcılık hizmetleri sunulmasına ve web sitelerinde reklam verilmesine izin vererek gelir sağlamalarına dayanır. Bu reklamlar demografiye ve tüketicilerin önceki satın alma

[250] Article 29 Working Party, **"Guidelines on Data Protection Officers ('DPOs')",** WP243, 5 Nisan 2017, s. 6.
[251] Art. 29 Working Party, WP243, s. 6; L'HOIRY / NORRIS, s. 493.

geçmişine dayalı olmasından dolayı veri öznelerinin davranışlarının çevrimiçi olarak geniş çaplı, düzenli ve sistematik olarak izlenmesini gerektirir.

Hastaneler ve sigorta şirketlerinin faaliyet alanları geniş çapta ve özel nitelikte kişisel verinin işlenmesini zorunlu kıldığından, bu kuruluşlar da veri koruma görevlisi belirlemesi gereken veri sorumlusuna örnektir. Bir bireyin sağlığına ilişkin bilgileri içeren veriler ile genetik ve biyometrik veriler hem Avrupa Konseyi hem de AB yasaları uyarınca özel nitelikte kişisel veri kategorisine girmektedir ve gelişmiş koruma sağlanmasını gerektirir. Sağlık kuruluşları ve sigorta şirketlerinin bu tür özel nitelikte kişisel verileri geniş çapta işlemelerinden dolayı Tüzük uyarınca veri koruma görevlisi belirlemesi gerekmektedir[252].

3.2.1.2.1. Temel Faaliyet

Tüzük m.37/f.1 (b) ve (c) bendinde *"veri sorumlusu veya veri işleyenin temel faaliyetleri"* ibaresine yer verilmiştir. Temel faaliyetlerden bahsedebilmek için kişisel verilerin yardımcı faaliyetler için değil; veri sorumlusu veya veri işleyenin hedeflerine ulaşmak için gerekli birincil faaliyetleri için işlenmesi gerekir[253]. Örnek vermek gerekirse, bir hastanenin güvenli ve etkili bir hizmet sağlayabilmesi için hastanın sağlık kayıtları gibi sağlık verilerini işlemesi gerekir. Bu bağlamda bu verilerin işlenmesi hastanenin temel faaliyetlerinden biri olarak düşünülmeli ve hastaneler için veri koruma görevlisi belirlenmesi gerektiği sonucuna varılmalıdır[254]. Yine bir başka örnekte, özel güvenlik şirketleri işi gereği özel alan ve belki de kamusal alanları gözetlemektedir ve bu gözetleme şirketin temel faaliyetine ilişkin olup kişisel verilerin işlenmesiyle de doğrudan bağlantılıdır. Bu durumda da güvenlik şirketlerinin temel faaliyetlerini gerçekleştirebilmek için kişisel veri işlediği göz önünde bulundurulduğunda veri koruma görevlisi belirlemesinin zorunlu olduğunun kabulü gerekir.

Online satış yapan bir ayakkabıcının (A) müşterilerinin siparişlerini işlemek ve ulaştırabilmek için müşterilerin verilerini işlediği durumda veri işleme faaliyeti,

[252] Handbook on European Data Protection Law, s. 176.
[253] Tüzük, Giriş Bölümü, par. 97.
[254] Art. 29 Working Party, WP243, s. 7; IT Governance Privacy Team, s. 34.

ayakkabı satışına ilişkin ana faaliyete yardımcı bir etkinlik olduğundan burada veri koruma görevlisi belirlemek muhtemelen zorunlu olmayacaktır. Ancak aynı örnekte A'nın işlerini büyütmeyi düşündüğü ve kimin hangi şehir yahut ülkeden sipariş verdiğini analiz ettiği ihtimalinde; burada A'nın web sitesini kullanan müşterilerin, çerez kullanımını kabul etmesi gerekir ve böylelikle A, web sitesini kullananların IP coğrafi konum verilerini analiz edebilir. Bu durumda A, kaç kişinin web sitesini ziyaret ettiğini, hangi müşterilerin hangi şehir veya ülkeden sipariş verdiğini, müşterilerin hangi ürünlere talebinin ne kadar olduğunu bilmek için veri işleme faaliyetinde bulunmuş olacaktır. A'nın işlerini büyütmek için veri işleme faaliyetinde bulunmasının bir amaç ve temel faaliyet hâline geldiği göz önünde bulundurulduğunda veri koruma görevlisi belirlemesinin zorunlu olduğu söylenebilir[255].

Veri sorumlusunun veya veri işleyenin temel faaliyetlerinin; o veri sorumlusu veya veri işleyenin para kazanmasına veya para kazanma sürecinin desteklenmesine yönelik faaliyetleri kapsadığı söylenebilir[256].

Hemen hemen bütün kuruluşlar çalışanlarının maaşlarını ödemek yahut temel insan kaynakları faaliyetlerini yürütmek gibi birtakım faaliyetlerde bulunmaktadır. Burada da kişilere ilişkin veriler işlenmekte ancak bu işleme kuruluşun temel, birincil ve doğrudan para kazanmasına yönelik faaliyetlerinden ziyade bu temel faaliyetlere yardımcı ikincil fonksiyonda bir işleve sahiptir[257]. Bu sebeple, çalışanların maaşlarını ödemek için ilgili verilerin işlenmesi yahut insan kaynakları faaliyetlerinin yürütülmesi için ilgili verilerin işlenmesi her ne kadar bir kuruluş açısından kaçınılmaz olsa da bu işleme "temel faaliyet" kapsamında değerlendirilemeyeceği için bu ve benzeri veri işleme faaliyetleri ilgili kuruluşun veri koruma görevlisi belirlemesini zorunlu kılmayacaktır[258].

[255] VOIGT / von dem BUSSCHE, s. 55.
[256] SHAW, s. 3.
[257] CHIRICA, s. 163.
[258] Art. 29 Working Party, WP243, s. 7; SHARMA, s. 80.

3.2.1.2.2. Geniş Çap

Tüzük m.37/f.1 (b) ve (c) bendi, zorunlu olarak veri koruma görevlisi belirlenmesi için geniş çaplı verinin işlenmesini şart koşmuş ancak geniş çaplı işleme ile anlaşılması gerekenin ne olduğu Tüzük metninde açıklanmamıştır. Geniş çap ibaresi ile ne anlaşılması gerektiği hususunda giriş bölümü 91. paragrafta yol gösterici bir açıklamaya yer verilmiştir. Bu açıklamaya göre önemli miktarda veriyi bölgesel, ulusal veya uluslararası düzeyde işlemeyi amaçlayan ve çok sayıda veri öznesini etkileyebilecek, yüksek risk ile sonuçlanması muhtemel veri işleme faaliyeti geniş çaplı işleme sayılmaktadır. Giriş bölümü 91. paragraf, açıklamanın ardından bir de örnek vermektedir. Buna göre teknolojinin kullanımına bağlı olarak veri konularına ilişkin hak ve özgürlüklerde yüksek risk oluşturan işleme faaliyetleri gerçekleşmekte, bu faaliyetler çok geniş çaplı veri öznesini etkilemekte ve yeni teknolojilerin kullanılmasıyla veri konularına ilişkin hak ve özgürlüklerin kullanımı zorlaşmaktadır[259].

Veri işleme faaliyetinin geniş çaplı olup olmadığına ilişkin kesin rakamlara dayalı niceliksel bir değerlendirme ölçütü olmamakla birlikte Article 29 Working Party, işlemenin geniş çaplı olup olmadığını belirlerken dikkate alınacak birtakım kriterler belirlemiştir[260]. Buna göre işlemenin geniş çaplı olup olmadığını belirlemede dikkate alınacak kriterler;

- İlgili veri konularının sayısı,
- Veri hacmi veya işlenen farklı veri öğeleri aralığı,
- Veri işleme faaliyetinin süresi ve kalıcılığı,
- Veri işleme faaliyetinin coğrafi kapsamıdır.

Kamu kurum ve kuruluşları arasında elektronik ağlar üzerinden veri alışverişinde bulunulması, pazarlama ve reklam amaçlı büyük çapta "yaşam tarzı veri tabanları" oluşturulması, ülke çapında seçmenler ile yapılan görüşmeler neticesinde elde edilen verilerin kayıt ve analiz edilmesi, toplu taşıma sistemini kullanan bireylerin

[259] Tüzük, Giriş Bölümü, par. 91.
[260] Art. 29 Working Party, WP243, s. 8.

seyahat verilerinin işlenmesi büyük çapta işleme faaliyetlerine; hastaneler, bankalar, sigorta şirketleri, telekom sağlayıcıları ise büyük çapta veri işleme faaliyetinde bulunan veri sorumlularına örnektir[261].

Burada belirtmek gerekir ki net ifadelerde bulunmaktan kaçınmakta fayda bulunmaktadır. Zira genelleme yapmaktan ziyade veri koruma etki değerlendirmeleri neticesinde bir sonuca varmak daha sağlıklı sonuç verecektir.

3.2.1.2.3. Düzenli ve Sistematik İzleme

Veri öznesinin düzenli ve sistematik bir şekilde izlenmesi kavramı Tüzük'te tanımlanmamış olup giriş bölümü 24. paragrafta *"veri öznelerinin davranışlarının izlenmesi"* kavramına yer verilmiştir. Buna göre davranışsal reklamcılık faaliyetleri de dâhil olmak üzere internetteki bütün davranışsal izleme ve profil oluşturma işlemleri, veri öznelerinin davranışlarının izlenmesi anlamına gelmektedir[262]. Giriş bölümü 24. paragrafta internetteki davranışsal izlemeye yer verilmişse de davranışsal izleme yalnızca çevrimiçi ortamla sınırlı değildir; ancak çevrimiçi davranış analizi veri sahiplerinin davranışlarının izlenmesinin bariz bir örneğini teşkil etmektedir[263].

Article 29 Working Party "düzenli" kavramının yorumunda aşağıdaki tanımlamaların bir veya birçoğunu içerdiğini belirtmiştir;

- Belirli bir dönemde belirli aralıklarla devam eden veya meydana gelen,
- Belirli bir zamanda diliminde tekrarlanan,
- Sürekli veya periyodik olarak gerçekleşen[264].

Article 29 Working Party "sistemli" kavramının yorumunda aşağıdaki tanımlamaların bir veya birçoğunu içerdiğini belirtmiştir;

---

[261] KORFF / GEORGES, s. 197; SHAW, s. 3; Art. 29 Working Party, WP243, s. 8.
[262] Tüzük, Giriş Bölümü, par. 24.
[263] Leyla KESER, **Çevrimiçi Davranışsal Reklamcılık Uygulamaları Özelinde Kişisel Verilerin Korunması,** İstanbul, 2014, s. 20.
[264] Art. 29 Working Party, WP243, s. 8.

- Bir sisteme göre meydana gelen,
- Önceden düzenlenmiş, organize edilmiş veya metodik olan,
- Veri toplanması amacıyla gerçekleştirilen bir planın parçası olan,
- Bir stratejinin parçası olarak yürütülen[265].

Düzenli ve sistematik izleme faaliyetlerine telekomünikasyon ağının işletilmesi, telekomünikasyon hizmetlerinin sağlanması, belirli bir kitle hedefine e-posta gönderilmesi, risk değerlendirmesi amacıyla profil oluşturulması ve puanlama yapılması (kredi puanlaması, sigorta primlerinin değerlendirilmesi, dolandırıcılığın önlenmesi vb.), mobil uygulamalarda olduğu gibi konum izleme, sadakat programları, giyilebilir cihazlarla sağlık ve form verileri gibi birtakım verilerin izlenmesi, kapalı devre televizyon sistemleri (CCTV), akıllı araçlar ve akıllı arabalar gibi bağlantılı cihazlar örnek verilebilir[266].

3.2.1.3. Özel Nitelikli Kişisel Verilerin veya Ceza Mahkûmiyeti ve Suça İlişkin Verilerin İşlenmesi

Veri sorumlusu veya veri işleyenin temel faaliyetlerinin Tüzük m.9 uyarınca özel kategorilerdeki verilerin veya Tüzük m.10'da belirtilen mahkûmiyet kararları ve ceza gerektiren suça ilişkin kişisel verilerin büyük çaplı olarak işlenmesinden meydana gelmesi hâlinde ilgili veri sorumlusunun veya veri işleyenin veri koruma görevlisi belirlemesi gerekir.

Tüzük m.9 hükmünde özel kategorilerdeki kişisel veriler sayılmış olup bunlar; ırk veya etnik kökene ilişkin veriler, siyasi görüşler, dini veya felsefi inançlar, sendika üyeliğinin ifşa edildiği veriler, bir gerçek kişinin kimlik teşhisinin yapılmasını sağlayan genetik veriler ile biyometrik veriler, sağlık ile ilgili veriler ve bir gerçek kişinin cinsel yaşamı veya cinsel eğilimine ilişkin verilerdir. Bir veri sorumlusu veya veri işleyen tarafından, sayılan özel kategorilerdeki kişisel verilerin büyük çapta işlenmesi durumunda veri koruma görevlisi belirlenmesi Tüzük uyarınca zorunludur. Yine bir veri sorumlusu veya veri işleyen tarafından mahkûmiyet kararları ve ceza

[265] Art. 29 Working Party, WP243, s. 9.
[266] Art. 29 Working Party, WP243, s. 9; IT Governance Privacy Team, s. 35.

gerektiren suça ilişkin kişisel verilerin büyük çaplı olarak işlenmesi hâlinde de veri koruma görevlisi belirlenmesi Tüzük uyarınca zorunludur.

3.2.2. Birden Çok Kuruluş İçin Tek Bir Veri Koruma Görevlisi Belirlenmesi

Bir teşebbüs grubu "her işletmeden kolay bir şekilde erişilebilmesi" koşuluyla tek bir veri koruma görevlisi belirleyebilir. Burada Tüzük erişilebilirliği şart koşmakla, veri koruma görevlisinin, veri özneleri ve denetim makamı ile ve elbette ilgili kuruluş içerisindeki çalışanlar ile iletişim ve temas noktası olması rolüne vurgu yapmaktadır.

Veri koruma görevlisinin, dâhili veya harici olarak belirlenmiş olması[267] fark etmeksizin, erişilebilir oluşu; iletişim imkânının Tüzük gereklerine uygun olarak var olması ile sağlanacaktır. Veri koruma görevlisi veri özneleri ve denetim makamı ile, ve görev aldığı organizasyon çalışanlarıyla etkili bir şekilde iletişim kurabilecek bir pozisyonda olmalıdır. Bu aynı zamanda iletişimin, veri öznelerinin ve denetim makamının kullandığı dilde gerçekleşmesi gerektiği anlamına gelmektedir[268]. Bu sebeple ilgili kuruluşun veri koruma görevlisi belirlemeden önce dil ve iletişimde yetkinliği dikkate alması gerekir.

Tüzük m.37/f.3 düzenlemesinde birden çok kuruluş için tek bir veri koruma görevlisi belirlenmesinin kamu kurum ve kuruluşları için de söz konusu olacağı belirtilmiştir. Birden çok kamu kurum ve kuruluşu tarafından ortak, tek bir veri koruma görevlisi belirlenmesinde ilgili kuruluşun organizasyonel yapısı ve büyüklüğü gibi etkenler dikkate alınacaktır[269].

Burada belirtmek gerekir ki birden çok kuruluşun tek bir veri koruma görevlisi belirlemesinin sebebi ekonomik kaygılara da dayanabilir. Ekonomik kaygılar ile tek bir veri koruma görevlisinin birden çok kuruluş tarafından paylaşılması daha "hesaplı" bir çözüm olarak düşünülerek tercih edilebilir[270].

---

[267] Bkz. s. 83 vd.
[268] Art. 29 Working Party, WP243, s. 10; IT Governance Privacy Team, s. 36.
[269] Art. 29 Working Party, WP243, s. 22.
[270] Çek Cumhuriyeti'nde yapılan bir araştırma bu konuya örnek teşkil etmektedir. Çek Cumhuriyeti'nde bir dernek tarafından yapılan araştırmaya göre 6.300 adet belediye, 5.100 adet anaokulu ve 4.100 adet ilkokul olmak üzere 15.500 adet kamu kurum ve kuruluşunun Tüzük hükümlerine tabi olacağı düşünülmektedir. Dernek, her 20 kuruluşun ortak tek bir veri koruma görevlisi atayacağı konusunda

3.2.3. Veri Koruma Görevlisinin Uzmanlık ve Becerileri

Veri koruma görevlisi mesleki nitelikleri, veri koruma mevzuatı ve uygulamaları konusundaki uzman bilgisi ve Tüzük m.39'da asgari olarak belirlenen görevlerini yerine getirmedeki becerisine göre belirlenecektir[271]. Veri koruma görevlisi, ulusal veri koruma kanunu ve uygulamalarında uzman bilgiye ve yeteneğe sahip olmalı; bunun yanı sıra muhakkak Avrupa veri koruma mevzuatına, özellikle Tüzük'e ve uygulamalarına hâkim olmalıdır.

Veri koruma görevlisi içinde yer aldığı organizasyonun Tüzük'e uyum sürecini izleyeceğinden dolayı gerektiğinde veri koruma alanında ilgili personele eğitim verebilmeli; mevzuat ve teknolojideki değişiklikleri ve gelişmeleri takip edip veri koruma programının nasıl organize edileceğini, yürütüleceğini, uygulanacağını ve gerektiğinde mutlaka güncelleneceğini bilmelidir.

Veri koruma görevlisinin veri koruma yasaları ve veri koruma uygulamaları konusunda uzman bilgiye ve Tüzük kapsamındaki görevlerini yerine getirme yeteneğine sahip olmasının yanı sıra bilgi teknolojileri konusunda da teknik bilgiye sahip olması gerekmektedir. Bilgi teknolojisindeki gelişmeler ile kişisel verilerin işlenmesinin kolaylaşması ve işleme faaliyetinde bilgi teknolojisinden faydalanılması, bu teknik bilgi donanımına sahip olmayı bir anlamda zorunlu kılmaktadır.

İşleme faaliyetlerinde bilgi teknolojilerinden faydalanıldığı gibi buna ek olarak günümüzde verilerin elektronik ortamlarda depolanması sebebiyle veri güvenliği de

---

hemfikir olacağını tahmin etmektedir. Bu tahmin sabit verilere dayanmıyor olmakla beraber, özellikle insan kaynakları uzmanları ile işbirliği içinde olan derneğin tahminlerine göre ortalama 775 adet veri koruma görevlisine ihtiyaç duyulacağı öngörülmüştür. Yine dernek tarafından veri koruma görevlisinin kamu kurum ve kuruluşlarına maliyetinin yaklaşık olarak hesap edilmesinde; her bir veri koruma görevlisinin aylık maliyetinin yaklaşık olarak 55.000 Çek Korunası (CZK) olması ihtimalinde yıllık maliyetinin 775 (veri koruma görevlisi sayısı) * 55.000 CZK * 12 (ay) = 511.500.000 CZK olacağı tahmin edilmiştir. Bu miktar da Çek Cumhuriyeti'nde ekonomik kaygılar ile özellikle yerel ve bölgesel nitelikte kamu kurum ve kuruluşlarının ortak bir veri koruma görevlisini paylaşma eğiliminde olacakları ihtimalini güçlendirmektedir. Merkezileşme ne kadar küçükse bir veri koruma görevlisi için ayrılacak bütçe o kadar az olacak ve veri koruma görevlisini paylaşma oranı o denli artacaktır. Eva Daniela CVIK/ , Radka MacGregor PELIKÁNOVÁ / Michal MALÝ, **"Selected Issues from the Dark Side of the General Data Protection Regulation"**, Review of Economic Perspectives, C.18, S.4, 2018, s. 396.

[271] Europen Data Protection Supervisor (EDPS), **"Position Paper On The Role Of Data Protection Officers Of The EU Institutions And Bodies"**, 30.09.2018, s. 6 (Çevrimiçi) https://edps.europa.eu/sites/edp/files/publication/18-09-30_dpo_position_paper_en.pdf

şüphesiz ki bilgi teknolojileri sayesinde sağlanacaktır. Veri güvenliğinin sağlanması için verilerin şifrelenmesi, verilerin saklanması veya taşınmasında şifreleme algoritmalarının kullanılması, verilere erişim kontrolünün sağlanması, erişim kontrolünü sağlamak adına erişimin kısıtlanması gibi güvenlik önlemleri teknik önlemler ile sağlanmaktadır. Dolayısıyla veri güvenliğinin sağlanabilmesi noktasında da veri koruma görevlisinin bilgi teknolojileri konusunda bilgi sahibi olması gerekliliği kaçınılmazdır.

Veri koruma görevlisinin bilgi teknolojileri konusunda bilgi sahibi olması gerekliliği, ülkelerin veri koruma otoriteleri tarafından da kabul edilmekte ve veri koruma görevlisinin uzmanlık ve becerileri belirlenirken bilgi teknolojileri konusunda bilgi sahibi olması gerekliliği vurgulanmaktadır. Örneğin Fransız Veri Koruma Otoritesi CNIL (Commission nationale de l'informatique et des libertés)[272], veri koruma görevlisinin uzmanlık ve becerilerine ilişkin olarak; veri koruma görevlisinin veri yönetimi, işletme sistemleri, yazılım yöntemleri, dosya ve veri depolama sistemleri, gizlilik gereksinimleri ve güvenlik politikalarına ilişkin veri şifreleme, elektronik imza, biyometri vb. konular hakkında bilgi sahibi olması gerekliliğini ayrıca ve özellikle belirtmiştir[273].

