İSTANBUL BİLGİ ÜNİVERSİTESİ
LİSANSÜSTÜ PROGRAMLAR ENSTİTÜSÜ
HUKUK YÜKSEK LİSANS PROGRAMI

KİŞİSEL VERİLERİN KORUNMASI KANUNU KAPSAMINDA VERİ SORUMLUSUNUN YÜKÜMLÜLÜKLERİ

Onur GÜNBEY
117613016

Tez Danışmanı
Dr. Öğr. Üyesi Nilgün BAŞALP YILDIRIM

İSTANBUL
2020

ÖNSÖZ

Tezimin yazım sürecinde gösterdiği destek ve paylaştığı bilgiler için tez danışmanım ve değerli hocam Dr. Öğretim Üyesi Nilgün Başalp Yıldırım'a

ve

hayatımın her aşamasında bana daima sevgiyle destek olan geniş ailemin tüm üyelerine ayrı ayrı teşekkürlerimi sunuyorum.

Av. Onur Günbey

İstanbul, 2020

ÖZET

KİŞİSEL VERİLERİN KORUNMASI KANUNU KAPSAMINDA VERİ SORUMLUSUNUN YÜKÜMLÜLÜKLERİ

Av. Onur GÜNBEY

Bilgi teknolojilerinde yaşanan gelişmeler, internet kullanımının ve veri işleme faaliyetlerinin yaygınlaşması veri temelli ekonomileri oluşturmaya başlamış ve kişisel verilerin korunmasına ilişkin ulusal ve uluslararası boyutta çeşitli ve kapsamlı düzenlemeler yapılmasının önünü açmıştır. Bununla birlikte; kişisel veri kavramının çok geniş bir kapsama sahip olması, kişisel verilerin otomatik yollarla işlenmesinin giderek artması ve bir insan hakkı olarak bireylere ait kişisel verilerin korunmasına ihtiyaç duyulması özellikle bu konuda veri sorumlularına bazı yükümlülükler getirilmesini gerektirmiştir. Çalışmanın özünü de veri sorumlularının 6698 sayılı Kişisel Verilerin Korunması Kanunu kapsamındaki yükümlülükleri oluşturmaktadır. Kanun uyarınca veri sorumlusunun esasen; aydınlatma yükümlülüğü, ilgili kişiler tarafından yapılan başvuruları cevaplandırma yükümlülüğü, Kişisel Verileri Koruma Kurulu kararlarını yerine getirme yükümlülüğü, veri güvenliğine ilişkin yükümlülükler, kişisel verilerin silinmesi, yok edilmesi veya anonim hale getirilmesi yükümlülüğü, veri sorumluları siciline kayıt olma yükümlülükleri bulunmaktadır. Üç bölümden oluşan bu çalışmanın birinci bölümünde kişisel verilerin korunması hukukunun tarihsel gelişimi ve temel kaynakları, ikinci bölümünde kişisel verilerin korunması hukukunun temel kavramları ve veri sorumlusunun genel yükümlülükleri, üçüncü bölümünde ise veri sorumlularının 6698 sayılı Kişisel Verilerin Korunması Kanunu kapsamındaki yükümlülükleri detaylı bir şekilde incelenecektir. Bu çalışma ile veri sorumlularının Kanundan doğan yükümlülüklerinin güncel gelişmelerle birlikte irdelenerek uygulamadaki uyum süreçlerine ışık tutulması amaçlanmıştır.

Anahtar Kelimeler: Kişisel Verilerin Korunması, Veri Sorumlusu, Veri Sorumlusunun Yükümlülükleri, 6698 Sayılı Kişisel Verilerin Korunması Kanunu, Kişisel Verilerin İşlenmesi

ABSTRACT

THE OBLIGATIONS OF DATA CONTROLLER UNDER LAW ON THE PROTECTION OF PERSONAL DATA

Av. Onur GÜNBEY

Developments in information technologies, increasing data processing activities and internet usage have begun to form the data-driven economies and thus catalyzed the legislative efforts at the national and international levels in this regard. Additionally, the broad concept of personal data, rising trends on data processing operations by automated means, and the necessity of protecting personal data as a human right required legislative authorities to impose the data controller with several obligations on this subject. The obligations of data controller under Law No. 6698 on the Protection of Personal Data, comprise the essence of this thesis. The data controller, pursuant to the Law, has the basic obligations of informing the data subject; responding to the requests of data subjects; complying with the board decisions of the Data Protection Authority; ensuring the data security; erasing, destructing or anonymizing the personal data; registering with the registry of data controllers. The thesis consists of three chapters. In the first chapter, historical development and primary sources of personal data protection law are reviewed. Then in the second chapter, basic concepts of data protection law, conditions of personal data processing and general obligations of data controller are reviewed. Finally, the obligations of data controller under Law No. 6698 on the Protection of Personal Data are analyzed in detail. The thesis aims to enlighten the compliance practices regarding data protection by scrutinizing the obligations of data controller arising from the Law and examining the most recent developments.