3.2.3.1. Görev Alınan Kuruluşun Faaliyet Konusu

Veri koruma görevlisi belirlemede dikkate alınacak gerekli uzmanlık ölçütü Tüzük'te tanımlanmamıştır. Ancak Tüzük'ün giriş bölümünün 97. paragrafında veri koruma görevlisinin uzmanlık bilgisi düzeyine ilişkin bir açıklamaya yer verilmiş olup buna göre veri koruma görevlisinin gerekli uzmanlık bilgisi düzeyi, yürütülen veri işleme operasyonlarına ve veri sorumlusu veya veri işleyen tarafından işlenen kişisel veriler için gerekli korumaya göre belirlenmelidir. Bu açıklamaya göre veri koruma görevlisinde aranacak uzmanlık ölçütü; yer aldığı kuruluşun büyüklüğü, işlenen verilerin niteliği (örneğin hassas veri işlenmesi) ve miktarına bağlı olarak

[272] Fransız Veri Koruma Otoritesi CNIL hakkında ayrıntılı bilgi için bkz. Çağla TANSUĞ, "**Fransız Hukukunda Veri Koruma Otoritesi: CNIL"**, Yeditepe Üniversitesi Hukuk Fakültesi Dergisi, C.14, S.2, 2017, s. 335-353.

[273] https://www.cnil.fr/sites/default/files/typo/document/CNIL_Guide_correspondants.pdf ; KORFF / GEORGES, s. 126.

değerlendirilecektir. Bir başka deyişle veri koruma görevlisinde aranacak gerekli uzmanlık bilgisi ve yetenek, görev alınan kuruluşun faaliyet konusuna bağlı olarak değişkenlik gösterebilir.

Bu çerçevede veri koruma görevlisinin, içinde bulunduğu kuruluşun faaliyet konusuna ilişkin özel mevzuat hükümlerine hâkim olması gerekecektir. Örneğin, faaliyet alanı elektronik ticarete ilişkin olan veyahut işletme konusu fark etmeksizin elektronik ticaret faaliyetine ilişkin işlemlerde bulunan bir kuruluşta görev alan veri koruma görevlisinin 6563 sayılı Elektronik Ticaretin Düzenlenmesi Hakkında Kanun'u ve bu Kanun'da yer alan kişisel verilere ilişkin hükümleri bilmesi; işletme faaliyetine ilişkin özel mevzuat ile kişisel verilere ilişkin mevzuat hükümlerini bir arada değerlendirme ve muhakeme yetkinliğine erişmiş olması gerekir.

6563 sayılı Kanun'un 10. maddesinde kişisel verilerin korunmasına ilişkin özel bir düzenleme yer almaktadır. Bu madde hükmünün birinci fıkrasına göre hizmet sağlayıcılar ve aracı hizmet sağlayıcılar bu Kanun çerçevesinde yapmış olduğu işlemler nedeniyle elde ettiği kişisel verilerin saklanmasından ve güvenliğinden sorumludur. Yine hükmün ikinci fıkrasına göre hizmet sağlayıcılar ve aracı hizmet sağlayıcılar, kişisel verileri ilgili kişinin onayı olmaksızın üçüncü kişilere iletemez ve başka amaçlarla kullanamaz.

Elektronik ticaret alanında faaliyet gösteren bir veri sorumlusu tarafından tayin edilen veri koruma görevlisinin saklanması gerekli kişisel verilerin ne olduğunu[274], hizmet sağlayıcı veya aracı hizmet sağlayıcı tarafından talep edilmediği hâlde alıcı tarafından girilen kişisel verilerin de korumadan yararlanıp yararlanamayacağını[275], internet üzerinden yapılan bir alışverişte ödeme bilgilerine ilişkin verilerin saklanmasına ilişkin özel bir düzenlemenin olup olmadığını[276] bilmesi ve bu konulara ilişkin mevzuat hükümlerine hâkim olması gerekir.

[274] Harun DEMİRBAŞ, **6563 Sayılı Elektronik Ticaretin Düzenlenmesi Hakkında Kanun Kapsamında Hizmet Sağlayıcıları ve Aracı Hizmet Sağlayıcılarının Yükümlülükleri,** Ankara, 2015, s. 60.
[275] DEMİRBAŞ, s. 64.
[276] DEMİRBAŞ, s. 68.

Yalnızca kişisel verilerin korunmasına ilişkin genel mevzuat hükümlerini bilmek kişisel verilerin ihlaline sebebiyet verecek iş ve eylemlerde bulunmaya neden olabilir. Türk hukukunda kişisel verilerin korunmasına ilişkin 6698 sayılı Kanun'un 8. maddesinin 1. fıkrasında *"kişisel veriler, ilgili kişinin açık rızası olmaksızın aktarılamaz"*, 3. fıkrasında "*kişisel verilerin aktarılmasına ilişkin diğer kanunlarda yer alan hükümler saklıdır"* hükmüne yer verilmiştir. Hükmün ilk fıkrasında genel bir düzenlemeye yer verilmiş iken son fıkrada kişisel verilerin aktarılmasına ilişkin diğer kanun hükümlerinin saklı olduğuna vurgu yapılarak istisnaların olabileceği belirtilmiştir.

Burada istisnalara ilişkin bir örnek vermek gerekirse, 5464 sayılı Banka Kartları ve Kredi Kartları Kanunu'nun m.23 hükmünde üye iş yerlerinin, kart hamilinin rızası olsa bile ödeme sırasında elde edilen kart bilgilerini üçüncü kişilerle paylaşamayacağı, satamayacağı, satın alamayacağı ve takas edemeyeceği kararlaştırılmıştır[277]. Mal veya hizmet satışı yapan bir kuruluşta görev yapan veri koruma görevlisinin, alıcı kart hamilinin kart bilgilerinin 6698 sayılı Kanun'da öngörülen açık rıza olsa bile üçüncü kişilerle paylaşılamayacağını, banka kartları ve kredi kartlarına ilişkin özel bir düzenlemenin var olduğunu bilmesi gerekir.

Veri koruma görevlisinin çalıştığı kuruluşun faaliyet konusuna ilişkin özel mevzuat hükümlerine hâkim olması gerekliliğine dair kamu kurum ve kuruluşlarından bir örnek vermek gerekirse, kişilerin vergisel ve mali durumları da kişisel veri sayılmakta ve verginin gerek tahakkuk gerek tahsil aşamasına ilişkin kanunlarda vergi mahremiyetini koruyucu hükümler yer almaktadır. Vergi mahremiyetinde tahakkuk aşamasında elde edilen verilere ilişkin 213 sayılı Vergi Usul Kanunu'nun 5. maddesinin 1. fıkrasında; vergi muameleleri ve incelemeleri ile uğraşan memurların, vergi mahkemeleri, bölge idare mahkemeleri ve Danıştay'da görevli olanların, vergi kanunlarına göre kurulan komisyonlara iştirak edenlerin, vergi işlerinde kullanılan bilirkişilerin görevleri dolayısıyla, mükellefin ve mükellefle ilgili kimselerin şahıslarına, muamele ve hesap durumlarına, işlerine, işletmelerine, servetlerine veya mesleklerine müteallik olmak üzere öğrendikleri sırları veya gizli kalması lazım gelen

[277] DEMİRBAŞ, s. 72.

diğer hususları ifşa edemeyecekleri ve kendilerinin veya üçüncü şahısların yararına kullanamayacakları hüküm altına alınmıştır[278].

Vergi borcunun tahsili aşamasındaki mahremiyet ve sır saklama yükümlülüğüne ilişkin ise 6183 sayılı Amme Alacaklarının Tahsili Usulü Hakkındaki Kanun'un 107. maddesinde özel bir düzenlemeye yer verilmiş olup 1. fıkra hükmüne göre; 6183 sayılı Kanun'un tatbikinde vazifeli bulunan kimselerin, bu vazifeleri dolayısıyla amme borçlusunun ve onunla ilgili kimselerin şahıslarına, mesleklerine, işlerine, muamele ve hesap durumlarına ait öğrendikleri sırlarla, gizli kalması lazım gelen diğer hususları ifşa ettikleri takdirde cezalandırılacağı kararlaştırılmıştır. Hangi bilgilerin paylaşılmasının suç sayılmayacağı ise aynı maddenin 2. fıkrasında belirtilmiştir[279].

Her iki Kanun uyarınca mahremiyet ihlali durumunda TCK m.239'da düzenlenen *ticarî sır, bankacılık sırrı veya müşteri sırrı niteliğindeki bilgi veya belgelerin açıklanması* suçundan ceza verilecektir.

Kişilerin mali durumuna ilişkin ve vergi mahremiyetinin ihlaline ilişkin özel düzenlemeler var olduğundan, verginin tahakkuk ve tahsilinde görevli bir kamu kurum ve kuruluşunda görev alan veri koruma görevlisinin de yine veri koruma kanunu haricindeki mevzuat hükümleri hakkında bilgi sahibi olması beklenecektir.

3.2.3.2. Yetkinliğe İlişkin Belgelendirme

Tüzük'te veri koruma görevlisinin yetkinliğine ilişkin bir belgelendirme yöntemi kararlaştırılmamıştır. Tüzük'ün *"Belgelendirme"* başlıklı 42. maddesinde belgelendirme yönteminden bahsedilmektedir; ancak bu belgelendirme veri koruma görevlisi hakkında değil, veri sorumlusu ve veri işleyene ilişkindir. İlgili hükümde veri sorumluları ve veri işleyenler tarafından gerçekleştirilen işleme faaliyetlerinin Tüzük ile uyumluluğunun gösterilmesi amacıyla, veri koruma belgelendirme mekanizmaları ve veri koruma mühürleri ve işaretlerinin oluşturulmasının teşvik edileceği düzenlenmiştir. Ayrıca madde metninde bu belgelendirmenin gönüllülük esasına

[278] Neslihan KARATAŞ DURMUŞ, **"Ticari Sırların Ve Kişisel Verilerin Korunması Kapsamında Vergi Mahremiyeti",** Türkiye Adalet Akademisi Dergisi, S.31, Temmuz 2017, s. 380.
[279] KARATAŞ DURMUŞ, s. 382.

dayanacağı belirtilmiş olup belgelendirme, veri sorumlusu veya veri işleyenin veri işleme süreçlerinin hukuka uygunluğunu göstermek amacıyla öngörülmüştür[280].

Veri koruma görevlisinin uzman bilgi ve yeteneğe sahip olduğunun nasıl tespit edileceği sorusu akla gelmektedir. Bu soruya AB üye ülkelerinin uygulamada bulduğu çözümler cevap olabilir. Ancak genel kabul görmüş bir düzenlemenin olmayışı üye ülkelerde birbirinden farklı uygulamalar ortaya konmasına sebep olmuştur.

AB üye ülkelerinin uygulamalarına bakıldığında, İspanya'da veri koruma görevlisi için resmi bir belgelendirme yapılması yönünde çalışmalar yapılmış olup bu belgelendirme ISO 17024'e (Personel belgelendirme faaliyetlerinin akreditasyonu) dayanmaktadır. Bu çalışmaya göre, İspanyol Veri Koruma Otoritesi'nce (Agencia Española de Protección de Dato) geliştirilen kriterlere ve resmi bir sınava dayanan, Ulusal İspanyol Akreditasyon Ajansı tarafından akredite edilen sertifika kuruluşlarınca verilen bir sertifikasyon programı hazırlanmıştır[281].

İspanya'da belgelendirme konusunda ISO 17024'e dayanılmasının, ISO 17024'ün personel yeteneklerine ilişkin olduğu dikkate alındığında isabetli bir tercih olduğu söylenebilir[282].

Fransa'da veri koruma görevlisinin sertifikasyonuna ilişkin Fransız Veri Koruma Otoritesi (CNIL) tarafından belirlenmiş ve 11 Ekim 2018 tarihinde ulusal Resmi Gazete'de yayınlanmış iki düzenleme yer almaktadır. Bunlardan ilki başvuruların kabul edilebilirlik koşulları ile veri koruma görevlisinin sertifikalandırılmasına ilişkin 17 kriter öngören sertifika referans sistemine (belgelendirme kriterleri)[283] ilişkin iken ikinci düzenleme ise Fransız Veri Koruma Otoritesi tarafından hazırlanan ve sertifikasyon ölçütüne dayanarak akredite olabilmek için kuruluşların yerine getirmesi gereken kriterleri belirleyen akreditasyon

[280] ÇEKİN, s.233.
[281] KORFF / GEORGES, s. 128.
[282] IT Governance Privacy Team, s. 41.
[283] https://www.legifrance.gouv.fr/affichTexte.do;jsessionid=46002F5EFD8F35A73251FDC7949EEDB6.tplgfr26s_2?cidTexte=JORFTEXT000037485691&dateTexte=&oldAction=rechJO&categorieLien=id&idJO=JORFCONT000037485359 (Erişim:07.04.2020).

ölçütüne[284] ilişkindir[285]. Fransa da, İspanya ile benzer şekilde belgelendirme kuruluşu olarak akredite olabilmek için başvuruda bulunan belgelendirme kuruluşlarının *ISO/IEC 17024:2012 sertifikasına* sahip olmasını akreditasyon ölçütü olarak kabul etmiştir.

Fransız Veri Koruma Otoritesi, veri koruma görevlisi olarak görev yapabilmek için belirlenen standartlara göre belgelendirilmenin zorunlu olmadığını, bu belgelendirmenin bir ön koşul değil, aksine veri koruma görevlisinin Tüzük'ün gerektirdiği şekilde uzman bilgi ve yeteneğe sahip olduğunu kanıtlamaya yarar bir araç niteliğinde olduğunu belirtmiştir[286].

Almanya'da ise veri koruma görevlilerine yönelik çeşitli kurs ve eğitim programları düzenlenmektedir ve bu kurs ve eğitim programlarının bir kısmı sertifikasyon programı şeklinde yapılmaktadır. Ancak bu eğitimler resmi makamlar tarafından organize edilmemekte, özel eğitim programı şeklinde yapılmaktadır[287].

Çeşitli ülkelerdeki uygulamalara baktığımız zaman veri koruma görevlisine ilişkin kurs ve eğitim programlarının birçoğu, katılımcılara özellikle Tüzük konusunda uzmanlık kazandırmayı ve Tüzük kapsamında veri koruma görevlisine verilen görev ve işlere ilişkin rehberlik etmeyi amaçlamaktadır[288]. Veri koruma görevlisinin belirlenmesi noktasında elbette belli nitelikler aranacak ve bu niteliklerin varlığını değerlendirebilme ihtiyacı doğacaktır. Bu ihtiyaca istinaden gelecekte devletlerin resmi olarak tanınmış veya desteklenen programlar hazırlamaları muhtemeldir. Bu programların hazırlanmasında Avrupa Veri Koruma Kurulu'nun (EDPB) kılavuz niteliğinde çalışmalarının olması devletlere rehberlik anlamında kolaylık sağlayacak bir uygulama olarak akla gelmektedir. Bunun haricinde bu programların Avrupa Veri Koruma Kurulu tarafından onaylanması ihtimali de söz konusu olabilir.

---

[284] https://www.legifrance.gouv.fr/affichTexte.do;jsessionid=46002F5EFD8F35A73251FDC7949EEDB6.tplgfr26s_2?cidTexte=JORFTEXT000037485671&dateTexte=&oldAction=rechJO&categorieLien=id&idJO=JORFCONT000037485359 (Erişim:07.04.2020).

[285] KORFF / GEORGES, s. 128.

[286] https://www.cnil.fr/sites/default/files/atoms/files/cnil_certification-scheme-dpo-skills-and-knowledge.pdf (Erişim:07.04.2020).

[287] KORFF / GEORGES, s. 128.

[288] Uluslararası Mahremiyet Uzmanları Birliği (IAPP) tarafından da veri koruma görevlisinin yetkinliğine ilişkin GDPR bilgi, perspektif ve anlayışına sahip olmayı amaçlayan CIPP/E sertifika programı geliştirilmiştir. https://iapp.org/certify/cippe/ (Erişim:07.04.2020).

Veri koruma görevlisinin uzmanlık ve becerilerine ilişkin son olarak, veri koruma görevlisinin güçlü iletişim becerilerine ve yabancı dil yetkinliğine sahip olması gerekliliğine değinilebilir. Veri koruma görevlisinin bulunduğu kuruluş içerisinde yönetim kurulu gibi üst düzey yöneticiler, veri özneleri ve veri koruma otoritesi ile iletişim hâlinde olması gerektiği düşünüldüğünde güçlü iletişim becerilerine sahip olması gerekliliği kaçınılmazdır. Ayrıca veri koruma görevlisi ilgili veri öznesi ve veri koruma otoriteleri ile iletişim kuracağından, bu durum aynı zamanda ilgili veri öznesi ve veri koruma otoriteleri ile aynı dili konuşabilmeyi gerektirir. Ancak burada örnek vermek gerekirse, AB ülkelerinde veri işleme faaliyetinde bulunan bir kuruluşta görev alan veri koruma görevlisinin AB ülkelerinde konuşulan her dili bilmesi gerektiği sonucuna varmak gerçekçi bir yaklaşım olmayacaktır.

3.2.3.3. Hukukçu Kimliğe Gereksinim

Veri koruma görevlisinin hukukçu kimliğe sahip olması gerekip gerekmediğine ilişkin açıklama yapmadan önce belirtmek gerekir ki veri koruma görevlisi rolüne kim belirlenirse belirlensin çıkar çatışması yaratabilecek kişiler olmamalıdır. Örneğin, görev aldığı organizasyonda avukat olan bir kişinin veri koruma görevlisi olarak belirlenmesi ihtimalinde, olası bir çıkar çatışmasına neden olabilecek herhangi bir idari veya yasal işlemde görev aldığı organizasyonu temsil yetkisinden muaf tutulması sağlanmalıdır. Yine konuya ilişkin bir başka örnek vermek gerekirse, Almanya'da veri koruma görevlisinin bilgi güvenliği operasyonlarındaki bağımsızlığına vurgu yapılarak bilgi işlem yöneticisinin rolü veri koruma görevlisi için çıkar çatışmasına sebep olabileceği gerekçesiyle uygun kabul edilmemiştir[289].

Tüzük'te veri koruma görevlisinin hangi meslek grubundan olacağına ilişkin bir düzenlemeye yer verilmemiştir. Kişisel verilerin korunmasında hukuk ve bilgi teknolojileri olmak üzere iki önemli etmen olduğu yadsınamaz bir gerçektir. Veri koruma görevlisi belirleyecek bir veri sorumlusunun yahut veri işleyenin özellikle bu iki alana ilişkin meslek grubundan kimseleri belirlemesi yerinde bir tercih olacaktır.

[289] https://iapp.org/news/a/german-company-fined-for-dpo-conflict-of-interest/ (Erişim:08.04.2020).

Veri koruma mevzuatına ve uygulamalarına, mahkemelerce verilen kararlara hâkim bir avukat yahut bilgi güvenliği konusunda uzmanlaşmış bir bilgi güvenliği uzmanı, veri koruma görevlisi olarak belirlemek için akla gelen ilk mesleklerdir[290].

Gelişen teknolojiyi anlamak giderek daha ehemmiyet kazandığından, veri koruma görevlisinin bilgi güvenliği kontrollerinden anlama, şifreleme ve benzeri bilgi güvenliği işlemleri ile başa çıkabilme yetkinliğine sahip olması avantaj sağlayacaktır. Bilgi güvenliği uzmanları risk konusunda ve bilgi güvenliğine ilişkin teknik meselelerde hukukçulara göre daha elverişli bir meslek grubu sayılabilecek iken hukukçuların ise müzakere yeteneği ve veri koruma yasalarında bilgi sahipliği noktasında bilgi güvenliği uzmanlarından daha fazla deneyim sahibi olduğu söylenebilir.

Veri koruma görevlisinden ülkesinde geçerli veri koruma mevzuatına, AB düzenlemelerine ve veri koruma uygulamalarına, ulusal ve uluslararası mahkemelerde verilen kararlara hâkim olması ve gerektiğinde yasal tavsiyede bulunup analiz yapabilmesi beklenir. Hukuku meslek edinmiş olan bir veri koruma görevlisini bilgi güvenliği uzmanı olan bir veri koruma görevlisinden ayıran en önemli farklardan birisi de bu özelliklere sahip oluşudur. İlk başta veri koruma görevlisi rolüne bir hukukçunun belirlenmesi hâlinde bilgi güvenliğine ilişkin teknik meselelerde yetkinlik konusunda endişe duyulması ihtimali akla gelse de hukukçu bir veri koruma görevlisi, veri koruma ekibinde deneyimli bir bilgi güvenlik denetçisine yer vererek pek ala bu endişeyi giderebilir. Kanaatimizce veri koruma görevlisi rolüne veri koruma hukuku alanında uzmanlaşmış ve deneyim sahibi, gizlilik ve teknoloji odaklı bir hukukçu belirlemek en elverişli ve yerinde bir tercih olarak söylenebilir.

Veri koruma görevlisinin, veri koruma hukukuna ilişkin yasal mevzuatın yalnızca ne söylediğini değil ne anlama geldiğini ve görev alınan organizasyonda nasıl uygulanacağını da bilmesi gerekir ki bu husus ancak hukuki muhakeme yeteneği ile başarılabilecektir. Hukuku meslek edinmemiş bir kimse de pek tabii yasayı bilebilir; ancak yasayı pratikte uygulamak konusunda hukuku meslek edinmiş bir kimsenin diğer meslek gruplarına göre daha tecrübeli olduğunun da kabulü gerekir. Ayrıca veri

[290] https://iapp.org/news/a/two-pros-square-off-must-the-dpo-be-a-lawyer/ (Erişim:08.04.2020).

koruma görevlisinin hukukçu olması, veri konularına ilişkin taleplerin daha etkin bir biçimde ele alınabilmesi ve cevaplanabilmesi hususunda da bilgi güvenliği uzmanlarına göre avantajlı sayılabilir.

3.2.4. Veri Koruma Görevlisinin Dâhili veya Harici Olarak Belirlenmesi

Veri koruma görevlisi, veri sorumlusunun veya veri işleyenin dâhili bir personeli olabileceği gibi harici model tercih edilerek dış kaynaktan hizmet alınması yoluyla da veri koruma görevlisi belirlenebilir[291]. Dâhili veya harici, hangi modelin veri sorumlusunun veya veri işleyenin ihtiyaçlarını en iyi şekilde karşıladığı, işletmenin somut veri işleme faaliyetlerinin yanı sıra büyüklüğü ve bütçesine göre belirlenmelidir. Yüksek riskli veri işleme faaliyetinde bulunan, büyük çaplı işletmeler veya grup şirketleri dâhili veri koruma görevlisi modelini uygularken küçük veya orta ölçekli işletmelerin harici modeli uygulamaları yerinde bir tercih olacaktır[292]. Örneğin Fransız Veri Koruma Otoritesi (CNIL) veri koruma görevlisinin, tercihen ilgili organizasyonun bir çalışanı olması gerektiğini belirtirken hemen akabinde küçük ve orta ölçekli işletmeler için bunun her zaman mümkün olmadığını vurgulamıştır[293].

Esasında bu değerlendirme, bir işletmenin işleyişini en iyi o işletmede bizzat faaliyet gösteren çalışanların bilmesinin bir sonucu olarak ortaya çıkmıştır. Veri işleme faaliyeti ne kadar risk barındırıyor veya bir işletme ne kadar büyük ise o işletmede her an var olabilecek ve işletmede yer almasından dolayı kolay ulaşılabilecek dâhili bir veri koruma görevlisi daha elverişli bir seçenek olarak akla gelmektedir. Ancak veri koruma görevlisinin dâhili olarak belirlenmesi ihtimalinde çıkar çatışmasına neden olmamasına dikkat edilmelidir.

Dâhili veri koruma görevlisini kolay ulaşılabilir ve ilgili işletme hakkında daha çok fikir sahibi olmasından dolayı daha verimli kabul eden görüşün aksi de mevcuttur[294]. Bu görüş, veri koruma görevlisinin harici olarak belirlenmesi

[291] Prashant MALI, **GDPR Articles With Commentary & EU Case Laws,** Cyber Infomedia, 2019, s. 86.
[292] VOIGT / von dem BUSSCHE, s. 58.
[293] KORFF / GEORGES, s. 126.
[294] IT Governance Privacy Team, s. 45.

durumunda harici olarak bu işi yapan veri koruma görevlisinin bir değil birden çok işletme ile muhatap olacağından ve aynı veya benzer sektör içindeki bir dizi kuruluş için aynı rolü yerine getireceğinden dolayı bu sektörü etkileyen belirli veri koruma sorunları hakkında daha fazla bilgiye ve tecrübeye sahip olması nedeniyle daha avantajlı görmektedir.

Dâhili veri koruma görevlisi veri sorumlusu veya veri işleyenin bir çalışanı iken veri koruma görevlisinin harici olarak belirlenmesi durumunda görevlerini veri sorumlusu veya veri işleyen arasında akdedecekleri sözleşmeye dayalı olarak yerine getirecektir. Veri koruma görevlisinin harici olarak belirlenmesi durumunda, belirlenen veri koruma görevlisi gerçek kişi olabileceği gibi tüzel kişi de olabilir. Tüzük'te gerçek kişinin veya tüzel kişinin veri koruma görevlisi olarak belirlenip belirlenemeyeceğine ilişkin ayrıca bir düzenlemeye yer verilmemiştir. Veri koruma görevlisinin gereksinimleri bir gerçek kişinin nitelikleriyle bağlantılı olmadığından ve Tüzük m.37 hükmü veri koruma görevlisinin tüzel kişi olma ihtimalini açıkça dışlamadığından dolayı tüzel kişinin de veri koruma görevlisi olabilmesi mümkün kabul edilmelidir. Özellikle uygulamada harici olarak belirlenmesi durumunda veri koruma görevlisinin genellikle tüzel kişiliği haiz danışmanlık firmaları olması muhtemeldir. Ancak burada belirtmek gerekir ki görevlendirilen her bir kimsenin Tüzük'ün dördüncü kısmında yer alan tüm gereksinimlere uygunluğunun sağlanması gerekir[295].

Harici olarak veri koruma görevlisi belirlenmesi ihtimalinde, ilgili organizasyonda ilgili kişilerle iletişime geçecek özellikle bir kişinin belirlenmesi gerekir. Tüm bu ayrıntılar veri sorumlusu veya veri işleyen tarafından yayınlanmalı ve veri koruma otoritesine bildirilmelidir[296].

Tüzük, veri koruma görevlisinin belirlenmesi için resmi bir gereklilik öngörmediği gibi görev süresi de belirlememiştir. Ancak veri koruma görevlisinin sınırlı bir süre için belirlenmesi ihtimali de dışlanmamıştır. Esasında, Tüzük'ün tasarı metninde veri koruma görevlisinin en az iki yıl süreyle belirlenmesi ve görev süresi

[295] Art. 29 Working Party, WP243, s. 12.
[296] SHARMA, s. 80.

boyunca veri koruma görevlisinin ancak görevlerinin gereklerini yerine getirmemesi durumunda görevden alınabileceği öngörülmüşse de Tüzük'ün nihai metninde böyle bir düzenlemeye yer verilmemiştir[297].

Burada ülkemiz açısından bir değerlendirme yapmak gerekirse, daha evvel belirttiğimiz ve çalışmamızın ilerleyen bölümlerinde daha ayrıntılı şekilde ele alacağımız üzere Türk mevzuatında henüz veri koruma görevlisine yer verilmemiş olmakla birlikte kişisel verilerin korunmasına ilişkin yapılacak yeniliklerin veri koruma görevlisi kurumunu da kapsaması muhtemeldir. Bu durumda veri koruma görevlisinin belirlenmesi noktasında Tüzük ile paralel şekilde dâhili veya harici belirleme şeklinde iki seçenek söz konusu olabilir.

Veri koruma görevlisinin dâhili veya harici olarak belirlenmesi durumunda veri sorumlusu veya veri işleyen ile veri koruma görevlisi arasındaki hukuki ilişkinin hangi sözleşme kapsamında kurulacağı sorusu akla gelecektir. Burada sorunun cevabı olarak TBK'da yer alan iş görme borcu doğuran sözleşmelerden hizmet sözleşmesi ve vekâlet sözleşmesi değerlendirilebilir.

Hizmet sözleşmesi, TBK'nın 393. maddesinde tanımlanmış olup; *işçinin işverene bağımlı olarak belirli veya belirli olmayan süreyle iş görmeyi ve işverenin de ona zamana veya yapılan işe göre ücret ödemeyi üstlendiği sözleşmedir.* Tanım maddesinden anlaşılacağı üzere bağımlılık, zaman, iş görme ve ücret hizmet sözleşmesinin esaslı unsurlarını oluşturmaktadır[298]. Hizmet sözleşmesi hukuki niteliği gereği tam iki tarafa borç yükleyen bir sözleşme olup işçi, işverenin iş organizasyonu içerisinde iş görür.

TBK m.395-400 uyarınca hizmet sözleşmesi kapsamında işçinin borçları; bizzat çalışma borcu, özen ve sadakat borcu, teslim ve hesap verme borcu, fazla çalışma borcu, düzenleme ve talimatlara uyma borcudur.

---

[297] Art. 35 Sec. 7 Proposal of the European Commission for the GDPR, Brussels, 25.1.2012 COM(2012) 11 final 2012/0011 (COD).

[298] Mustafa Alper GÜMÜŞ, **6098 sayılı Türk Borçlar Kanunu'na Göre Borçlar Hukuku Özel Hükümler,** C.I, 3.Baskı, İstanbul, 2013, s. 382-384; Cevdet YAVUZ / Faruk ACAR / Burak ÖZEN, **Borçlar Hukuku Dersleri Özel Hükümler,** 8.Baskı, İstanbul, 2010, s. 300-305; Fikret EREN, **Borçlar Hukuku Özel Hükümler,** 4.Baskı, Ankara, 2017, s. 534; Murat AYDOĞDU / Nalan KAHVECİ, **Türk Borçlar Hukuku Özel Borç İlişkileri Sözleşmeler Hukuku,** 4.Baskı, Ankara, 2019, s. 730-732.

Hizmet sözleşmesini diğer iş görme sözleşmelerinden ayıran en önemli ve temel unsur bağımlılıktır[299]. Buna göre işçi, iş görme edimini işveren ile kişisel, organizasyonel ve ekonomik yönden bağımlılık ilişkisi içerisinde yerine getirir[300]. Kişisel bağımlılık, işçinin işverenin emir ve talimatlarına uygun olarak iş edimini yerine getirmesi ve işverene hesap vermesi olarak somutlaşmakta iken; organizasyonel bağımlılık bakımından işçi işverenin araç, gereç ve malzemelerini kullanmakta ve bizzat işverenin belirlediği iş organizasyonu içerisinde yer almaktadır. Ekonomik bağımlılık ise işçinin bir ücret karşılığında iş görme edimini işverenin emrine sunması anlamına gelmektedir.

Vekâlet sözleşmesi TBK'nın 502. maddesinde tanımlanmış olup; *vekilin vekâlet verenin bir işini görmeyi veya işlemini yapmayı üstlendiği sözleşmedir.* Vekâlet sözleşmesi ile vekil, vekâlet verenin çıkarına ve iradesine uygun olarak bir zaman kaydına tabi olmaksızın ve nispeten bağımsız şekilde iş görme borcu altına girer.

TBK m.505-509 uyarınca vekâlet sözleşmesi kapsamında vekilin borçları; vekâlet verenin talimatlarına uyma borcu, vekâlet borcunu bizzat ifa borcu, sadakat ve özen borcu, vekâlet verene yürüttüğü işin hesabını verme borcu ve iade borcudur[301]. Ücret, vekâlet sözleşmesinin zorunlu unsuru olmayıp vekâlet sözleşmesi prensip itibariyle tek tarafa borç yükleyen sözleşmedir[302]. Ancak vekâlet verenin ücret ödeme borcu altına girdiği durumda tam iki tarafa borç yükleyen bir sözleşmenin varlığı kabul edilecektir.

Hizmet sözleşmesinde yer alan bağımlılık unsuru, veri koruma görevlisinin görev aldığı organizasyonda bağımsız olması ve bağımsızlığını sağlamaya yönelik işvereni olacak veri sorumlusu veya veri işleyen tarafından özellikle koruyucu hükümler getirilmesi gerekliliği ile çelişiyor gibi gözükse de bağımlılık unsurunun

[299] GÜMÜŞ, s. 384; YAVUZ / ACAR/ ÖZEN, s. 301; EREN, s. 535; Sinan Sami AKKURT, **"Türk Özel Hukukunda İş Sözleşmesi ile Eser Sözleşmesinden Kaynaklanan Başlıca Yükümlülükler ve Anılan Sözleşmelerin Ayırt Edilmesi"**, Dokuz Eylül Üniversitesi Hukuk Fakültesi Dergisi, C.10, S.2, 2010, s. 18.
[300] GÜMÜŞ, s. 384; AYDOĞDU / KAHVECİ, s. 731.
[301] Fahrettin ARAL / Hasan AYRANCI, **Borçlar Hukuku Özel Borç İlişkileri,** 9.Baskı, Ankara, 2012, s. 400; YAVUZ / ACAR / ÖZEN, s. 461.
[302] YAVUZ / ACAR / ÖZEN, s. 451; AYDOĞDU / KAHVECİ, s. 791.

göreceli olduğu ve işin niteliğine göre değişebileceği kabul edilmektedir. Bağımlılık unsuru işçinin iş yerindeki statüsü ve çalışma ilişkisine göre değişmektedir[303]. Burada önemle belirtmek gerekir ki veri koruma görevlisinin bağımsızlığı, mesleki uzmanlık alanına ilişkin "bağımsız görüş bildirebilmesi" üzerine inşa edilmiştir. Bağımsız görüş bildirebilmek, bağımsız iş görmek anlamında olmamakla birlikte veri koruma görevlisinin, veri sorumlusunun veya veri işleyenin iş yerinde istihdam edilmesi, iş yerindeki ekipman ve gereçleri kullanması, çalışma saatlerinin işveren tarafından belirlenmesi gibi hususlar dâhili olarak belirlenecek bir veri koruma görevlisi ile veri sorumlusu veya veri işleyen arasındaki hukuki ilişkiyi bir hizmet sözleşmesi olarak kabul etmemize imkan tanımaktadır. Veri koruma görevlisi kurumunun Tüzük'te yer aldığı gibi verimli şekilde işletilebilmesi için veri sorumlusunun veya veri işleyenin, görevini nasıl yapacağı ve ne yönde karar alacağı konusunda veri koruma görevlisine talimat verememesi gerekmektedir. Ancak bu talimat verememe iş ve hizmetin görümünde alınacak karar ve ulaşılacak sonuca ilişkin olup yine hangi iş ve hizmetin görüleceği konusunda veri koruma görevlisi, işvereni olan veri sorumlusu veya veri işleyenin emir ve talimatları doğrultusunda hareket edecektir. Örnek vermek gerekirse, veri işleme faaliyetlerine ilişkin veri koruma etki analizi yapılıp yapılmaması noktasında veri koruma görevlisine bir değerlendirmede bulunması yönünde talimat verilebilir; ancak veri koruma görevlisinin bu değerlendirmeye ilişkin izleyeceği yöntem ve ulaşacağı sonuç konusunda yönlendirilmemesi gerekir.

Veri koruma görevlisinin harici olarak belirlenmesi ihtimalinde ise veri koruma görevlisi, veri sorumlusunun veya veri işleyenin işletmesi dışında, kendi iş yerinde bağımsız olarak çalışacak olup veri sorumlusunun veya veri işleyenin, veri koruma görevlisine karşı işçi-işveren ilişkisinde olduğu gibi çalışanı koruma, çalışanın sağlığı ve iş güvenliği gibi birtakım özel borçları söz konusu olmayacaktır. Bu durumda veri koruma görevlisinin harici olarak belirlenmesi hâlinde veri sorumlusu veya veri işleyen ile aralarında vekâlet sözleşmesi ilişkisi kurulabileceği söylenebilir.

Veri koruma görevlisinin harici olarak belirlenmesi ihtimalinde görev süresi, veri sorumlusu veya veri işleyen ile arasında akdedilen sözleşmede belirlenen süreyle

[303] Doğa Ekrem DOĞANCI, **"Vekâlet Sözleşmesinin Hukuki Niteliği ve Benzer Hukuki İlişkiler ile Karşılaştırılması",** Sakarya Üniversitesi Hukuk Fakültesi Dergisi, C.2, S.4, Temmuz 2014, s. 109.

sınırlı olacaktır. Dâhili olarak belirleme ihtimalinde ise dâhili veri koruma görevlisi görev alınan kuruluşun çalışanı olduğundan genellikle belirsiz süre için belirlenecek ve sözleşmenin feshi sadece belirli koşullar yerine getirildiğinde gerçekleşecektir. Sözleşmenin belirli süreli olması ve veri koruma görevlisinin belirlenmesinin zamanla sınırlanması ihtimali de elbette mümkündür. Veri koruma görevlisinin belirsiz süreli yahut bir süreye bağlı olarak belirlenmesinde esas alınacak ölçüt, tutarlı bir veri koruma düzeyini ve işleme faaliyetlerinin sürekli izlenmesini sağlamak olmalıdır[304].

3.2.5. Veri Koruma Görevlisinin İletişim Bilgilerinin Yayınlanması

Tüzük'ün m.37/f.7 hükmünde veri sorumlusu ve veri işleyen açısından, veri koruma görevlisinin iletişim bilgilerinin yayınlanması ve denetim makamına bildirilmesi yükümlülüğü açıkça düzenlemiştir. Bu yükümlülük ile veri sahibinin ve denetim makamının veri koruma görevlisi ile kolayca iletişime geçebilmesi amaçlanmıştır[305].

İletişim araçları, veri sahibinin ve denetim makamının veri koruma görevlisine kolayca ulaşabilmesini sağlayacak bilgileri içermelidir. E-posta adresi ve doğrudan veri koruma görevlisine ulaşacak bir telefon numarası bu anlamda verimli iletişim araçları olarak değerlendirilebilir olup yine veri koruma görevlisine hitaben iletişim formları gibi diğer iletişim araçları da kullanılabilir. Veri koruma görevlisinin iletişim bilgilerinin yayınlanması, veri sorumlusu veya veri işleyenin internet sitesinde mevcut olan veri koruma politikaları çerçevesinde de gerçekleştirilebilir.

Article 29 Working Party, veri koruma görevlisinin iletişim bilgilerinin veri sahibi ve denetim makamı hariç veri koruma görevlisinin görev aldığı organizasyonun çalışanlarının da kolayca ulaşabilmesi amacıyla dâhili telefon rehberinde, internet sitesinde veya görev alınan kuruluşun organizasyon şemasında yer almasını iyi bir uygulama olarak nitelendirerek tavsiye etmektedir[306].

[304] VOIGT / von dem BUSSCHE, s. 57.
[305] CLIZA / SPATARU-NEGURA, s. 498.
[306] Art. 29 Working Party, WP243, s. 13.

Tüzük m.37/f.7 hükmü, veri koruma görevlisinin iletişim bilgileri ile beraber isminin yayınlanması yahut bildirilmesi gereğini içermemektedir. Buna göre veri koruma görevlisinin ismi, iletişim bilgilerine dâhil değildir. Veri koruma görevlisinin ismini bildirmek veri sorumlusu veya veri işleyenin takdirine bırakılmıştır. Ancak, veri koruma görevlisinin denetim makamıyla işbirliği görevi ve veri sorumlusu veya veri işleyen ile denetim makamı arasında temas noktası olması özelliği düşünüldüğünde isminin de denetim makamına iletilmesi gerekecektir.

Burada veri sorumlusunun, veri koruma görevlisinin iletişim bilgilerini denetim makamına bildirmesi yükümlülüğüne ilişkin Tüzük m.33'e atıf yapılacak olursa *bir kişisel veri ihlalinin denetim makamına bildirilmesini* düzenleyen maddede veri koruma görevlisi veya daha fazla bilginin elde edilebileceği başka bir temas noktasının isim ve irtibat bilgilerinin denetim makamına iletileceği açıkça düzenlenmiş iken; m.37, bildirim yükümlülüğünü yalnızca iletişim bilgileri ile sınırlı tutmuştur. Ancak bahsedildiği üzere Tüzük her ne kadar veri koruma görevlisinin düzenlendiği madde metinlerinde bu hususu bir yükümlülük olarak görmese de veri koruma görevlisinin denetim makamıyla işbirliği görevi ile temas noktası olması özelliği göz önünde bulundurulduğunda isminin de denetim makamına iletilmesi isabetli bir uygulama olacaktır.

3.3. VERİ KORUMA GÖREVLİSİNİN KONUMU

3.3.1. Uygun Bir Şekilde ve Zamanında Müdahil Olma

Tüzük m.38/f.1 hükmüne göre veri sorumlusu ve veri işleyen, veri koruma görevlisinin kişisel verilerin korunması ile ilgili tüm konulara *"uygun bir şekilde"* ve *"zamanında"* müdahil olmasını sağlamalıdır. Esasında bu düzenleme genel mahiyette olup "uygun bir şekilde" ve "zamanında" ibareleri ile ifade edilmek istenenin, veri koruma görevlisinin veri konularına ilişkin işlemlerin en başından itibaren konuya dâhil edilmesini sağlamak olduğu söylenebilir. Veri koruma görevlisi kişisel verilerin korunmasına ilişkin tüm konulara dâhil edilmelidir ve bunu sağlayacak olan veri sorumlusu ve veri işleyendir.

Veri koruma görevlisinin kişisel verilerin korunması konusuna ilişkin tüm iş ve eylemlerde mümkün olduğunca en erken aşamada yer alması çok önemlidir. Zira veri koruma görevlisinin kişisel verilere ilişkin konularda başlangıçta bilgilendirilmesi ve veri konularına ilişkin işlemlere başlanmadan veri koruma görevlisine danışılması, ilgili organizasyonun Tüzük'e uyumunu kolaylaştıracak ve hesap verilebilirlik ilkesine uygun hareket edildiğini gösterecektir.

Yapılan açıklamalar ışığında veri koruma görevlisinin kişisel verilerin korunması ile ilgili konulara uygun bir şekilde ve zamanında müdahil olmasını sağlamak amacıyla en azından yapılabilecekler şöyle sıralanabilir[307]:

- Veri koruma görevlisi yönetim toplantılarına düzenli olarak katılmaya davet edilebilir.
- Kişisel verilere ve veri koruma konularına ilişkin alınan kararlara ve ilgili organizasyon içerisinde yapılan çalışmalara veri koruma görevlisinin katılımı sağlanmalıdır[308]. Ayrıca yeterli tavsiyede bulunabilmesini sağlamak için ilgili konuya ilişkin tüm bilgiler, veri koruma görevlisine zamanında iletilmelidir.
- Veri koruma görevlisinin tavsiye ve görüşlerine her zaman önem verilmelidir. Veri koruma görevlisinin tavsiyesine uyulmaması hâlinde; tavsiyeye neden uyulmadığı izah edilerek bu durum belgelendirilmelidir.
- Bir veri ihlali yahut veri koruma konularına ilişkin istenmeyen bir durum meydana geldiğinde veri koruma görevlisine derhal danışılmalıdır.

Son olarak, madde metni dikkate alındığında veri koruma görevlisinin görev aldığı organizasyon içerisinde bir nevi "tartışma ortağı" olarak görülebileceği söylenebilir. Bu anlamda çalışanların veri koruma görevlisine zamanında danışmasını sağlayabilmek için veri sorumlusu veya veri işleyen tarafından veri koruma görevlisine ne zaman danışılması gerektiğini belirleyen kılavuz vb. çalışmalar hazırlanabilir.