Keywords: Protection of Personal Data, Data Controller, Obligations of the Data Controller, Law No. 6698 on the Protection of Personal Data, Processing of Personal Data

İÇİNDEKİLER

İKİNCİ BÖLÜM
KİŞİSEL VERİLERİN KORUNMASI HUKUKUNUN TEMEL KAVRAMLARI VE VERİ SORUMLUSUNUN GENEL YÜKÜMLÜLÜKLERİ

ÜÇÜNCÜ BÖLÜM
VERİ SORUMLULARININ KİŞİSEL VERİLERİN KORUNMASI KANUNU KAPSAMINDAKİ ÖZEL YÜKÜMLÜLÜKLERİ

KISALTMALAR

a.g.e.	:	Adı geçen eser
AB	:	Avrupa Birliği
ABAD	:	Avrupa Birliği Adalet Divanı (Court of Justice of the European Union - CJEU)
AİHM	:	Avrupa İnsan Hakları Mahkemesi (The European Court of Human Rights)
AİHS	:	Avrupa İnsan Hakları Sözleşmesi (Convention for the Protection of Human Rights and Fundamental Freedoms)
AK	:	Avrupa Konseyi (The Council of Europe)
Bkz.	:	Bakınız
BM	:	Birleşmiş Milletler
C.	:	Cilt
CNIL	:	Commission Nationale de l'Informatique et des Libertés (Bilgi ve Özgürlük Ulusal Komitesi - Fransa)
E.	:	Esas sayısı
EU	:	European Union (Avrupa Birliği)
GDPR	:	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) (Genel Veri Koruma Tüzüğü - AB)
K.	:	Karar sayısı
KVKK	:	6698 sayılı ve 24 Mart 2016 tarihli Kişisel Verilerin Korunması Kanunu
m.	:	Madde
OECD	:	The Organisation for Economic Co-operation and Development (Ekonomik İş Birliği ve Kalkınma Örgütü)
s.	:	Sayfa

S.	:	Sayı
TCK	:	5237 sayılı ve 26 Eylül 2004 tarihli Türk Ceza Kanunu
TMK	:	4721 sayılı ve 22 Kasım 2001 tarihli Türk Medeni Kanunu
vb.	:	ve benzeri
vd.	:	ve devamı

GİRİŞ

Kişisel verilerin korunmasına duyulan ihtiyaç teknolojinin gelişmesi, internetin hayatımıza girmesi ve bilgi teknolojilerinde yaşanan gelişmeler neticesinde daha önce hiç olmadığı kadar önemli bir noktaya gelmiştir. Bu doğrultuda son elli sene içerisinde kişisel verilerin korunmasına ilişkin ulusal ve uluslararası boyutta düzenlemeler yapılmıştır. Özellikle Avrupa Birliği'nin 95/46/EC sayılı Direktif ve GDPR başta olmak üzere kişisel verilerin korunması alanında yaptığı düzenlemeler, konuyla ilgili yasama faaliyeti yapma hazırlığına girişen birçok ülkeyi etkilemiştir.

Kişisel verilerin korunması alanında imzalayan devletler açısından bağlayıcı olan ilk uluslararası düzenleme Avrupa Konseyi'nin 108 Sayılı Kişisel Verilerin Otomatik İşleme Tabi Tutulması Karşısında Bireylerin Korunması Sözleşmesi'dir. 1981 yılında ilk imzalayan devletlerden birisi olan Türkiye, 108 sayılı Sözleşme'yi imzalamasından yaklaşık otuz beş sene sonra, Avrupa Birliği'nin 1995 yılında kabul ettiği 95/46/EC sayılı Direktifi esas alarak bir yasama çalışması yapmış ve 2016 yılında 6098 sayılı Kişisel Verilerin Korunması Kanunu'nu kabul etmiştir.

Çalışmamızın temel amacı kişisel verilerin korunması hukukuna ilişkin temel kavram ve ilkeleri açıkladıktan sonra veri sorumlularının KVKK'dan kaynaklı yükümlülüklerine ilişkin detaylı bir inceleme yapmaktır. Bunu yaparken ulusal ve uluslararası mevzuattan, Kişisel Verileri Koruma Kurumu'nun yayınladığı rehberlerden, belgelerden ve Kişisel Verileri Koruma Kurulu'nun konuyla ilgili verdiği çeşitli kararlardan yararlanılmıştır.