[307] Art. 29 Working Party, WP243, s. 13.
[308] Örnek olarak; veri sorumlusu tarafından işlenecek yeni bir veri kategorisine ilişkin güvenlik düzeyini belirlerken veri koruma görevlisi ile temasa geçilmedir. Bkz. SHARMA, s. 82.

3.3.2. Veri Sorumlusu ve Veri İşleyen Tarafından Gerekli Kaynakların Sağlanması

Tüzük m.38/f.2 hükmünde veri koruma görevlisinin görevlerini gerçekleştirebilmesi, kişisel veriler ile işleme faaliyetlerine erişilebilmesi ve uzmanlık bilgisini en azından aynı seviyede tutabilmesi için veri koruma görevlisine gerekli kaynakları sağlanması konusunda veri sorumlusu ve veri işleyene yasal bir yükümlülük getirilmiştir.

Bu yükümlülüğün yerine getirilebilmesi için yapılabilecekler şöyle sıralanabilir[309]:

- Veri koruma görevlisi, görev aldığı organizasyondaki yönetim tarafından etkin bir biçimde desteklenmelidir.
- Veri koruma görevlisine, görevlerini yerine getirebilmesi için yeterli zaman tanınmalıdır. Yeterli zaman tanınması, dâhili bir veri koruma görevlisinin yarı zamanlı çalışması hâlinde veya harici bir veri koruma görevlisinin diğer görevlerine ek olarak veri koruma görevini yürüttüğü zamanlarda özellikle önem arz etmektedir. Aksi takdirde görev önceliklerinin çelişmesi ve veri koruma görevlisinin görevlerini ihmal etmesi ihtimali söz konusu olabilir.
- Finansal kaynak, altyapı (tesis, donanım) ve personel açısından yeterli destek sağlanmalıdır.
- Veri koruma görevlisinin görev aldığı organizasyonda varlığının ve işlevinin bilinmesini sağlamak için insan kaynakları ve bilgi işlem biriminde görev alanlar başta olmak üzere tüm çalışanlar bilgilendirilmelidir.
- Veri koruma görevlisinin insan kaynakları, hukuk, bilgi işlem gibi diğer birimlere gerektiğinde erişim sağlayarak gerekli destek ve bilgilere ulaşabilmesi sağlanmalıdır.
- Veri koruma görevlisi, veri koruma alanındaki güncel gelişmelerden haberdar olma fırsatına sahip olmalıdır. Yine veri koruma görevlisinin bilgi ve

[309] Art. 29 Working Party, WP243, s. 14; KORFF / GEORGES, s. 137; IT Governance Privacy Team, s. 38.

uzmanlık seviyesini arttırıcı mahiyette, mesleki gelişimine ilişkin eğitim vb. faaliyetlere katılımı teşvik edilmelidir.

- Görev alınan organizasyonun büyüklüğü ve yapısı dikkate alınarak gerekirse bir veri koruma ekibi kurulmalıdır. Bu durumda ekibin iç yapısı ve her bir üyenin görev ve sorumlulukları açıkça belirlenmeli ve belgelenmelidir.

Yukarıda sayılanların en azından yapılabilecekler olarak kabul edilmesi isabetli olacaktır. Esasında her bir kuruluşun yapısı ve büyüklüğü, işleme faaliyetinin karmaşıklığı ve hassasiyeti vs. gibi etkenler göz önünde bulundurularak veri sorumlusu ve veri işleyen tarafından veri koruma görevlisine sağlanacak kaynaklar da değişebilecektir. Genel olarak, veri işleme faaliyetleri ne kadar karmaşık ve hassas ise veri koruma görevlisine sağlanan kaynağın işlev ve miktarının buna bağlı olarak o kadar fazla olması; bununla beraber işleme faaliyetlerine göre etkili ve yeterli olması gerektiği söylenebilir.

Veri koruma görevlisine finansal kaynak sağlanması konusunda, görev aldığı organizasyonun kural ve prosedürlerine uygun olarak kendi sorumluluğunda doğrudan bir bütçe sağlanması ve ek kaynak talebi olması hâlinde bunun üst'ün kararına değil de görev aldığı kuruluştaki yönetimin kararına bağlı olması; veri koruma görevlisinin görevini bağımsız bir şekilde yerine getirebilmesi için isabetli bir uygulama olduğu söylenebilir[310].

3.3.3. Veri Koruma Görevlisinin Bağımsızlığı

Tüzük m.38/f.3 hükmü ve giriş bölümü 97. paragraf birlikte değerlendirildiğinde veri sorumlusunun ve veri işleyenin, veri koruma görevlisine görevini nasıl yapacağı konusunda talimat verememesi açıkça kararlaştırılmıştır. Burada veri koruma görevlisinin görevlerini yerine getirirken herhangi bir baskı altında kalmasının önüne geçilmeye çalışıldığı söylenebilir. Bu çerçevede veri koruma görevlisi belirleyen veri sorumlusunun veya veri işleyenin, veri koruma görevlisinin bağımsız olarak ve herhangi bir çıkar çatışması olmaksızın hareket edebilmesini sağlamak için iç kurallar

[310] KORFF / GEORGES, s. 136.

oluşturmak gibi gerekli önlemleri alması gerekir[311]. Veri koruma görevlisi ile veri sorumlusu veya veri işleyen arasında akdedilecek sözleşmede, sözleşmeyi feshe yönelik veri koruma görevlisi açısından ne kadar çok koruyucu güvence varsa veri koruma görevlisi o kadar çok bağımsız hareket edebilecektir.

Burada, veri koruma görevlisinin sorumluluklarının bir çalışana yüklenmiş olması hâlinde bile veri korumanın denetlenmesine ilişkin yükümlülüklerini yerine getirmede bağımsız olduğu unutulmamalıdır[312].

Veri koruma görevlisinin bağımsız oluşu kabul edilmekle beraber veri koruma görevlisinin bağımsızlığı Tüzük m.39'da sayılan görevlerini aşacak nitelikte karar alma ve işlem yapma yetkisine sahip olduğu anlamına gelmemektedir[313].

Tüzük m.38/f.3 hükmünün son cümlesinde, veri koruma görevlisinin doğrudan veri sorumlusunun veya veri işleyenin en üst yönetimine rapor vereceği kararlaştırılmıştır. Veri sorumlusunun veya veri işleyenin, veri koruma görevlisinin ve Tüzük'ün tavsiyeleri ile uyumsuz kararlar vermesi durumunda, veri koruma görevlisine ilgili konu hakkında muhalif görüşünü üst yönetime bildirme imkânı verilmelidir. Bu imkân; veri koruma görevlisinin veri sorumlusu veya veri işleyeni bilgilendirme ve tavsiyede bulunma görevinin bir parçası olarak yönetim kurulu gibi üst düzey yönetimin, veri koruma görevlisinin bilgilendirmelerinin ve tavsiyelerinin farkında olmasını sağlar. Veri koruma görevlisinin yıllık olarak üst yönetime faaliyet raporu sunması da doğrudan raporlama faaliyetine örnektir.

Burada son olarak belirtelim ki veri koruma görevlisinin, veri sorumlusu veya veri işleyen ile veri koruma otoritesi arasındaki irtibatlı, bağlantılı kişi olmasından dolayı veri koruma hususuna ilişkin bir konu ile nasıl başa çıkılacağı, ne sonuca ulaşılması gerektiği, bir şikâyetin nasıl araştırılacağı ve veri koruma otoritesine danışılıp danışılmayacağına karar verme konusunda veri koruma görevlisine önemli ölçüde bağımsızca karar alma imkânı verilmelidir.

---

[311] CLIZA / SPATARU-NEGURA, s. 495.
[312] George-Cristian IOAN, **"The effects of Regulation no. 679/2016 on the Romanian commercial environment. The new obligations in the field of personal data",** Juridical Tribune, C.8, Özel Sayı, 2018, s. 121.
[313] Art. 29 Working Party, WP243, s. 15.

3.3.4. Veri Koruma Görevlisinin Görevine Bağlı Olarak İşten Çıkarılamaması veya Cezalandırılamaması

Veri koruma görevlisinin stratejik önemine istinaden Tüzük m.38/f.3'te veri koruma görevlisinin bağımsızlığını sağlamaya yönelik birtakım koruyucu önlemler hüküm altına alınmıştır. Bu bağlamda veri koruma görevlisinin görevlerinin yerine getirilmesi nedeniyle veri sorumlusu ya da veri işleyen tarafından işten çıkarılamayacağı veya cezalandırılamayacağı da Tüzük'te düzenlenmiştir. Tüzük metninde her ne kadar "haksız sebep" ifadesi geçmiyor olsa da bu hükmü elbette "veri koruma görevlisi görevlerinin yerine getirilmesi nedeniyle veri sorumlusu ya da veri işleyen tarafından haksız sebeple işten çıkarılamaz ve cezalandırılamaz" olarak anlamak gerekir. Veri koruma görevlisi bir iş akdi ile görevini ifa ediyorsa bu durumda ulusal iş kanununda tanınan işçiyi koruyucu hükümlerden de yararlanacaktır[314].

Görevine bağlı olarak veri koruma görevlisinin doğrudan veya dolaylı olarak cezalandırılması; promosyon verilmemesi veya diğer çalışanlara göre geç verilmesi, terfi almasının önlenmesi, diğer çalışanlara sağlanan imkanlardan yoksun bırakılması gibi çeşitli biçimlerde olabilecektir. Burada hüküm geniş yorumlanmalı ve Tüzük'ün veri koruma görevlisini yalnızca fiili olarak cezalandırmadan değil cezalandırılma tehdidinden de koruduğu kabul edilmelidir[315].

Veri koruma görevlisinin uyumluluğa ilişkin risk temelli bir yaklaşım benimsemesi gerekliliği de hakkında koruyucu hüküm getirilmesini gerekli kılmıştır. Örneğin, veri koruma görevlisi bir veri işleme faaliyetinin yüksek riskli olduğuna ve etki değerlendirmesi yapılması gerektiğine karar verir ancak yönetim bu değerlendirmeyi kabul etmezse; yönetim, kendi kararı hilafına hareket ediyor gerekçesi ile veri koruma görevlisini görevden alamaz.

Tüzükte veri koruma görevlisi için tanınan koruyucu hüküm, veri koruma görevlisinin yalnızca görevine ilişkin konularda olup görevine ilişkin olmayan nedenlerden ötürü (örneğin; fiziksel veya psikolojik taciz, hırsızlık) ve iş kanunu, ceza

[314] CLIZA / SPATARU-NEGURA, s. 497.
[315] Art. 29 Working Party, WP243, s. 15.

kanunu ve sair yasal mevzuat hükümleri uyarınca veri koruma görevlisinin görevine son verilebilecektir.

Öte yandan Tüzük'ün bir veri koruma görevlisinin hangi şartlarda, nasıl ve ne zaman görevden alınabileceğini veya yerine bir başka veri koruma görevlisinin atanabileceğini hüküm altına almadığını belirtmek gerekir. Burada kanaatimizce veri koruma görevlisinin dâhili veya harici olarak çalışması gibi hususlar ile ulusal mevzuat hükümleri birlikte değerlendirilerek bir çözüme ulaşılması gerekir. Örneğin, veri koruma görevlisinin dâhili olarak çalışması durumunda iş kanununda yer alan işverenin haklı sebeple fesih imkânının veri koruma görevlisi için de kullanılabileceğinin kabulü gerekir. Yahut veri koruma görevlisinin harici olarak görev yapması durumunda, veri sorumlusu veya veri işleyen ile veri koruma görevlisi arasında akdedilecek sözleşmenin veri koruma görevlisi tarafından ihlali hâlinde sözleşmeyi fesih imkânının varlığı kabul edilmelidir.

3.3.5. Veri Sahibinin Veri Koruma Görevlisi İle İrtibata Geçmesi

Tüzük m.38/f.4 hükmüne göre veri sahipleri kişisel verilerinin işlenmesi ve Tüzük kapsamındaki haklarının kullanımı ile ilgili tüm hususlarla alakalı olarak veri koruma görevlisiyle irtibata geçebilir. Gerçekten de Tüzük'te belirlenen veri sahibinin haklarına ilişkin; *erişim hakkı* (m.15), *düzeltme hakkı* (m.16), *silme hakkı/unutulma hakkı* (m.17), *işleme faaliyetini kısıtlama hakkı* (m.18), *veri taşınabilirliği hakkı* (m.20), *itiraz hakkı* (m.21), *profil çıkarma da dahil olmak üzere otomatik münferit karar verme hakkı* (m.22) konularında veya kişisel verilere ilişkin genel anlamda bir sorusu veyahut şikayeti olan veri sahipleri bu hak, soru veyahut şikayetine ilişkin öncelikle ilgili kuruluşun veri koruma görevlisine başvurmalıdır. Veri sahibinin ilgili kuruluşta veri koruma görevlisi hariç bir başka kimseye hitaben talepte bulunması durumunda da bu talep veri koruma görevlisine iletilmelidir.

Burada önem arz eden husus; "Veri Koruma Görevlisinin Konumu" başlığı altında düzenlenen ve veri sahibinin veri koruma görevlisi ile irtibata geçebilmesini düzenleyen Tüzük m.38/f.4 hükmünün, veri koruma görevlisinin iletişim bilgilerinin yayınlanması gerekliliğine ilişkin Tüzük m.37/f.7 hükmü ve veri koruma görevlisinin

kişisel verilerin korunması ile ilgili tüm konulara uygun bir şekilde ve zamanında müdahil olmasını sağlamaya ilişkin Tüzük m.38/f.1 hükmü ile irtibatlı olduğudur. Daha önce çalışmamızın "Veri Koruma Görevlisinin İletişim Bilgilerinin Yayınlanması" başlığı altında ele aldığımız üzere veri koruma görevlisinin irtibat bilgilerinin veri sahipleri tarafından kendisine kolayca ulaşabilmesini sağlayacak nitelikte olması gerekir. Yine veri koruma görevlisinin kişisel verilerin korunması ile ilgili tüm konulara uygun bir şekilde ve zamanında müdahil olması, veri sahiplerinden gelen talepleri cevaplayabilmesini kolaylaştırıcı bir unsurdur.

Veri koruma görevlisi, veri sahibine verilen yanıtı kendisi yazmalı yahut muhakkak gözden geçirmelidir. Veri sahibine verilen yanıt, veri sahibinin yanıttan memnun olmaması durumunda denetim makamına başvurulabileceği bilgisini de içermelidir. Nitekim burada veri sahibinin ilgili kuruluşa talep, soru veya şikâyetini yöneltmiş olması denetim makamına şikâyette bulunma hakkını bertaraf etmemekte; veri sahibinin denetim makamına başvuru hakkı saklı kalmaktadır[316].

3.3.6. Sır Saklama Yükümlülüğü

Tüzük'te veri koruma görevlisinin, birlik veya üye devlet hukuku uyarınca görevini yerine getirmesi ile ilgili olarak sır saklama veya gizlilik ilkelerine bağlı olduğu belirtilmiştir. Bu yükümlülük veri koruma görevlisinin denetim makamı ile işbirliği yapma görevi ile çelişiyor gibi gözükse de esasında, olası bir veri ihlali durumunda Tüzük kapsamında veri koruma görevlisinin bunu denetim makamına bildirme yükümlülüğü olmadığı düşünüldüğünde çelişkili bir durumunun da olmadığı anlaşılacaktır. Nihayetinde olası bir veri ihlalinde sorumluluk veri sorumlusu veya veri işleyene aittir.

[316] Denetim makamının şikayetleri ele alma, soruşturma ve bilgilendirmesine ilişkin Tüzük m.57/f.1 (f) bendi: *" 80. madde uyarınca bir veri sahibi veya bir organ, kuruluş ya da bir birlik tarafından yapılan şikayetleri ele alır ve şikayetin konusunu, uygun olduğu ölçüde, soruşturur ve özellikle daha ayrıntılı soruşturma ya da başka bir denetim makamı ile koordinasyonun gerekmesi durumunda, şikayet sahibini soruşturmanın ilerlemesi ve sonucu konusunda makul bir süre içerisinde bilgilendirir."*.

3.3.7. Çıkar Çatışması Kavramı

Veri sorumlusu veya veri işleyen, çıkar çatışmasına sebep olmadığı sürece veri koruma görevlisine ek görev ve vazife verebilir. Veri koruma görevlisi Tüzük'te yer alan konumu gereği veri işleme ile ilgili görevleri yerine getiremez. Veri koruma görevlisinin, kendisinin Tüzük'e uyumluluğunu izlemek gibi bir durumu söz konusu olmadığından ve hâliyle olamayacağından; veri işleme faaliyetinin amaçlarını ve araçlarını belirlemek gibi konularda görevlendirilemez. Her işletmenin organizasyon yapısı birbirinden farklı olmakla birlikte genel müdür, mali işler müdürü gibi üst düzey yöneticiler, insan kaynakları birimi ve bilgi işlem birimi sorumlusu gibi veri işleme amaç ve araçlarının belirlenmesinde görevli olan rollerden birine veri koruma görevlisini atamak çıkar çatışmasına sebep olabilir.

Veri koruma görevlisinin çıkar çatışmasına sebebiyet verebilecek bir görevde yer almasına ilişkin örnek vermek gerekirse; veri koruma görevlisi, görev aldığı organizasyonun Tüzük m.42'de belirtilen belgelendirme mekanizmalarından olan sertifika alması amacıyla, sertifikasyon kuruluşuna sertifikasyon prosedürünü yürütmek için gerekli olan tüm bilgilerin sağlanması hususunda yardımcı olabilir. Ancak sertifikasyon programının ilgili sertifikasyon kuruluşu tarafından akredite edilmiş bağımsız uzmanları tarafından organizasyonun veri işleme faaliyetlerinin değerlendirilmesine geldiği noktada veri koruma görevlisi artık bu rolde hareket edemeyecektir. Zira bu durum çıkar çatışması oluşturur[317]. Yine bir şirketin pazarlama müdürünün, şirketin hangi müşterilerinin hedefleneceğinin, bu müşteriler ile nasıl iletişim kurulacağının belirlendiği ve kişisel özelliklere ilişkin ayrıntıların yer alacağı bir reklam kampanyası hazırlaması durumunda bu kişi aynı zamanda veri koruma görevlisi olarak belirlenemeyecektir[318]. Çünkü burada pazarlama müdürünün reklam kampanyası kapsamında veri işleme amaçları ve araçları hakkında karar alması ile veri koruma yükümlülükleri arasında çıkar çatışması ortaya çıkacaktır.

Çıkar çatışmasına sebebiyet vermeksizin veri koruma görevlisinin veri güvenliği konusundaki bilgi ve uzmanlığından yararlanmak adına Tüzük kapsamındaki asgari

[317] KORFF / GEORGES, s. 236.
[318] Information Commissioner's Office (ICO), **"Guide to the General Data Protection Regulation (GDPR)"**, s. 197.

görevlerine ek olarak başkaca birtakım görevler vermek elbette faydalı olacaktır. İşletmenin faaliyetine, büyüklüğüne ve yapısına bağlı olarak veri sorumlusu veya veri işleyen, veri koruma görevlisinin işlevine uygun olacak pozisyonları belirleyerek ve çıkar çatışmasını önleyici iç kurallar hazırlayarak buna uygun şekilde veri koruma görevlisine ek görev ve vazife verilebilecektir[319]. Yine veri koruma görevlisinin dâhili veya harici olarak görev yapmasına göre de çıkar çatışmasına sebep olacak hususlara bağlı olarak verilen görev ve vazifeler değişebilecektir.

3.3.8. Veri Koruma Gereksinimlerine Uyulmamasından Kişisel Olarak Sorumluluk

Veri koruma görevlisi veri koruma gereksinimlerinden kişisel olarak sorumlu mudur, sorusuna verilecek yanıt olumsuz olacaktır[320]. Tüzük kapsamında, veri koruma görevlisi veri koruma gereksinimlerine uyulmamasından kişisel olarak sorumlu değildir. Ancak her halükarda veri koruma görevlisinin görevlerini yerine getirmekten sorumlu olduğu düşünüldüğünde; veri özneleri ile veri sorumlusu veya veri işleyenin veri koruma görevlisinin yükümlülüklerinin ihlalinden kaynaklanan zararlar için tazminat talep etme hakkının baki olduğu söylenebilir.

Tüzük m.24'te veri sorumlusunun sorumluluğu düzenlenmiştir. Buna göre;

"1. Veri sorumlusu, işleme faaliyetinin mahiyeti, kapsamı, bağlamı ve amaçlarının yanı sıra gerçek kişilerin hakları ve özgürlükleri açısından çeşitli olasılıklar ve ciddiyetlere sahip riskleri dikkate alarak, işleme faaliyetinin bu Tüzük uyarınca gerçekleştirilmesini sağlamak ve bu şekilde gerçekleştirildiğini gösterebilmek için uygun teknik ve düzenlemeye ilişkin tedbirler uygular. Bu tedbirler gözden geçirilir ve gerektiğinde, güncellenir.

2. İşleme faaliyetleri ile ilgili olarak ölçülü olması halinde, 1. paragrafta atıfta bulunulan tedbirler veri sorumlusu tarafından uygun veri koruma politikalarının uygulanmasını kapsar.".

[319] VOIGT / von dem BUSSCHE, s. 61.
[320] Art. 29 Working Party, WP243, s. 24.

Tüzük kapsamında hüküm altına alındığı üzere, veri koruma kurallarına uyum veri koruma görevlisinin değil, veri sorumlusunun sorumluluğundadır. Veri koruma görevlisinin görevleri danışmanlık ve denetim olmak üzere genel olarak iki kategoride özetlenebilir. Danışmanlık kapsamındaki görevleri, veri sorumlusunu veya veri işleyeni sorumluluk ve yükümlülükleri hakkında bilgilendirmek iken; denetim kapsamındaki görevleri ise veri koruma konularında ve olası bir ihlal hâlinde öneri ve çözüm bulmaktır. Ancak kanunun kendisine tanıdığı yetkilere istinaden uyum konusunda birtakım yükümlülüklerin yerine getirilmesi noktasında veri koruma görevlisinin, içinde bulunduğu organizasyonun yönetim organı ile müteselsil sorumluluğundan bahsetmek mümkündür[321]. Her halükarda veri koruma görevlisi kendi faaliyet alanına ilişkin hatalarından sorumlu olacaktır.

Veri koruma görevlisinin sorumluluğuna ilişkin bir örneğe yer verilecek olursa; bir elektronik ticaret firmasında görev yapan veri koruma görevlisinin, bir gün ofisten iş bilgisayarlarını kilitlemeden çıktığını ve bilinmeyen bir kişi tarafından bu bilgisayar içerisindeki verilere ulaşılıp binlerce veri içerir dosyanın çalındığını ve bu durumun şirketin 1.000.000,00 Euro ceza ödemesine sebep olduğunu varsayalım. Burada veri koruma görevlisinin sorumlu olmadığından bahsetmek elbette mümkün değildir; zira örnekte yer aldığı üzere veri koruma görevlisi iş bilgisayarlarını kilitlemeden ofisten çıkmıştır. Burada verileri çalınan elektronik ticaret şirketi hem veri koruma görevlisine karşı aralarındaki sözleşmeden kaynaklanan görevlerin yerine getirilmemesi ve sözleşmenin ihlali sebebiyle karşı dava açabilecektir hem de veri öznelerinin şirkete karşı açtığı davalarda veri koruma görevlisini suçlamayı bir savunma aracı olarak kullanabilecektir[322].

Bu örnekten anlaşılacağı üzere; Tüzük uyarınca veri koruma görevlisinin veri koruma gereksinimlerinden kişisel olarak sorumlu olmaması mutlak bir sorumsuzluk anlamına gelmemekte olup yine görevlerinin yerine getirilmemesinden dolayı hukukun diğer kaideleri uyarınca veri koruma görevlisinin sorumluluğu gündeme gelecektir. Devletler kendi iç hukuklarında da gerek sözleşmeler hukuku gerek iş

[321] ÇEKİN, s. 144.
[322] SHARMA, s. 84.

hukuku gerekse diğer mevzuat hükümlerine göre veri koruma görevlisinin sorumluluğuna ilişkin kanuni düzenlemelere yer verebilir.

3.4. VERİ KORUMA GÖREVLİSİNİN GÖREVLERİ

Veri koruma görevlisinin görevleri Tüzük m.39'da kararlaştırılmış olup madde metni;

"1. Veri koruma görevlisinin en azından aşağıdaki görevleri bulunur:

(a) veri sorumlusu veya veri işleyen ile işleme faaliyetleri gerçekleştiren çalışanların bu Tüzük ile Birlik veya üye devletlerin diğer veri koruma hükümleri uyarınca yükümlülükleri hususunda bilgilendirilmesi ve onlara tavsiyede bulunulması;

(b) bu Tüzük'e, Birlik veya üye devletlerin diğer veri koruma hükümlerine uyumluluğu ve sorumlulukların verilmesi, işleme faaliyetlerine müdahil personelin bilinçlendirilmesi ve eğitimi ve ilgili denetimler de dâhil olmak üzere veri sorumlusu veya veri işleyenin kişisel verilerin korunmasına ilişkin politikalarına uyumluluğun izlenmesi;

(c) talep üzerine veri koruma etki değerlendirmesine ilişkin tavsiyede bulunulması ve 35. madde uyarınca bu değerlendirmenin performansının izlenmesi;

(d) denetim makamıyla işbirliği yapılması;

(e) 36. maddede atıfta bulunulan ön istişare de dâhil olmak üzere işleme faaliyetine ilişkin konularda denetim makamına yönelik bir temas noktası olarak hareket edilmesi ve, uygun olduğu hallerde, diğer her türlü konu ile ilgili olarak danışılması.

2. Veri koruma görevlisi, görevlerini yerine getirirken, işleme faaliyetinin mahiyeti, kapsamı, bağlamı ve amaçlarını dikkate alarak, işleme faaliyetleri ile ilişkili riski göz önünde bulundurur." şeklinde düzenlenmiştir.

Burada öncelikli olarak söylenmesi gereken husus; veri koruma görevlisi, yer aldığı organizasyonda bir "veri koruma kültürü" oluşturulmasını teşvik etmeli ve görev aldığı organizasyonda veri koruma yasalarının uygulanmasına yardım etmelidir. Bu çerçevede veri koruma görevlisi, veri koruma konusunda farkındalığı artırarak, çalışanları bilinçlendirip eğiterek ve denetimler yaparak bir veri koruma kültürü geliştirilmesini teşvik edebilir.

Madde hükmüne göre veri koruma görevlisinin Tüzük uyarınca asgari görevleri genel olarak; veri sorumlusunu/veri işleyeni/çalışanları veri koruma yükümlülükleri hakkında bilgilendirmek ve onlara tavsiyelerde bulunmak, veri sorumlusunun/veri işleyenin Tüzük'e ve gizlilik politikasına uyumunu izlemek, veri işleme faaliyetinde görevlendirilen personelin sorumluluklarının belirlenmesini, bilinçlendirilmesini ve eğitilmesini sağlamak, talep edildiği takdirde veri koruma etki değerlendirmesine ilişkin tavsiyede bulunmak ve bu değerlendirmenin performansını izlemek, veri koruma etki değerlendirmesinin doğru şekilde yapılıp yapılmadığını ve sonuçlarının veri koruma yasalarına uygun olup olmadığını değerlendirmek, denetim makamı ile işbirliği yapmak ve denetim makamı ile temas noktası olarak hareket etmek olarak sayılabilir.

Burada Tüzük metninde kanun koyucu "en azından" demek suretiyle sayılan görevlerin numerus clauses ilkesine tabi olmadığına işaret etmiştir. Tüzük, veri koruma görevlisinin asgari görevlerini belirlemiş olup m.39'da sayılan görevler haricinde de veri sorumlusu, çıkar çatışmasını gözetmek şartıyla veri koruma görevlisine ek görev ve vazife verebilecektir.

3.4.1. Tüzük'e ve Ulusal Veri Koruma Yasasına Uyum Sürecini İzleme

Veri sorumlusu, ilgili kuruluşun Tüzük'e ve ulusal veri koruma yasalarına uyumuna ilişkin olarak kişisel verilerin korunması hakkında belgelenmiş bir politika geliştirmelidir. Veri koruma görevlisi ise bu politikanın Tüzük'e ve ilgili yasalara uyumu ile ilgili kuruluş ve politika arasındaki uygunluğu izlemelidir. Veri koruma görevlisi uyum sürecini izlemek amacıyla; veri işleme faaliyetlerini tanımlamak için bilgi toplamak ve bu faaliyetlerin kaydını tutmak, veri işleme faaliyetlerinin Tüzük'e

ve veri koruma yasalarına uygunluğunu analiz ve kontrol etmek, veri işleme operasyonlarını gözden geçirmek, veri işleme faaliyetlerinin oluşturduğu riskleri değerlendirmek, veri sorumlusuna veya veri işleyene bilgi vermek, tavsiyelerde bulunmak ve sorunlar hakkında çözüm üretmek gibi faaliyetlerde bulunabilir[323]. Öte yandan veri koruma görevlisi, görev aldığı organizasyon içerisinde veri koruma konularına ilişkin iyileştirme yapılması konusunda pratik önerilerde ve veri koruma yasalarının yorumlanması ve uygulanması hakkında tavsiyelerde bulunmalıdır.

Veri koruma görevlisi, görev aldığı kuruluşun Tüzük'e ve veri koruma yasalarına uyumundan sorumlu değildir; bu sorumluluk veri sorumlusuna aittir[324]. Burada belirtmek gerekir ki veri koruma görevlisinin Tüzük uyum sürecini izlemesi görevi, uyumsuzluğun olduğu yerde sorumluluğun veri koruma görevlisinde olduğu anlamına gelmemektedir. Veri sorumlusunun sorumluluğunun düzenlendiği Tüzük m.24 hükmü, veri işleme faaliyetinin Tüzük'e uygun olarak yapılmasını sağlamak ve bunu gösterebilmek için uygun teknik ve idari tedbirleri uygulamanın veri sorumlusunun sorumluluğunda olduğunu açıkça ortaya koymuştur.

Tüzük m.30'da her veri sorumlusunun ve veri işleyenin kendi sorumluluğu altındaki işleme faaliyetlerine ilişkin bir kayıt tutacağı ve bu kaydın da aşağıdaki bilgilerin tamamını içereceği hüküm altına alınmıştır:

> *"(a) veri sorumlusu ve uygun olduğu hallerde, ortak veri sorumlusu, veri sorumlusu temsilcisi ve veri koruma görevlisinin isim ve irtibat bilgileri;*
>
> *(b) işleme amaçları;*
>
> *(c) veri sahibi kategorileri ve kişisel veri kategorileriyle ilgili bir açıklama;*
>
> *(d) üçüncü ülkeler veya uluslararası kuruluşlardaki alıcılar da dahil olmak üzere, kişisel verilerin açıklandığı veya açıklanacağı alıcı kategorileri;*
>
> *(e) uygun olduğu hallerde, üçüncü bir ülke veya uluslararası bir kuruluşun tanımlanması ve, 49(1) maddesinin ikinci alt paragrafında atıfta bulunulan*

[323] Art. 29 Working Party, WP243, s. 17.
[324] Şehriban İpek AŞIKOĞLU, **Avrupa birliği ve Türk Hukukunda Kişisel Verilerin Korunması ve Büyük Veri**, İstanbul, 2018, s.69.

aktarımlar olması halinde, uygun güvencelere ilişkin belgelendirme de dahil olmak üzere, söz konusu üçüncü ülke veya uluslararası kuruluşa yönelik kişisel veri aktarımları;

(f) mümkün olması halinde, farklı kategorilerdeki verilerin silinmesiyle ilgili öngörülen süre sınırları;

(g) mümkün olması halinde, 32(1) maddesinde atıfta bulunulan teknik ve düzenlemeye ilişkin güvenlik tedbirlerine yönelik genel bir açıklama.".

Bu kaydı tutmak ve elbette gerektiğinde güncellemek, veri sorumlusunun ve veri işleyenin görevi olmakla birlikte aslında bu kayıt hesap verilebilirlik ilkesi ile yakından bağlantılıdır[325]. Hesap verilebilirlik ilkesi ile bağlantılı olarak denetim makamı tarafından etkin denetimi kolaylaştıracak bir kayıt olduğu göz önünde bulundurulduğunda ve uyum sürecini izlemenin de bir gereği olduğu düşünüldüğünde; uygulamada bu kaydı tutmak görevinin veri koruma görevlisine verilebileceği düşünülmektedir[326].

Kayıt tutma yükümlülüğü, hesap verilebilirlik ilkesi çerçevesinde her ne kadar veri sorumlusu ve veri işleyene ait olsa da veri koruma görevlisinin de görev aldığı organizasyonda veri saklama, yönetim ve imha politika ve prosedürlerine sahip olunduğunu bilmesi gerekir. Veri koruma görevlisi tarafından bu politika ve prosedürler düzenli olarak gözden geçirilmeli ve bu politika ve prosedürlerin özeti de dâhil olmak üzere organizasyonun veri işleme faaliyetleri hakkında raporlama yapılmalıdır[327]. Bu kayıt aynı zamanda veri koruma görevlisinin uyumluluğu izleme, veri sorumlusunu ve veri işleyeni bilgilendirme ve tavsiyede bulunma görevlerini yerine getirmesini sağlayan araçlardan biri olarak düşünülebilir[328].

[325] Bkz. s. 51 vd.
[326] CLIZA / SPATARU-NEGURA, s. 496.
[327] LAMBERT, **Data Protection Officer**, s. 168.
[328] KORFF / GEORGES, s. 153.

3.4.2. Veri Koruma Etki Değerlendirmesinde Veri Koruma Görevlisinin Rolü

Veri koruma görevlisinin Tüzük kapsamındaki görevlerinden birisi de veri koruma etki değerlendirmesine ilişkin veri sorumlusuna tavsiyede bulunmaktır. Veri koruma etki değerlendirmesi Tüzük m.35'te tanımlanmış olup buna göre;

"*1. Özellikle yeni teknolojiler kullanıldığında ve işleme faaliyetinin mahiyeti, kapsamı, bağlamı ve amaçları dikkate alındığında bir işleme türünün gerçek kişilerin hakları ve özgürlükleri açısından yüksek bir riske sebebiyet vermesinin muhtemel olduğu hallerde, veri sorumlusu, işleme faaliyetinden önce, öngörülen işleme faaliyetlerinin kişisel verilerin korunmasına olan etkisine ilişkin bir değerlendirme yapar. Tek bir değerlendirmede benzeri yüksek riskler taşıyan bir dizi benzer işleme faaliyeti ele alınabilir.*

2. Veri sorumlusu, bir veri koruma etki değerlendirmesi gerçekleştirirken, belirlenmiş olması halinde, veri koruma görevlisinin tavsiyesine başvurur.".

Tüzük hükmüne göre veri koruma etki değerlendirmesi yapmak veri koruma görevlisinin değil veri sorumlusunun sorumluluğundadır. Ancak bununla birlikte veri koruma görevlisinin veri sorumlusuna tavsiyede bulunmak noktasında çok önemli bir rolü vardır. Veri koruma görevlisinin görevlerinin asgari ölçüde belirlendiği Tüzük m.39'da veri koruma etki değerlendirmesine ilişkin olarak veri koruma görevlisine sırasıyla; talep üzerine veri koruma etki değerlendirmesine ilişkin tavsiyede bulunulması ve m.35 uyarınca bu değerlendirmenin performansının izlenmesi görevi verilmiştir.

Veri koruma etki değerlendirmesine ilişkin Article 29 Working Party tarafından 4 Ekim 2017 tarihli rehber yayınlanmış olup bu rehberde veri koruma etki değerlendirmesini yürütecek olan kimseler belirlenmiştir. *"Veri koruma etki değerlendirmesini kim yürütecektir?"* sorusuna cevap olarak rehber; veri sorumlusunun veri koruma görevlisi ve veri işleyen/işleyenler ile birlikte bu değerlendirmeyi yürüteceğini belirtmiştir[329]. Ancak veri koruma etki değerlendirmesi kim tarafından yürütülürse yürütülsün, ki organizasyon içerisinde yapmak yahut

[329] Art. 29 Working Party, WP248, s. 14.

konuya ilişkin dış kaynaktan hizmet almak da mümkündür, nihayetinde sorumluluk veri sorumlusuna ait olacaktır.

Article 29 Working Party, veri sorumlusunun veri koruma etki değerlendirmesine ilişkin hangi konularda veri koruma görevlisine danışılacağına ilişkin öneride bulunmuş olup buna göre; veri koruma etki değerlendirmesi yapılıp yapılmayacağı, veri koruma etki değerlendirmesi yapılırken nasıl bir yöntem izleneceği, veri koruma etki değerlendirmesinin organizasyon içinde mi yapılacağı yahut dış kaynaktan hizmet almak yolu ile mi yapılacağı, veri öznelerinin hak ve menfaatlerine yönelik riskleri azaltmak için hangi önlemlerin uygulanacağı, veri koruma etki değerlendirmesinin doğru bir şekilde gerçekleştirilip gerçekleştirilmediği ve sonuçlarının Tüzük'e uygun olup olmadığına ilişkin konularda veri koruma görevlisine danışılmalıdır[330].

Veri sorumlusunun bu tavsiyelere uyup uymaması kendi takdirindedir. Bir başka deyişle, veri koruma görevlisinin tavsiyeleri veri sorumlusu açısından bağlayıcı değildir. Ancak veri sorumlusunun, veri koruma görevlisinin tavsiyesine uymaması yahut veri koruma görevlisi ile aynı fikirde olmaması durumunda, tavsiyeye neden uymadığını gerektiğinde denetim makamına sunmak üzere gerekçeleri ile birlikte yazılı olarak belgelemesi gerekmektedir[331].

3.4.3. Denetim Makamı İle İşbirliği Yapmak ve İletişim Noktası Olarak Hareket Etmek

Veri koruma görevlisinin Tüzük'te asgari olarak belirlenen görevleri arasında *denetim makamıyla işbirliği yapılması*[332] ve *36. maddede atıfta bulunulan ön istişare de dâhil olmak üzere işleme faaliyetine ilişkin konularda denetim makamına yönelik bir temas noktası olarak hareket edilmesi ve, uygun olduğu hâllerde, diğer her türlü konu ile ilgili olarak danışılması*[333] sayılmış olup buna göre veri koruma görevlisi

[330] Art. 29 Working Party, WP243, s. 17.
[331] Art. 29 Working Party, WP243, s. 17.
[332] Tüzük m.39/f.1 (d).
[333] Tüzük m.39/f.1 (e).

denetim makamı ile işbirliği yapmak ve iletişim noktası olarak hareket etmekle görevlendirilmiştir.

Tüzük'te "işbirliği" kelimesine yer verilmesi veri koruma görevlisinin denetim makamı ile görev alınan organizasyon arasında nasıl konumlandırılacağı sorusunu akla getirmektedir. Tüzük'te kullanılan "işbirliği" ifadesi ile veri koruma görevlisi her ne kadar denetim makamının bir temsilcisiymiş gibi görünse de veri koruma görevlisi denetim makamının bir temsilcisi değil; görev aldığı organizasyonun bir parçası olarak anlaşılmalıdır[334].

Veri koruma görevlisinin denetim makamı ile işbirliği içerisinde olması, veri koruma görevlisinin denetim makamından kendisine hitaben gelen talepleri bizzat cevaplayabilmeyi ve denetim makamı tarafından veri sorumlusuna gelen taleplerin dikkate alındığından emin olmayı gerektirmektedir[335]. İletişim araçlarının da bu anlamda veri koruma görevlisinin görevlerini yerine getirebilmesine ve denetim makamı ile birebir iletişim kurmasına olanak sağlayacak nitelik ve işlevde olması gerekir.

Veri koruma görevlisi, denetim makamı ile veri sorumlusu ve veri işleyen arasındaki iletişimin sağlanmasında ve birçok durumda aracı olarak görev yaparak adeta bir köprü görevi üstlenecektir. Bu çerçevede denetim makamı, veri sorumlusundan talep ettiği bilgilere veri koruma görevlisi vasıtasıyla erişebilmelidir. Burada hemen belirtelim ki veri koruma görevlisinin aracılık görevinde tek temas noktası olması özelliği vardır ve veri koruma görevlisinin bu tek temas noktası olma özelliği denetim makamının yetki ve görevlerini yerine getirmesinde de kolaylık sağlayıcı bir özellik olarak karşımıza çıkmaktadır. Zira denetim makamının veri sorumlusuna veya veri işleyene ulaşması gerektiği bir durum söz konusu olduğunda veri koruma görevlisinin tek temas noktası olması özelliği ile aslında belirli bir muhatabın varlığı söz konusu olacaktır. Belirli bir muhatabın varlığı da denetim makamının veri sorumlusuna veya veri işleyene ulaşması gerektiğinde kime başvuracağını bilmesi anlamına gelmektedir ki böylece denetim makamı ile veri

[334] KORFF / GEORGES, s. 237; Europen Data Protection Supervisor (EDPS), **"Position Paper On The Role Of Data Protection Officers Of The EU Institutions And Bodies"**, s. 15.
[335] IT Governance Privacy Team, s. 44.

sorumlusu veya veri işleyen arasındaki iletişim elverişli bir şekilde sağlanmış olacaktır.

Öte yandan veri koruma görevlisinin denetim makamı ile işbirliği yapması ve iletişim noktası olarak hareket etmesi, denetim makamının görev ve yetkileri ile de bağlantılıdır. Bu anlamda denetim makamının görevlerinin düzenlendiği Tüzük m.57 hükmüne ve denetim makamının yetkilerinin düzenlendiği Tüzük m.58 hükmüne değinilebilir.

Denetim makamının Tüzük m.57'de yer alan görevlerinin ve m.58'de yer alan soruşturma, düzeltme, yetkilendirme ve danışma yetkilerinin yerine getirilebilmesi için birtakım bilgi ve belgelere erişebilmesi gerekir. Veri koruma görevlisi tam da bu noktada bu bilgi ve belgelere erişimin sağlanmasında denetim makamına yardımcı olacak aktör olarak karşımıza çıkmaktadır. Yine burada belirtmek gerekir ki denetim makamı şikâyet ve sorguların ele alınmasında veri koruma uygulamalarına ilişkin tedbir ve önlem alabilir. Bu tedbirlerin iyi ve etkili bir biçimde uygulanmasının sağlanmasında ise veri koruma görevlisi stratejik ortak olarak görülebilir[336]. Bilgi ve belgelere erişim ile alınan tedbirlerin takibinin sağlanmasında veri koruma görevlisine güvenilebilir/güvenilmelidir.

Veri koruma görevlisinin denetim makamı ile iletişim ve işbirliği içerisinde olmasını sağlamak adına veri sorumlusu veya veri işleyen tarafından gerekli iletişim bilgilerinin denetim makamına bildirilmesi gerekmektedir. Bu noktada veri koruma görevlisinin iletişim bilgilerinin denetim makamına bildirilmesine ilişkin Tüzük'ün 33. ve 37. maddelerine atıfta bulunmak gerekirse, Tüzük m.33'te *bir kişisel veri ihlalinin denetim makamına bildirilmesi* düzenlenmiştir. *Bir kişisel veri ihlali olması durumunda, kişisel veri ihlalinin gerçek kişilerin hakları ve özgürlükleri açısından bir riske sebebiyet vermesinin muhtemel olmaması haricinde, veri sorumlusu, gereksiz gecikmeye mahal vermeden ve uygun olması halinde, ihlalden haberdar olduktan itibaren en geç 72 saat içerisinde, kişisel veri ihlalini 55. madde uyarınca yetkin denetim makamına bildirir*[337]. Bu bildirimde veri koruma görevlisinin isim ve irtibat

[336] Europen Data Protection Supervisor (EDPS), **"Position Paper On The Role Of Data Protection Officers Of The EU Institutions And Bodies"**, s. 16.
[337] Tüzük m.33/f.1.

bilgilerinin de bulunması gerekir[338]. Tüzük metninde *veri koruma görevlisi veya daha fazla bilginin elde edilebileceği başka bir temas noktasının isim ve irtibat bilgilerinin iletilmesi* denmek suretiyle aslında seçimlik bir bildirim yükümlülüğü getirilmiştir. Tüzük m.33'te "veya" sözcüğünün kullanılmasıyla getirilen bu seçimlik bildirim yükümlülüğü ile veri koruma görevlisinin tek temas noktası olması özelliği çelişiyor gibi gözükmektedir. Ancak burada bir çelişkiden ziyade, Tüzük metninden en azından ve her halükarda veri koruma görevlisinin isim ve irtibat bilgilerinin iletilmesi; bunun yanı sıra veri koruma görevlisinden daha fazla bilgi sahibi bir kimse var ise bu kişinin isim ve irtibat bilgilerinin iletilmesi gerektiği sonucuna varılırsa çelişki ortadan kalkmış olacaktır.

Belirtelim ki bir veri ihlali olması durumunda veri koruma görevlisinin veri sorumlusu veya veri işleyen ile denetim makamı arasında arabuluculuk özelliği önemlidir. Veri koruma görevlisi, kişisel veri ihlalinin olması durumunda veri sorumlusu veya veri işleyenin Tüzük m.33'te sayılan şartları yerine getirmesinde ve ihlale ilişkin olayın yanıtlanmasında arabulucu olarak çalışabilir[339].

"Veri Koruma Görevlisinin İletişim Bilgilerinin Yayımlanması" başlığı altında daha önce değindiğimiz üzere Tüzük m.37'de, veri sorumlusu ve veri işleyen için veri koruma görevlisinin iletişim bilgilerinin denetim makamına bildirilmesi yükümlülüğü getirilmiştir. Veri sorumlusu veya veri işleyenin bu yükümlülüğü bir anlamda veri koruma görevlisinin denetim makamı ile işbirliği yapma ve temas noktası olarak hareket etme görevini yerine getirebilmesine hizmet etmektedir. Dolayısıyla Tüzük hem veri koruma görevlisinin görevlerini belirlemiş hem de bu görevlerin yerine getirilebilmesi adına gerekli şartlar ne ise bunların gereğinin yapılmasını sağlamaya çalışmıştır.

Burada son olarak belirtmek gerekir ki veri koruma görevlisinin, Birlik veya üye devlet hukuku uyarınca, görevlerinin yerine getirilmesi ile ilgili olarak sır saklama veya gizlilik ilkelerine bağlı olduğu unutulmamalıdır[340]. Ancak veri koruma

[338] Tüzük m.33/f.3 (b).
[339] IT Governance Privacy Team, s. 4.
[340] Tüzük m.38/f.5: *"Veri koruma görevlisi, Birlik veya üye devlet hukuku uyarınca, görevlerinin yerine getirilmesi ile ilgili olarak sır saklama veya gizlilik ilkelerine bağlıdır."*.

görevlisinin sır saklama ve gizlilik ilkeleri ile bağlı olması veri koruma görevlisinin denetim makamı ile iletişim kurmasını ve denetim makamından tavsiye almasını yasaklamamalıdır[341].

3.4.4. Risk Temelli Yaklaşım

Tüzük m.39/f.2 hükmü *"Veri koruma görevlisi, görevlerini yerine getirirken, işleme faaliyetinin mahiyeti, kapsamı, bağlamı ve amaçlarını dikkate alarak, işleme faaliyetleri ile ilişkili riski göz önünde bulundurur."* şeklinde düzenlenmiş olup veri koruma görevlisinin görevlerini yerine getirirken risk temelli yaklaşıma sahip olması gerektiği belirtilmiştir.

Belirtelim ki Tüzük "risk" kavramını tanımlamamıştır. Her ne kadar bir tanıma doğrudan yer verilmemiş olsa da veri özneleri açısından neyin risk oluşturabileceğine ve hangi verilerin işlenmesinin veri özneleri bakımından zarara yol açabileceğine ilişkin rehberlik edici hükümlere yer verilmiştir[342]. Risk, bir veri işleme faaliyetinin risk veya yüksek risk içerip içermediğinin tespit edildiği objektif bir değerlendirme temelinde değerlendirilmelidir. Tüzük, yeni teknolojiler kullanıldığında ve işleme faaliyetinin mahiyeti, kapsamı, bağlamı ve amaçları dikkate alındığında bir işleme türünün gerçek kişilerin hakları ve özgürlükleri açısından zarara sebebiyet vermesinin muhtemel olduğu hâllerde veri işleme faaliyetinin de yüksek riskli olacağına işaret etmektedir[343].

Giriş bölümünün 75. paragrafında risk ve zarar kavramı bir arada ele alınmış ve gerçek kişilerin hak ve özgürlükleri açısından zarara yol açabilecek veri işleme faaliyetinin riskli olabileceği değerlendirilmiştir. Yine 75. paragrafta hangi veri işleme faaliyetlerinin bireylerin hak ve özgürlükleri açısından zararlı olabileceği sayılmış

---

[341] Art. 29 Working Party, WP243, s. 18.

[342] Centre for Information Policy Leadership, **"Risk, High Risk, Risk Assessments and Data Protection Impact Assessments under the GDPR",** CIPL GDPR Interpretation and Implementation Project, 21 Aralık 2016, s. 13 (Çevrimiçi) https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_gdpr_project_risk_white_paper_21_december_2016.pdf (Erişim:12.07.2020).

[343] Tüzük m.35/f.1.

olup bu sayımın sınırlı sayı ilkesine tabi olmadığı ve rehberlik sağlama amaçlı olduğu unutulmamalıdır.

Tüzük m.35/f.1 hükmü ve *"Risk Değerlendirmesi"* başlıklı giriş bölümünün 76. paragrafına göre veri sahibinin hak ve özgürlüklerine yönelik risk olasılığı ve ciddiyeti; işlemenin niteliği, kapsamı, içeriği ve amacına göre belirlenmelidir.

Veri Koruma Etki Değerlendirmesi'nin düzenlendiği Tüzük m.35 hükmünün 3. fıkrasında hangi durumların kişilerin hak ve özgürlükleri için yüksek risk barındırdığı belirtilmiş olup buna göre; "*gerçek kişilerle ilgili kişisel özellikler hususunda profil çıkarma da dahil olmak üzere otomatik işlemeye dayalı olan ve gerçek kişi ile ilgili hukuki sonuçlar doğuran veya gerçek kişiyi kayda değer şekilde etkileyen kararların dayandığı sistematik ve kapsamlı bir değerlendirme, 9(1) maddesinde atıfta bulunulan özel kategorilerdeki verilerin veya 10. maddede atıfta bulunulan mâhkumiyet kararları ve ceza gerektiren suçlara ilişkin kişisel verilerin büyük çaplı olarak işlenmesi veya kamunun erişebileceği bir alanın büyük çaplı olarak sistematik bir şekilde izlenmesi"* kişilerin hak ve özgürlükleri açsından doğası gereği yüksek risk içeren veri işleme faaliyetlerindendir.

Çalışmamızın *"Veri Koruma Etki Değerlendirmesinde Veri Koruma Görevlisinin Rolü"* başlıklı bölümünde açıklandığı üzere; veri koruma etki değerlendirmesine ilişkin veri sorumlusu veya veri işleyenin talebi üzerine veri koruma görevlisi tavsiyede bulunacaktır. Burada madde hükmünden yola çıkarak herhangi bir şart koşma veya zorunluluk değil, tavsiye mahiyetinde bir değerlendirmenin varlığından söz edebiliriz. Ancak uygulamada bu değerlendirmenin veri koruma görevlisinin görüşüne bağlı olacağını söylemek mümkündür[344]. Veri koruma görevlisi veri koruma etki değerlendirmesi yapılırken nasıl bir yöntem izleneceği, hangi konuların iç veya dış denetime tabi olacağı, veri işlenmesinden sorumlu personel ve yönetime hangi eğitimlerin verilmesi gerektiği, hangi işleme faaliyetlerine daha fazla zaman ve kaynak ayrılması gerektiği konularında veri sorumlusuna yardımcı olmalıdır[345].

[344] KORFF / GEORGES, s. 179.
[345] Art. 29 Working Party, WP243, s. 18.

İşleme faaliyetinin gerçekleştirilmesinde risk temelli yaklaşımın yalnızca veri koruma görevlisi için değil; esasen veri sorumlusu için kararlaştırıldığını belirtmek isteriz[346]. *"Veri Sorumlusunun Sorumluluğu"* başlıklı Tüzük m.24/f.1 hükmü *"Veri sorumlusu, işleme faaliyetinin mahiyeti, kapsamı, bağlamı ve amaçlarının yanı sıra gerçek kişilerin hakları ve özgürlükleri açısından çeşitli olasılıklar ve ciddiyetlere sahip riskleri dikkate alarak, işleme faaliyetinin bu Tüzük uyarınca gerçekleştirilmesini sağlamak ve bu şekilde gerçekleştirildiğini gösterebilmek için uygun teknik ve düzenlemeye ilişkin tedbirler uygular. Bu tedbirler gözden geçirilir ve, gerektiğinde, güncellenir."* şeklinde düzenlenmiş olmakla veri sorumlusunun veri işleme faaliyetinde risk temelli yaklaşıma sahip olması gerektiği belirtilmiştir.

Veri sorumlusunun sorumluluğunun düzenlendiği Tüzük m.24 hükmünde açıkça bireylerin hak ve özgürlüklerine vurgu yapılmış olmasına rağmen veri koruma görevlisinin görevlerinin düzenlendiği m.39 hükmünde bireylerin hak ve özgürlüklerine ilişkin bir ibareye yer verilmemişse de; risk temelli yaklaşım ifadesi ile kastedilenin veri koruma görevlisinin görevlerini yerine getirirken bireylerin temel hak ve özgürlüklerine ilişkin riskleri dikkate alma yükümlülüğü olduğu söylenebilir[347]. Bu bağlamda veri koruma görevlisinin bireylerin temel hak ve özgürlükleri bakımından daha fazla risk barındıran kişisel veri işleme faaliyetlerine öncelik vermesi gerekecektir. Böylelikle değerlendirilecek riskin dar anlamda yalnızca veri ihlalinin olasılığı ve etkisine ilişkin güvenlik riskini değil, veri işleme faaliyetine konu bireylerin hak ve özgürlüklerine ilişkin riski de barındırdığı söylenebilir[348].

İşleme faaliyetinin riskli olması durumunda veri koruma görevlisi, veri işleme faaliyetinde bulunan ilgili sorumlu kişiye alternatif eylemler önermelidir; ilgili kişinin bu alternatif eylemlere uymaması durumunda ise bu hususu yer aldığı organizasyonda var olan üst yönetime bildirmelidir.

Veri koruma görevlisinin işleme faaliyetlerine ilişkin riski göz önünde bulundurması, ilgili risklerin tespit edilmesini gerektirir. Bu tespit, kişisel veri işleme

---

[346] Bkz. s. 53 vd.
[347] Centre for Information Policy Leadership, **"Risk, High Risk, Risk Assessments and Data Protection Impact Assessments under the GDPR",** s. 20.
[348] KORFF / GEORGES, s. 179.

envanterinin hazırlanması, işleme faaliyetinin kaydının tutulması ve bunların gözden geçirilmesi ile bağlantılı olarak yapılacaktır. Ve yine tespit edilen risklerin ve bu risklere yönelik bulunulan önerilerin de kaydının tutulması gerekir.

Hesap verilebilirlik açısından veri koruma görevlisinin önerilerinin dikkate alındığı; risk barındıran veri işleme faaliyetinin ve risklerin gerçekten değerlendirilip bu değerlendirmeye göre önlem alınması ve bu değerlendirmeye istinaden alınan önlemlerin riske uygun olduğunun kanıtlanması yolu ile gösterilebilir[349]. Ancak Tüzük'te veri sorumlusu açısından veri koruma görevlisinin tavsiyesine uymasının veri sorumlusunun sorumluluğunu bertaraf edeceğine ilişkin kesin hüküm olmadığı ve her halükarda sorumluluğun veri sorumlusunda olduğu göz önünde bulundurulduğunda; veri sorumlusunun en azından veri koruma görevlisinin tavsiyelerine uyması, bunun haricinde yine veri işleme faaliyetinin Tüzük'e uygunluğunu sağlayacak varsa başka tedbirleri almaktan çekinmemesi yerinde bir uygulama olacaktır.

Risk değerlendirmesi, aslında bir bakıma veri koruma görevlisinin bütün görevlerini yerine getirirken gözetmesi gereken bir husus olarak düşünülebilir. Konuya ilişkin örnek vermek gerekirse, işlenen verilerin kaydını tutan veri koruma görevlisi, veri sorumlusunun tabi olduğu bir yasal yükümlülüğe uygunluk sağlanması amacı ile yasaya uygun olarak işlenen veri işleme faaliyetinin veri minimizasyonu[350] ilkesine aykırı olarak işlendiğini tespit etmesi üzerine sırf bu hususun risk oluşturduğunu değerlendirip olası riskleri önlemek için gereksiz verilerin toplanmasından vazgeçilmesi ve hâlihazırda tutulan bu tür verilerin silinmesi gibi tedbirler alabilir[351].

[349] KORFF / GEORGES, s. 187.
[350] Tüzük m.5/fl. (c): *"Kişisel veriler: işlendikleri amaçlarla ilgili olarak yeterli, yerinde ve gerekli olanla sınırlıdır"* ('verilerin en az seviyeye indirilmesi').
[351] KORFF / GEORGES, s. 179.

3.5. VERİ KORUMA GÖREVLİSİ BELİRLENMEMESİNİN YAPTIRIMI

Tüzük uyarınca belirlenmesi zorunlu olmasına rağmen veri sorumlusu veya veri işleyen tarafından veri koruma görevlisi belirlenmemesi hâlinde uygulanacak yaptırım da yine Tüzük'te belirtilmiştir. Yaptırıma ilişkin düzenleme *"İdari para cezaları kesilmesine ilişkin genel koşullar"* başlıklı Tüzük m.83/f.4 hükmünde yer almaktadır. Tüzük m.83/f.4 hükmü aynen şu şekildedir: "*Aşağıdaki hükümlere ilişkin ihlaller, 2. paragraf uyarınca, 10.000.000 Euro'ya kadar veya bir teşebbüs olması hâlinde, bir önceki mali yılın yıllık dünya çapındaki cirosunun %2'sine kadar idari para cezalarına (hangi meblağ yüksek ise, o geçerlidir) tabidir:*

a) Veri sorumlusu veya veri işleyenin 8, 11, 25 ila 39 ile 42 ve 43. maddeler uyarınca yükümlülükleri;
b) belgelendirme organının 42 ve 43. maddeler uyarınca yükümlülükleri;
c) izleme organının 41(4) maddesi uyarınca yükümlülükleri.".

(a) bendinde "25 ila 39. maddeler uyarınca" ibaresine yer verilmekle 37 ila 39. maddeler arasında düzenlenen veri koruma görevlisinin anılan fıkra kapsamına girdiği anlaşılmaktadır. Böylelikle Tüzük'ün veri koruma görevlisine ilişkin hükümlerini ihlal eden veri sorumlusu veya veri işleyen 10.000.000 Euro'ya kadar veya bir teşebbüs olması hâlinde, bir önceki mali yılın yıllık dünya çapındaki cirosunun %2'sine kadar idari para cezalarına tabi olacaktır.

Cezanın hangi kıstaslar doğrultusunda verileceğine, her münferit durumda bir idari para cezası kesilip kesilmeyeceğine ve idari para cezası meblağına karar verilirken hangi hususların dikkate alınacağına ilişkin 4. fıkra düzenlemesi 2. fıkra düzenlemesine atıf yapmaktadır. Buna göre; "*İdari para cezaları, her münferit durumun özelliklerine dayalı olarak, 58(2) maddesinin (a) ila (h) ve (j) bentlerinde atıfta bulunulan tedbirlere ek olarak veya bu tedbirler yerine kesilir. Her münferit durumda bir idari para cezası kesilip kesilmeyeceğine karar verilirken ve idari para cezası meblağına karar verilirken, aşağıdaki hususlar dikkate alınır:*

a) ilgili işleme faaliyetinin mahiyeti, kapsamı veya amacı dikkate alındığında ihlalin mahiyeti, ciddiyeti ve süresinin yanı sıra etkilenen veri sahibi sayısı ve veri sahiplerinin yaşadığı zarar düzeyi;

b) ihlalin kasıtlı olması veya ihmalkarlıktan kaynaklanması;

c) veri sahiplerinin yaşadığı zararın azaltılması için veri sorumlusu veya veri işleyen tarafından gerçekleştirilen herhangi bir işlem;

d) 25 ve 32. maddeler uyarınca kendileri tarafından uygulanan teknik ve düzenlemeye ilişkin tedbirler dikkate alındığında, veri sorumlusunun veya veri işleyenin sorumluluk derecesi;

e) veri sorumlusu veya veri işleyenin geçmişte konuyla ilgili ihlalleri;

f) ihlalin düzeltilmesi ve ihlalin olası olumsuz etkilerinin azaltılması amacı ile denetim makamı ile gerçekleştirilen işbirliği derecesi;

g) ihlalden etkilenen kişisel veri kategorileri;

h) veri sorumlusu veya veri işleyenin ihlali bildirip bildirmediği ve bildirdiyse ne ölçüde bildirdiği başta olmak üzere, denetim makamının ihlalden haberdar edilme şekli;

i) 58(2) maddesinde atıfta bulunulan tedbirlerin ilgili veri sorumlusu veya veri işleyene karşı aynı konu ile ilgili olarak daha önceden alınmış olduğu hallerde, bu tedbirlere uyum;

j) 40. madde uyarınca onaylı davranış kurallarına veya 42. madde uyarınca onaylı belgelendirme mekanizmalarına uygun hareket edilmesi;

k) ihlal nedeniyle doğrudan veya dolaylı olarak elde edilen maddi menfaatler veya kaçınılan zararlar gibi durumun özellikleri açısından geçerli diğer ağırlaştırıcı veya hafifletici faktörler.".

AB hukukunda kamu kurum ve kuruluşları belirtilen idari para cezasından muaf tutulmamıştır. Bu nedenle ulusal mevzuatta aksi belirtilmedikçe idari para cezaları kamu kurum ve kuruluşları için de geçerli olacaktır[352]. Bunun yanı sıra Tüzük'ün m.83/f.7 hükmüne göre her üye devlet, söz konusu üye devlette kurulu bulunan kamu kurum ve kuruluşlarına idari para cezası kesilip kesilemeyeceğine ve ne ölçüde kesileceğine ilişkin kurallar belirleyebilir.

[352] CLIZA / SPATARU-NEGURA, s. 499.

3.6. TÜRKİYE'DEKİ VERİ KORUMA HUKUKU DÜZENLEMELERİ AÇISINDAN VERİ KORUMA GÖREVLİSİNİN DEĞERLENDİRİLMESİ

Veri koruma hukukuna ilişkin Türkiye'de yapılan yasal düzenlemelerde veri koruma görevlisine henüz yer verilmemiştir. Ancak burada 6698 sayılı Kanun'un geçici m.1/f.5 hükmüne değinmek gerekir ki bu madde ile veri koruma görevlisi ile örtüşmeyen ancak kısmen benzer bir düzenlemeye kamu kurum ve kuruluşları açısından yer verilmiştir[353]. Bu madde ile 6698 sayılı Kanun'un yayım tarihi olan 7 Nisan 2016 tarihinden itibaren bir yıl içinde, kamu kurum ve kuruluşlarında 6698 sayılı Kanun'un uygulanmasıyla ilgili koordinasyonu sağlamak üzere üst düzey bir yöneticinin belirlenerek Başkanlığa bildirilmesi kararlaştırılmıştır. Bu kişinin AB düzenlemelerinde yer verilen veri koruma görevlisi ile tek benzer yönü, kamu kurum ve kuruluşlarının ulusal veri koruma yasalarına uyumun sağlanmasından sorumlu olması olup elbette Yönerge'nin 18. maddesinin 2. fıkra düzenlemesinde tercihe bırakılan, Tüzük uyarınca kimi durumlarda zorunlu kılınan veri koruma görevlisinin birebir karşılığı kabul edilmesi mümkün değildir.

6698 sayılı Kanun'da kişisel verilerin işlenmesi açısından veri sorumlusu, veri işleyen, veri sorumlusu temsilci olmak üzere üç temel aktör saptanmış olup bunların yanı sıra Veri Sorumluları Sicili Hakkında Yönetmelik'te bir de irtibat kişisine yer verilmiştir. Veri sorumlusu[354] ile veri işleyene[355] çalışmamızın birinci bölümünde detaylı bir şekilde yer verilmiş olup veri sorumlusu temsilcisi ile irtibat kişisi ve bu aktörlerin veri koruma görevlisi karşısındaki konumu açıklanacaktır.

6698 sayılı Kanun'un çeşitli maddelerinde[356] yer alan veri sorumlusu temsilcisi Veri Sorumluları Sicili Hakkında Yönetmelik'in m. 4/f.1 (p) bendinde tanımlanmıştır. Buna göre merkezi Türkiye'de olmayan veri sorumlularının, Yönetmelik m.11/f.3'te

[353] KÜZECİ, s. 321.
[354] Bkz. s. 24 vd.
[355] Bkz. s. 26 vd.
[356] *"Veri Sorumlusunun Aydınlatma Yükümlülüğü"* başlıklı 10. maddede, *"Veri Sorumluları Sicili"* başlıklı 16. maddede ve *"Kurulun Görev ve Yetkileri"* başlıklı 22. maddede veri sorumlusu temsilcisine yer verilmiştir.

belirtilen konularda[357] Türkiye'de yerleşik tüzel kişi ya da Türkiye Cumhuriyeti vatandaşı gerçek kişiyi veri sorumlusu temsilcisi olarak belirlemesi gerekmektedir.

İrtibat kişisi ise Yönetmelik m.4/f.1 (ç) bendinde tanımlanmış olup buna göre; Türkiye'de yerleşik olan tüzel kişi veri sorumluları ile Türkiye'de yerleşik olmayan tüzel kişi veri sorumlusu temsilcileri bir irtibat kişisi belirlemek zorundadır. 28.04.2019 tarihli Resmi Gazete'de yayınlanan Veri Sorumluları Sicili Hakkında Yönetmelikte Değişiklik Yapılmasına Dair Yönetmelik ile Yönetmelik'te değişiklik yapılmadan önce irtibat kişisinin, veri sorumlusunun hem Kurum ile kuracağı iletişimde hem de ilgili kişiler ile kuracağı iletişimde ilgili kişilerden gelecek taleplerin cevaplandırılmasında etkin rol oynayacağı kararlaştırılmış iken; Yönetmelik'in nihai metninde irtibat kişisinin yalnızca Kurum ile veri sorumlusu arasındaki iletişimde etkin rol oynayacağı belirtilmiştir. İrtibat kişisi veri sorumlusunu temsile yetkili olmayıp[358] bu kişi veri sorumlusu ile Kurum arasında iletişim noktası[359] olarak hareket eder.

Veri sorumlusu temsilcisinin veri sorumlusu ile Kurum ve ilgili kişiler arasında irtibat noktası olması; yine irtibat kişisinin de Kurum ile veri sorumlusu arasında iletişimi sağlaması gibi görevleri bu iki aktörün veri koruma görevlisinin denetim makamı ile irtibat noktası olarak hareket etme görevi ile örtüşmektedir. Tüzük'te irtibat kişisine yer verilmemiş, bilhassa denetim makamı ile veri sorumlusu ve veri işleyen arasındaki iletişimin sağlanmasında veri koruma görevlisinin tek temas noktası olması özelliği vurgulanmıştır. Veri koruma görevlisinin ülkemiz veri koruma mevzuatında da yer bulması ile denetim makamı ile iletişim noktası olarak belirlenecek kişinin Tüzük ile uyumlu olacak şekilde yalnızca veri koruma görevlisinin görevlerine dâhil edilmesi kanaatimizce yerinde bir uygulama olacaktır.

---

[357] Veri Sorumluları Sicili Hakkında Yönetmelik (VSSHY) m.11/f.3: *"Veri sorumlusu temsilcisi atama kararı, asgari olarak aşağıda belirtilen hususları kapsayacak şekilde düzenlenir: a) Kurum tarafından yapılan tebligat veya yazışmaları veri sorumlusu adına tebellüğ veya kabul etme, b) Kurum tarafından veri sorumlusuna yöneltilen talepleri veri sorumlusuna iletme, veri sorumlusundan gelecek cevabı Kuruma iletme, c) Kurul tarafından başkaca bir esasın belirlenmemiş olması halinde; ilgili kişilerin Kanunun 13 üncü maddesinin birinci fıkrası uyarınca veri sorumlusuna yönelteceği başvuruları veri sorumlusu adına alma ve veri sorumlusuna iletme, ç) Kurul tarafından başkaca bir esasın belirlenmemiş olması halinde; ilgili kişilere Kanunun 13 üncü maddesinin üçüncü fıkrası uyarınca veri sorumlusunun cevabını iletme, d) Veri sorumlusu adına Sicile ilişkin iş ve işlemleri yapma.".*

[358] VSSHY m.11/f.4.

[359] ÇEKİN, s. 223.

Zira görev ayrımının net bir şekilde belirlenmemesi ilgili kişi yahut Kurum'dan gelecek bir talebin kim tarafından cevaplandırılacağı, ilgili kişilerin yahut Kurum'un kimi muhatap alacağı hususunda karışıklık yaşanmasına sebebiyet verecektir.

Veri koruma görevlisinin görev alanı Tüzük'te oldukça kapsamlı ve geniş çerçevede düzenlenmiş iken veri sorumlusu temsilcisi ve irtibat kişisi, veri sorumlusu ile Kurum arasındaki iletişim kanalı olarak görevlendirilmiştir. Bunun yanı sıra veri koruma görevlisinin bağımsızlığı Tüzük'te ayrıca ve özellikle düzenleme alanı bulmuş iken veri sorumlusu temsilci ve irtibat kişisinin bağımsızlığından bahsedilmemektedir.

95/46/EC sayılı Yönerge referans alınarak hazırlanan 6698 sayılı Kanun'da veri koruma görevlisine ilişkin herhangi bir hükme yer verilmemiştir[360]. Ancak Kanun'da veri koruma görevlisinin ayrıca ve özellikle düzenlenmemiş olması geri dönülemez bir eksilik olmadığı gibi mevcut hükümler yönünden veri koruma görevlisi belirlenmesine engel bir düzenleme de yer almamaktadır. Veri sorumlusunun veri güvenliğine ilişkin yükümlülükleri Kanun'da belirtilmiş olup kişisel verilerin hukuka aykırı olarak işlenmesini önlemek, kişisel verilere hukuka aykırı olarak erişilmesini önlemek, kişisel verilerin muhafazasını sağlamak amacıyla uygun güvenlik düzeyini temin etmeye yönelik gerekli her türlü teknik ve idari tedbirleri almak zorunda olan veri sorumlusunun teknik ve idari tedbirler kapsamında bir veri koruma görevlisi belirlemesi AB mevzuatı ile uyum konusunda önemli bir adım olarak değerlendirilebilir.

23 Temmuz 2019 tarihli 30840 sayılı Resmi Gazete'de[361] yayınlanan ve 2019-2023 dönemini kapsayan On Birinci Kalkınma Planı'nın 479.1'inci satırında, *"6698 sayılı Kişisel Verilerin Korunması Kanunu AB'nin Genel Veri Koruma Tüzüğü dikkate alınarak güncellenecektir."* ifadesine yer verilmiştir. Veri koruma hukukundaki güncel yasal metinler ve AB hukuku ile uyum çerçevesinde Tüzük esas

[360] 6698 sayılı Kanun, 95/46/EC sayılı Yönerge referans alınarak hazırlanmış olmakla beraber Kişisel Verileri Koruma Kurulu vermiş olduğu kararlarda Tüzük hükümlerine de atıf yapmaktadır. Bu durum Kurul'un, Tüzük ile getirilen düzenlemeleri dikkate aldığını göstermektedir. Kurul'un Tüzük hükümlerine atıf yaptığı *"Spor salonu hizmeti sunan veri sorumlularının, üyelerinin giriş-çıkış kontrolünü biyometrik veri işleyerek yapması ile ilgili Kişisel Verileri Koruma Kurulunun 25/03/2019 Tarihli ve 2019/81 Sayılı Karar ve 31/05/2019 Tarihli ve 2019/165 sayılı Karar Özeti"* için bkz. https://www.kvkk.gov.tr/Icerik/5496/2019-81-165 (Erişim:29.11.2020).

[361] https://www.resmigazete.gov.tr/eskiler/2019/07/20190723M1.pdf

alınarak 6698 sayılı Kanun'un güncellenmesi ve geliştirilmesine ilişkin yapılacak değişiklikler veri koruma görevlisini de kapsamalıdır.

Tüzük ile veri koruma hukukunda veri işleme faaliyetlerinin hukuka uygunluğunu sağlamak adına hesap verilebilirlik ilkesine dayalı bütüncül bir yaklaşım benimsenmiş ve veri koruma hukuku düzeni adeta bu ilke üzerine inşa edilmiştir. 6698 sayılı Kanun'da hesap verilebilirlik ilkesine doğrudan ve ayrıca yer verilmemiş olmakla birlikte Kişisel Verileri Koruma Kurumu, Kurul kararlarında bu ilkeye yer vermekle hesap verilebilirlik anlayışına özel bir anlam atfettiğini bir anlamda ifade etmektedir[362]. Temel hesap verilebilirlik araçlarından biri olan veri koruma görevlisi de bu bağlamda veri koruma hukuku düzeni açısından önem kazanacak olup hesap verilebilirlik ilkesinin amacına uygun şekilde işletilebilmesini sağlamak adına Tüzük ile paralel şekilde veri koruma görevlisine ilişkin ayrıntılı düzenlemeler yapma ihtiyacı doğacaktır.

Kanun'da birtakım veri sorumlusu ve veri işleyenler için veri koruma görevlisi belirlenmesine ilişkin yasal düzenleme yapılması elbette mümkündür. Ancak bunun yanı sıra 6698 sayılı Kanun'un 22. maddesinde Kişisel Verileri Koruma Kurulu'nun görev ve yetkileri sayılmıştır. İlgili maddede Kurul'a birtakım düzenleyici işlemler yapma görev ve yetkisi verilmiş olup düzenleyici işlem yapma yetkisi verilen konular; Kurul'un görev alanı ile Kurum'un işleyişine ilişkin, veri güvenliğine ilişkin ve veri sorumlusunun ve temsilcisinin görev, yetki ve sorumluluklarına ilişkin konular olarak belirtilmiştir. Bu kapsamda 6698 sayılı Kanun'un veri güvenliğine ilişkin veri sorumlusunun her türlü teknik ve idari tedbir alma yükümlülüğünün düzenlendiği 12. maddesi ve 22. maddesine dayanılarak hazırlanacak ve Kurum tarafından yürürlüğe konulacak bir ikincil mevzuat ile birtakım veri sorumluları ve veri işleyenler için veri koruma görevlisi belirlenmesine ilişkin düzenleme yapılarak veri koruma görevlisi kavramının Türk hukuk mevzuatında yer alması sağlanabilir.

[362] Kurul'un hesap verilebilirlik ilkesine atıf yaptığı *"Veri sorumlusunun kanuni yükümlülüğünü yerine getirmek için işlediği kişisel verileri meşru menfaat çerçevesinde kullanma talebiyle Kuruma yapmış olduğu başvuru"* konulu 25/03/2019 tarihli ve 2019/78 sayılı Karar Özeti için bkz. https://www.kvkk.gov.tr/Icerik/5434/2019-78 (Erişim:10.02.2021).

Ülkemiz açısından da veri koruma görevlisi, bir takım veri sorumlusu ve veri işleyenler açısından belirlenmesi zorunlu bir aktör olarak düzenlenebilecek olup; hesap verilebilirlik anlayışının gerçekten de işletilebilmesi ve bu aktörün veri koruma kültürü oluşturulması hususunda görev aldığı kuruluşta bir organizasyon geliştirebilmesi için Tüzük'te olduğu gibi bağımsızlığı özellikle sağlanmalı ve buna ilişkin görevine bağlı olarak işten çıkarılamaması veya cezalandırılamaması gibi hakkında koruyucu hükümlere yer verilmelidir. Yine Tüzük'te, veri koruma görevlisinin görevleri arasında veri sorumlusu veya veri işleyen ile ilgili kişiler ve denetim makamı arasında iletişim ve koordinasyonu sağlamak gibi aracılık görevi düzenlenmiş olup Türk hukukunda da veri koruma görevlisine yer verilmesi hâlinde bu aracılık görevine de yer verilmekle muhataplık sorunu çözüme kavuşturulmuş olacaktır. Veri koruma görevlisinin iletişim noktası olarak mevzuatımızda yer bulması ihtimalinde veri sorumluları ve veri işleyenler, veri koruma görevlisinin iletişim bilgilerinin ilgili kişiler ve denetim makamı açısından ulaşılabilir olmasını sağlamalıdır.

Veri koruma görevlisi esasında bir anlamda, görev aldığı organizasyonda her an var olan adeta bir denetçi olarak kabul edilebilir. Bu bağlamda veri koruma görevlisinin uzmanlık konusu olan kişisel verilerin korunmasına ilişkin hemen her konuya dâhil edilmesi sağlanmalı ve görüşüne başvurulmalıdır. Veri koruma görevlisinin veri koruma hukukuna ilişkin konularda bir "tartışma ortağı" olarak kabul edilmesini sağlamak adına çalışanlar da bilinçlendirilmelidir.

Veri koruma görevlisinin uzmanlık ve becerileri ile bu konudaki yetkinliğin tespiti açısından çeşitli ülkelerden de örnekler vermek suretiyle çalışmamızda ayrıntılı açıklamalarda bulunulmuş olup[363] ülkemiz açısından bir değerlendirme yapmak gerekirse; Tüzük ve AB mevzuatı ile uyum çerçevesinde, ülkemizde kişisel verileri koruma hukukuna ilişkin mevzuatta veri koruma görevlisine yer verilmesi hâlinde veri koruma görevlisinin yetkinliğinin tespiti konusu ülkemiz açısından da tartışılır bir mesele hâline gelecektir. Burada Kişisel Verileri Koruma Kurulu'nun belirleyeceği usul ve esaslar çerçevesinde geliştirilecek bir belgelendirme programı ile meselenin

[363] Bkz. s. 78-81.

çözüme kavuşturulacağı kanaatindeyiz. Zira Kişisel Verileri Koruma Kurumu Teşkilat Yönetmeliği'nde[364], Kurul'un görev ve yetkileri sayılmış olup Yönetmeliğin ilgili 7. maddesinin 1. fıkrasının (ı) bendinde *"Kişisel verilerin korunması, işlenmesi ve güvenliği ile ilgili sektörel uygulama esaslarını belirlemek ve akreditasyon, sertifikasyon, eğitim ile rehberlik konularında usul ve esasları belirlemek"* görev ve yetkisi Kurul'a verilmiştir. Buna göre veri koruma görevlisinin yetkinlik ölçütü olarak kabul edilebilecek sertifikasyon programına ilişkin Kurul'un belirleyeceği usul ve esaslar ile kriterler çerçevesinde bir belgelendirme mekanizması hazırlanabilir.

[364] Yönetmelik metni için bkz. https://www.mevzuat.gov.tr/MevzuatMetin/3.5.201811296.pdf

SONUÇ

Kişi, ardında bıraktığı verilerden ibaret değildir. Bir başka deyişle kişi, ardında bıraktığı verilerden çok daha fazlasıdır. Kişisel veriler, mahremiyete ilişkin insan özel yaşamının bir parçasını oluşturmakta ve bu anlayış kişisel verilerin korunmasının temel insan hakkı olarak kabul edilmesi sonucunu beraberinde getirmektedir. Kişisel verilerin temel insan hakları düzeyinde kabul edilmesinin yanı sıra bilgi ve iletişim teknolojisindeki gelişmelerin bir sonucu olarak bilgi ekonomisinin temel kaynağını oluşturması da yadsınamaz bir gerçektir. Kişisel verilerin hem insan özel yaşamının bir parçasını oluşturması hem sanayi toplumundan bilgi toplumuna geçişte toplanma, saklanma, işlenme ve aktarılma gibi bireysel hak ve özgürlükler açısından endişe yaratacak faaliyetlere konu olması; kişisel verilerin korunmasının hukuki düzenleme alanı olarak ortaya çıkması sonucunu beraberinde getirmiştir.

Devletlerin, bireylerin kişisel verilerine ve mahremiyetine saygı duyduğunun bir göstergesi de veri koruma rejiminin hayata geçirilmesidir. Bu çerçevede gerek devletlerin ulusal hukuk düzenlemelerinde gerek uluslararası hukuk belgelerinde kişisel verilerin korunması ayrıca ve özellikle düzenleme alanı bulmuştur. Avrupa Birliği'nde üye bütün devletler açısından uyumlaştırma ve yeknesaklaştırma çalışmalarının bir sonucu olarak Avrupa Birliği Genel Veri Koruma Tüzüğü, Mayıs 2018 yılında 95/46 sayılı Yönerge'yi ilga ederek yürürlüğe girmiştir. Ülkemizde ise kişisel verilerin korunmasına ilişkin 6698 sayılı Kanun'un kurgulanmasında Yönerge dikkate alınmış olup hiç şüphesiz Tüzük ile hukuk düzeninde yer bulup Kanun'da yer almayan birtakım veri koruma kurallarına istinaden Kanun'un modernize edilmesi ve güncellenmesi gerekmektedir.

Avrupa Birliği Genel Veri Koruma Tüzüğü ile veri koruma hukukuna ilişkin birtakım yeni düzenlemelere yer verilmiş; veri koruma hukukuna ilişkin ilkeler bilgi ve iletişim teknolojisindeki gelişmelerle uyumlu olacak esneklikte olacak şekilde güncellenmiştir. Tüzük ile artırılmış veri koruması eğilimine paralel olarak sorumluluk rejiminde de birtakım yenilikler benimsenmiş ve 6698 sayılı Kanun'dan ve Yönerge'den farklı olarak veri sorumlusunun -öncelikle- devlet eliyle kontrolü yerine; en baştan itibaren veri koruma ilkelerine uygun bir şekilde veri işleme faaliyetinde

bulunması, bu konuda gerekli her türlü teknik ve idari tedbiri alması ve gerektiğinde bunu belgeleyebilmesi kuralı kabul edilmiştir. Bu kural veri koruma ilkelerinden olan hesap verilebilirlik ilkesinin bir sonucu olarak karşımıza çıkmaktadır.

Tüzük ile sorumluluk bakımından hesap verilebilirliğe dayalı daha kapsamlı düzenlemelere yer verilmiştir. Çalışmamızda ayrıntılı bir şekilde açıklandığı üzere Tüzük'te birtakım veri sorumluları ve veri işleyenler açısından uyumun sağlanması ve hesap verilebilirlik ilkesinin bir gereği olarak alınması gereken teknik ve idari tedbirler ile uyumluluğu artırmaya ilişkin kurallar kapsamında zorunlu olarak veri koruma görevlisi belirlenmesi kuralı kabul edilmiştir. Veri koruma görevlisi, veri koruma hukukunun temel aktörlerinden biri olarak düzenleme alanı bulmuş olup ilk olarak veri koruma kurallarına uyum; ikinci olarak bu kurallara uyumda sürekliliğin sağlanması adına birtakım görevler ile donatılmıştır. Tüzük, yalnızca bu görevleri belirlemekle yetinmemiş ayrıca bu görevlerin yerine getirilmesini sağlamak için ayrıntılı düzenlemelere yer vermiştir. Veri koruma görevlisinin bağımsızlığı ve görevine bağlı olarak işten çıkarılamaması ve cezalandırılamaması gibi birtakım koruyucu düzenlemeler ile getirilen sorumluluk rejiminin amacına uygun hareket etmesi güvence altına alınmıştır.

Veri koruma görevlisinin mesleki kimliği, görevlerini yerine getirmesinde yetkinlik ölçütleri gibi birtakım hususlar kesinlik kazanmamış olmakla birlikte çalışmamızda bu hususlar çeşitli ülkelerde yer alan hukuki düzenlemeler çerçevesinde açıklanmaya çalışılmış ve ülkemiz açısından değerlendirmelerde bulunulmuştur.

Tüzük kapsamında ayrıntılı bir şekilde düzenlenen veri koruma görevlisi münferit olarak henüz ülkemiz veri koruma mevzuatında yer almamaktadır. Ancak bu durum geri dönülemez bir eksiklik olmadığı gibi 6698 sayılı Kanun'da veri koruma görevlisi belirlenmesine engel bir düzenleme de bulunmamaktadır. AB yasaları ile uyum ve güncel veri koruma kurallarının ülkemiz açısından da kabul edilmesi açısından 6698 sayılı Kanun'un modernize edilmesi ve güncellenmesi ihtiyacının bir sonucu olarak ülkemiz veri koruma mevzuatında veri koruma görevlisi kurumuna yer verilmesi gündeme gelecektir. Çalışmamızda Tüzük hükümleri uyarınca veri koruma görevlisi kurumu ayrıntılı bir şekilde açıklanmakla birlikte; bu kurumu hayata geçiren

ülkelerden örnekler verilerek ülkemiz açısından da gelecekte veri koruma görevlisi kurumuna ilişkin meydana gelecek sorulara/sorunlara ilişkin değerlendirmelerde bulunulmuştur.

Ülkemiz veri koruma mevzuatının AB düzenlemeleri ile uyumlaştırılması yasal düzenleme yapılmasını gerektirmekle birlikte Kişisel Verileri Koruma Kurulu'nun yapacağı ikincil düzenlemeler ve uygulamadaki pratikler yoluyla ve ayrıca Kurul kararlarında Tüzük'e yapılacak atıflar ile uyumun sağlanması söz konusu olacaktır. Bu kapsamda AB düzenlemelerine ve güncel veri koruma kurallarına uyumun bir gereği olarak veri koruma görevlisi kurumuna ikincil düzenlemelerde yer yerilmek suretiyle veri koruma görevlisi kavramının ülkemiz veri koruma mevzuatında yer alması sağlanabilir. İkincil düzenlemelere bırakılan hususlar ile Kurul kararlarında Tüzük ilke ve hükümlerinin dikkate alınması AB düzenlemelerine uyumun sağlanmasında verimli bir yöntem olarak tercih edilebilir.

KAYNAKÇA

KİTAP VE MAKALELER

AKGÜL, Aydın, **Danıştay ve Avrupa İnsan Hakları Mahkemesi Kararları Işığında Kişisel Verilerin Korunması**, İstanbul, 2014.

AKİPEK, Jale / AKINTÜRK, Turgut / ATEŞ, Derya, **Türk Medeni Hukuku Başlangıç Hükümleri Kişiler Hukuku,** 15.Baskı, İstanbul, 2019.

AKKURT, Sinan Sami, **"Türk Özel Hukukunda İş Sözleşmesi ile Eser Sözleşmesinden Kaynaklanan Başlıca Yükümlülükler ve Anılan Sözleşmelerin Ayırt Edilmesi"**, Dokuz Eylül Üniversitesi Hukuk Fakültesi Dergisi, C.10, S.2, 2010, s. 13-64 (Kısaltılmışı *İş Sözleşmesi ile Eser Sözleşmesi*).

AKKURT, Sinan Sami **"Kişisel Veri Kavramının Hukuki Niteliğine İlişkin Yaklaşımlara Mukayeseli Bir Bakış"**, Kişisel Verileri Koruma Dergisi, C.2, S.1, 2020, s. 20-32 (Kısaltılmışı *Kişisel Veri*).

AKSOY, Hüseyin Can, **Medeni Hukuk ve Özellikle Kişilik Hakkı Yönünden Kişisel Verilerin Korunması,** Ankara, 2010.

ARAL, Fahrettin / AYRANCI, Hasan, **Borçlar Hukuku Özel Borç İlişkileri,** 9.Baskı, Ankara, 2012.

AŞIKOĞLU, Şehriban İpek, **Avrupa birliği ve Türk Hukukunda Kişisel Verilerin Korunması ve Büyük Veri**, İstanbul, 2018.

ATAK, Songül, "**Avrupa Konseyi'nin Kişisel Veriler Açısından Sağladığı Temel Güvenceler"**, TBB Dergisi, S.87, 2010, s. 90-120.

ATASOY, Kemal, **"Kişilik Hakkı Kapsamında Sosyal Medyada Kişisel Verilerin Korunması ve Veri Sahibinin Rızası",** Marmara Üniversitesi Hukuk Fakültesi Hukuk Araştırmaları Dergisi, C.22, S.3, 2016, s. 269-301.

AYAN, Mehmet / AYAN, Nurşen, **Kişiler Hukuku**, 8.Baskı, Ankara, 2016.

AYDOĞDU, Murat / KAHVECİ, Nalan, **Türk Borçlar Hukuku Özel Borç İlişkileri Sözleşmeler Hukuku,** 4.Baskı, Ankara, 2019.

AYÖZGER, Çiğdem, **Kişisel Verilerin Korunması Hukuku Elektronik Haberleşme Sektörüne İlişkin Özel Düzenlemeler Dâhil**, 2.Baskı, İstanbul, 2019.

BAŞALP, Nilgün, **Kişisel Verilerin Korunması ve Saklanması,** Ankara, 2004 (Kısaltılmışı *Kişisel Verilerin Korunması*).

BAŞALP, Nilgün, "**Avrupa Birliği Veri Koruması Genel Regülasyonu'nun Temel Yenilikleri",** MÜHF-HAD, C.21, S.1, 2015, s. 77-106 (Kısaltılmışı *Regülasyonun Temel Yenilikleri*).

BAYKAL, Sanem / GÖÇMEN**,** İlke, **"Avrupa Birliği Hukukunun Kaynakları Bakımından Normlar Hiyerarşisi",** Prof. Dr. Erdal Onar'a Armağan, Ankara, 2013, s. 317-325.

BAYRAM, Mehmet Hanifi, **Avrupa Birliği Hukuku Dersleri**, 4.Baskı, Ankara, 2019.

CHIRICA, Simona, "**The Main Novelties and Implications of the New General Data Protection Regulation",** C.6, S.1, 2017, s. 159-176.

CLIZA, Marta-Claudia / SPATARU-NEGURA, Laura-Cristiana, **"The General Data Protection Regulation: What does the public authorities and bodies need to know and to do? The rise of the data protection officer",** Juridical Tribune, C.8, S.2, 2018, s. 489-501.

CVIK, Eva Daniela / PELIKÁNOVÁ, Radka MacGregor / MALÝ Michal, **"Selected Issues from the Dark Side of the General Data Protection Regulation",** Review of Economic Perspectives, C.18, S.4, 2018, s. 387-407.

ÇEKİN, Mesut Serdar, "**6698 Sayılı Kişisel Verilerin Korunması Hakkında Kanun'un Big Data (Büyük Veri) ve İrade Serbestisi Açısından Değerlendirilmesi",** İÜHFM, C. LXXIV, S.2, 2016, s. 629-644 (Kısaltılmışı *Big Data ve İrade Serbestisi Açısından Değerlendirme)*.

ÇEKİN, Mesut Serdar, **Avrupa Birliği Hukukuyla Mukayeseli Olarak 6698 Sayılı Kanun Çerçevesinde Kişisel Verilerin Korunması Hukuku,** 3.Baskı, İstanbul, 2020 (Kısaltılmışı *Kişisel Verilerin Korunması*).

DEMİRBAŞ, Harun, **6563 Sayılı Elektronik Ticaretin Düzenlenmesi Hakkında Kanun Kapsamında Hizmet Sağlayıcıları ve Aracı Hizmet Sağlayıcılarının Yükümlülükleri**, Ankara, 2015.

DEVELİOĞLU, Hüseyin Murat, **6698 sayılı Kişisel Verilerin Korunması Kanunu ile Karşılaştırmalı Olarak Avrupa Birliği Genel Veri Koruma Tüzüğü Uyarınca Kişisel Verilerin Korunması Hukuku**, İstanbul, 2017.

DOĞANCI, Doğa Ekrem, **"Vekâlet Sözleşmesinin Hukuki Niteliği ve Benzer Hukuki İlişkiler ile Karşılaştırılması",** Sakarya Üniversitesi Hukuk Fakültesi Dergisi, C.2, S.4, Temmuz 2014, s. 95-131.

DURAL, Mustafa / ÖĞÜZ, Tufan, **Türk Özel Hukuku Cilt II Kişiler Hukuku**, 18.Baskı, İstanbul, 2017.

DÜLGER, Murat Volkan, **"Kişisel Verilerin Korunması Kanunu ve Türk Ceza Kanunu Bağlamında Kişisel Verilerin Ceza Normlarıyla Korunması"**, İMÜHFD, C.3, S.2, 2016, s. 101-167 (Kısaltılmışı *TCK Bağlamında Koruma*).

DÜLGER, Murat Volkan, "**İnsan Hakları ve Temel Hak ve Özgürlükler Bağlamında Kişisel Verilerin Korunması",** İMÜHFD, C.5, S.1, 2018, s. 71-143 (Kısaltılmışı *İnsan Hakları Bağlamında Koruma*).

DÜLGER, Murat Volkan, "**Avrupa Birliği Genel Veri Koruma Tüzüğü Bağlamında Kişisel Verilerin Korunması",** Yaşar Hukuk Dergisi, C.1, S.2, 2019, s. 71-174 (Kısaltılmışı *Tüzük Bağlamında Koruma*).

EREN, Fikret, **Borçlar Hukuku Özel Hükümler,** 4.Baskı, Ankara, 2017.

GEZDER, Ümit, **"Ölüm Sonrası Hatırayı Koruma Doktrini ve Ölüm Sonrası Kişiliğin Korunması Teorisi"**, İÜHFM, C.65, S.1, 2007, s. 207-222.

GILBERT, Francoise, **"European Data Protection 2.0: New Compliance Requirements in Sight - What the Proposed EU Data Protection Regulation Means for U.S. Companies"**, Santa Clara High Tech. L.J., C.28, S.4, 2012, s. 815-863.

GUTWIRTH, Serge / LEENES, Ronald / HERT, Paul / POULLET, Yves, **European Data Protection; In Good Health?,** Springer, 2012.

GÜMÜŞ, Mustafa Alper, **6098 sayılı Türk Borçlar Kanunu'na Göre Borçlar Hukuku Özel Hükümler,** C.I, 3.Baskı, İstanbul, 2013.

GÜMÜŞ, Ali Tarık, **"Türk Anayasasında Kişinin Maddi ve Manevi Varlığını Koruma Ve Geliştirme Hakkı"**, SÜHFD, C. 13, S. 2, 2005, s. 133-172.

Handbook on European Data Protection Law, Publications Office of the European Union, Lüksemburg, Nisan 2018.

HATEMİ, Hüseyin, **Kişiler Hukuku,** 8.Baskı, İstanbul, 2020.

HELVACI, Serap, **Gerçek Kişiler**, 5.Bası, İstanbul, 2013.

HENKOĞLU, Türkay, **Bilgi Güvenliği ve Kişisel Verilerin Korunması**, Ankara, 2015.

HORNUNG, Gerrit, **A General Data Protection Regulation for Europe? Light and Shade in the Commission's Draft of 25 January 2012,** Scripted, C.9, S.1, 2012, s. 64-81.

IOAN, George-Cristian, "**The effects of Regulation no. 679/2016 on the Romanian commercial environment. The new obligations in the field of personal data"**, Juridical Tribune, C.8, Özel Sayı, 2018, s. 110-127.

IT Governance Privacy Team, **EU General Data Protection Regulation: An Implementation and Compliance Guide**, It Governance Publishing, 2.Baskı, Birleşik Krallık, 2017.

KANG, Jerry, **"Information Privacy in Cyberspace Transactions",** Stanford Law Review, C.50, 1998, s. 1193-1294.

KARATAŞ DURMUŞ, Neslihan, **"Ticari Sırların Ve Kişisel Verilerin Korunması Kapsamında Vergi Mahremiyeti",** Türkiye Adalet Akademisi Dergisi, S.31, 2017, s. 371-410.

KARLIDAĞ, Serpil, **"Ekonomi Politik Açıdan Kişisel Verilerin Korunması"**, Amme İdaresi Dergisi, C.46, S.1, 2013, s. 127-152.

KAYA, Cemil, **"Avrupa Birliği Veri Koruma Direktifi Ekseninde Hassas (Kişisel) Veriler ve İşlenmesi"**, İÜHFM, C.LXIX, S.1-2, 2011, s. 317-334.

KAYA, Mine, **Elektronik Ortamda Kişilik Hakkının Korunması**, Ankara, 2015.

KESER, Leyla, **Çevrimiçi Davranışsal Reklamcılık Uygulamaları Özelinde Kişisel Verilerin Korunması,** İstanbul, 2014.

KILINÇ, Doğan, "**Anayasal Bir Hak Olarak Kişisel Verilerin Korunması"**, AÜHFD, C. 61, S.3, 2012, s. 1089-1169.

KORFF, Douwe, **Study on the Protection of the Rights and the Interests of Legal Persons of Personal Data Relating to Such Persons,** Commission of the European Communities Report, Ekim 2008 (Kısaltılmışı *Study on the Protection*).

KORFF, Douwe, **New Challenges to Data Protection Study - Working Paper No. 2: Data Protection Laws in the EU: The Difficulties in Meeting the Challenges Posed by Global Social and Technical Developments,** European Commission DG Justice, Freedom and Security Report, Haziran 2010 (Kısaltılmışı *New Challenges to Data Protection)*.

KORFF, Douwe / GEORGES, Marie, **The DPO Handbook Guidance for data protection officers in the public and quasi-public sectors on how to ensure compliance with the European Union General Data Protection Regulation**, Temmuz 2019 (Kısaltılmışı *The DPO Handbook*).

KORKMAZ, İbrahim, "**Kişisel Verilerin Korunması Kanunu Hakkında Bir Değerlendirme",** TBB Dergisi, C.29, S. 124, 2016, s. 81-152 (Kısaltılmışı *Değerlendirme*).

KORKMAZ, İbrahim, **Kişisel Verilerin Ceza Hukuku Kapsamında Korunması**, 2.Baskı. Ankara, 2019.

KÜZECİ, Elif, **Kişisel Verilerin Korunması**, 3. Baskı, Ankara, 2019.

KÜZECİ, Elif / KILIÇ, Şebnem, **"6698 Sayılı Kişisel Verilerin Korunması Kanunu'nun İş Sözleşmesi Çerçevesinde Değerlendirilmesi: Veri Sorumlusu, Veri İşleyen Ve Diğer Aktörler",** Legal İş Hukuku ve Sosyal Güvenlik Hukuku Dergisi, C.16, S.63, 2019 (Kısaltılmışı *İş Sözleşmesi Çerçevesinde Değerlendirme)*.

L'HOIRY, Xavier Duncan / NORRIS, Clive, **"The Honest Data Protection Officer's Guide to Enable Citizens to exercise Their Subject Access Rights: lessons from a ten country European study",** International Data Privacy Law, C.5, S.3, 2015, s. 190-204.

LAMBERT, Paul, **Understanding the New European Data Protection Rules**, CRC Press Taylor&Francis Group, 2017 (Kısaltılmışı *Data Protection Rules*).

LAMBERT, Paul, **The Data Protection Officer Profession, Rules and Role**, CRC Press Taylor&Francis Group, 2017 (Kısaltılmışı *Data Protection Officer*).

MALI, Prashant, **"GDPR Articles With Commentary & EU Case Laws",** Cyber Infomedia, 2019.

MEMİŞ, Tekin, "**Veri Sorumlusu ve Veri İşleyen Arasındaki İlişkiler ve Sorumluluk Düzeni",** Beykent Üniversitesi Hukuk Fakültesi Dergisi, C.3, S.6, 2017, s. 9-23.

OĞUZMAN, Kemal / SELİÇİ, Özer / OKTAY ÖZDEMİR, Saibe, **Kişiler Hukuku Gerçek ve Tüzel Kişiler,** İstanbul, 2016.

ÖZDEMİR, Hayrunnisa, **Elektronik Haberleşme Alanında Kişisel Verilerin Özel Hukuk Hükümlerine Göre Korunması,** Ankara, 2009.

ÖZDEMİR, Hayrunnisa, "**Haberleşmenin Gizliliği ve Kişisel Veriler"**, EÜHFD, C.13, S.1-2, 2009, s. 285-303.

ÖZMAN, Mehmet Aydoğan, "**Avrupa İnsan Hakları Divanı'nın 1978 Yılında Verdiği Kararlar",** AÜHFD, C.35, S.1, 1978, s. 195-218.

QUELLE, Claudia, **The 'risk revolution' in EU data protection law: We can't have our cake and eat it, too,** Tilburg Law School Legal Studies Research Paper Series 1, No:17/2017.

RECIO, Miguel, **"Practitioner's Corner Data Protection Officer: The Key Figure to Ensure Data Protection and Accountability",** European Data Protection Law Review, C.3, S.1, 2017, s. 114-118.

SHARMA, Sanjay, **Data Privacy and GDPR Handbook**, John Wiley & Sons, 2019.

SHAW, Thomas J., **DPO Handbook Data Protection Officers Under The GDPR**, International Association of Privacy Professionals (IAPP), 2.Baskı, 2018.

STALLA-BOURDILLON, Sophie / KNIGHT, Alison**, Anonymous Data V. Personal Data-A False Debate: An EU Perspective on Anonymization, Pseudonymization and Personal Data**, Wisconsin International Law Journal, 34 (2), 2017, s. 284-322.

TANSUĞ, Çağla, **"Fransız Hukukunda Veri Koruma Otoritesi: CNIL",** Yeditepe Üniversitesi Hukuk Fakültesi Dergisi, C.14, S.2, 2017, s. 335-353.

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

TEZCAN, Durmuş, **"Bilgisayar Karşısında Özel Hayatın Korunması",** Anayasa Yargısı Dergisi, C.8, 1991, s. 385-392.

TURAN, Metin, **Karşılaştırmalı Hukukta Kişisel Verilerin Korunması,** 2.Baskı, Ankara, 2019.

VOIGT, Paul / Axel von dem BUSSCHE, **The EU General Data Protection Regulation (GDPR) A Practical Guide**, Springer, 2017.

YAVUZ, Cevdet / ACAR, Faruk / ÖZEN, Burak, **Borçlar Hukuku Dersleri Özel Hükümler,** 8.Baskı, İstanbul, 2010.

YÜCEDAĞ, Nafiye, "**Medeni Hukuk Açısından Kişisel Verilerin Korunması Kanununun Uygulama Alanı ve Genel Hukuka Uygunluk Sebepleri",** İÜHFM, C.75, S.2, 2017, s. 765-789.

YÜKSEL CİVELEK, Dilek, **Kişisel Verilerin Korunması ve Bir Kurumsal Yapılanma Önerisi,** Ankara, 2011.

İNTERNET KAYNAKLARI

Article 29 Working Party, **"Opinion 1/2010 on the Concepts of "Controller" and "Processor"",** WP 169, 16 Şubat 2010.

Article 29 Working Party **"Opinion 3/2010 on the Principle of Accountability",** WP173, 13 Temmuz 2010.

Article 29 Working Party, **"Opinion 03/2013 on Purpose Limitation",** WP203, 2 Nisan 2013.

Article 29 Working Party, **"Statement on the role of a risk-based approach in data protection legal frameworks",** WP218, 30 Mayıs 2014.

Article 29 Working Party, **"Guidelines on Data Protection Officers ('DPOs')",** WP243, 5 Nisan 2017.

Article 29 Working Party, **"Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679",** WP248, 4 Ekim 2017.

Centre for Information Policy Leadership (CIPL), **"Ensuring the Effectiveness and Strategic Role of the Data Protection Officer under the General Data Protection Regulation",** CIPL GDPR Project DPO Paper, 17 Kasım 2016.

Centre for Information Policy Leadership (CIPL), **"Risk, High Risk, Risk Assessments and Data Protection Impact Assessments under the**

GDPR", CIPL GDPR Interpretation and Implementation Project, 21 Aralık 2016.

EUROPEN DATA PROTECTION SUPERVISOR (EDPS), **"Position paper on the role of Data Protection Officers in ensuring effective compliance with Regulation (EC) 45/2001"**, Brüksel, 28.11.2005 (Çevrimiçi) https://edps.europa.eu/sites/edp/files/publication/05-11-28_dpo_paper_en.pdf

EUROPEN DATA PROTECTION SUPERVISOR (EDPS), **"Opinion of the European Data Protection Supervisor on the Data Protection Reform Package"**, Brüksel, 07.03.2012 (Çevrimiçi) https://edps.europa.eu/sites/edp/files/publication/12-03-07_edps_reform_package_en.pdf

EUROPEN DATA PROTECTION SUPERVISOR (EDPS), **"Position Paper on the Role of Data Protection Officers of the EU Institutions and Bodies"**, 30.09.2018 (Çevrimiçi) https://edps.europa.eu/sites/edp/files/publication/18-09-30_dpo_position_paper_en.pdf

Information Commissioner's Office (ICO), "**What is personel data? Key definitions",** 24 Mayıs 2018 (Çevrimiçi), https://ico.org.uk/media/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/what-is-personal-data-1-0.pdf

Information Commissioner's Office (ICO), **"Guide to the General Data Protection Regulation (GDPR)"**, 2 Ağustos 2018 (Çevrimiçi) https://ico.org.uk/media/for-organisations/guide-to-the-general-data-protection-regulation-gdpr-1-0.pdf

Kişisel Verileri Koruma Kurumu, **"Ulusal Ve Uluslararası Alanda Kişisel Verilerin Korunmasına Duyulan İhtiyaç"**, Ankara, 2017 (Çevrimiçi) https://www.kvkk.gov.tr/SharedFolderServer/CMSFiles/8e39e0a1-6ec4-4179-a5d3-bbd8e78dce31.pdf

Kişisel Verileri Koruma Kurumu, **"6698 Sayılı Kanun'da Yer Alan Temel Kavramlar"**, Ankara, 2017 (Çevrimiçi) https://www.kvkk.gov.tr/SharedFolderServer/CMSFiles/45af208d-3718-49ed-b51a-9be9edde6ff2.pdf

Kişisel Verileri Koruma Kurumu, **"6698 Sayılı Kişisel Verilerin Korunması Kanununun Uygulanmasına Yönelik Soru Cevaplar"**, Ankara, 2017 (Çevrimiçi) https://www.kvkk.gov.tr/yayinlar/6698%20SAYILI%20K%C4%B0%C5%9E%C4%B0SEL%20VER%C4%B0LER%C4%B0N%20KORUNMASI%20KANUNUNUN%20UYGULANMASINA%20Y%C3%96NEL%C4%B0K%20SORU%20VE%20CEVAPLAR.pdf

GAZETE VE DERGİ HABERLERİ, YARARLANILAN BAŞLICA İNTERNET SİTELERİ

https://www.newlawjournal.co.uk/content/mind-gdpr (Erişim: 20.10.2019)

https://www.fieldfisher.com/en/services/privacy-security-and-information/privacy-security-and-information-law-blog/everything-youve-ever-wanted-to-know-about-dpo-but-never-dared-to-ask (Erişim: 25.10.2019)

https://www.compliancejunction.com/small-business-dpo-gdpr/ (Erişim: 10.11.2019)

Avrupa Komisyonu, (Çevrimiçi) https://www.coe.int/en/web/portal/home

General Data Protection Regulation, (Çevrimiçi) https://gdpr-info.eu/

Mevzuat, (Çevrimiçi), https://www.mevzuat.gov.tr/

OECD, (Çevrimiçi) http://www.oecd.org/

Resmi Gazete, (Çevrimiçi), https://www.resmigazete.gov.tr/