Çalışmamızın birinci bölümünde kişisel verilerin korunması hukukunun tarihsel gelişimi, kişisel verilerin korunması ihtiyacının temelleri, kişisel verilerin korunması alanındaki ilk düzenlemeler, kişisel verilerin korunması hakkının bir insan hakkı mı yoksa bir ekonomik hak mı olduğu temel ayrımı üzerinden kişisel verilerin korunması hukuki niteliği, kişisel verilerin korunması alanındaki uluslararası ve ulusal mevzuat dikkate alınarak incelenmiştir.

Çalışmamızın ikinci bölümünde veri sorumlularının genel yükümlülüklerinin anlatılabilmesi adına; kişisel verilerin korunması hukukunun temel kavramları,

95/49/EC sayılı Direktif, GDPR ve KVKK ile karşılaştırmalı olarak kişisel verilerin işlenmesine ilişkin temel ilkeler, kişisel verilerin işlenme şartları ve ilgili Kurul kararları bağlantılı olduğu ölçüde inceleme konusu olmuştur. Özellikle kişisel verilerin işlenmesine ilişkin temel ilkeler ve işlenme şartlarının incelenmesi veri sorumlularının yükümlülüklerinin tam olarak anlaşılabilmesi bağlamında büyük önem arz etmektedir. Zira bu ilkelere ve veri işlenme şartlarına uymaksızın veri sorumlusu tarafından hukuka uygun bir veri işleme faaliyetinin gerçekleştirilmesi mümkün değildir. Bu sebeple ikinci ve üçüncü bölüm veri sorumlusunun KVKK kapsamındaki yükümlülüklerinin anlatımı açısından birlikte bir bütünlük arz etmektedir.

Çalışmamızın son bölümü olan üçüncü bölümünde ise KVKK kapsamında veri sorumlusunun özel yükümlülükleri ele alınmıştır. Bu kapsamda veri sorumlusunun; aydınlatma yükümlülüğü, ilgili kişiler tarafından yapılan başvuruları cevaplandırma ve kurul kararlarını yerine getirme yükümlülüğü, veri güvenliğine ilişkin yükümlülükler, kişisel verilerin silinmesi, yok edilmesi veya anonim hale getirilmesi yükümlülüğü, veri sorumluları siciline kayıt olma yükümlülüğü detaylı şekilde incelenmiş, konuyla ilgili çeşitli Kurul kararları açıklanmış ve söz konusu yükümlülüklere uyulmaması durumunda ilgili veri sorumlusunun karşı karşıya kalabileceği yaptırımlar üzerinde durulmuştur.

BİRİNCİ BÖLÜM
KİŞİSEL VERİLERİN KORUNMASI HUKUKUNUN TARİHSEL GELİŞİMİ VE TEMEL KAYNAKLARI

1. KİŞİSEL VERİLERİN KORUNMASI HUKUKUNUN TARİHSEL GELİŞİMİ

Tarih boyunca kişilere ilişkin veriler, diğer kişiler ve kurumlar için çeşitli sebeplerle önem arz etmiştir. Bu önem kişiler arası ilişkilerde bazen salt bir meraktan doğsa da çoğu zaman ekonomik, siyasi, sosyolojik ve teknolojik sebepler başta olmak üzere çeşitli sebeplere dayanmaktadır[1].

18. yüzyılda Avrupa'da başlayan Sanayi Devrimi bireylerin çalışma hayatları ve bu eksende hayat koşullarında çok ciddi değişimler meydana getirmiştir; bu değişim kişisel verilerin korunmasına ilişkin yasal düzenlemelerin temellerinin atılmasına sebep oluşturacak yeni sosyo-ekonomik ve siyasi parametreler yaratmıştır. Örnek olarak; hızlı sanayileşme ile beraber artan fabrikalar, üretim ve çalışma alanlarında yüksek sayıda işçi çalıştıran işverenler, başta sağlıklı bir istihdam ilişkisinin tesis edilmesi ve sürdürülmesi gibi amaçlarla çalıştırdıkları işçilerin kişisel verilerini işlerken, aynı zamanda mal ve hizmetlerini sundukları pazarlardaki kişilerin çeşitli kişisel verilerini başta satış ve pazarlama gibi amaçlarla işlemeye ve gerek işçilerin gerekse pazardaki bireylerin verilerini sistematik şekilde tutmaya başlamışlardır. Diğer yandan, feodal yönetim biçiminin 15. yüzyılda zayıflamaya başlaması ve son kalıntılarının ise 18. yüzyılda başlayan Sanayi Devrimi ile birlikte yok olmasının ardından, önceki yönetim biçimlerine göre çok daha fazla kişisel veriye ihtiyaç duyan "modern devlet", merkezi yönetim ile karmaşık bürokratik yapılanma esasına dayalı bir devlet modeli olarak 20. yüzyıl itibariyle tüm dünyaya yayılmıştır. Modern devlet gerek sosyal devlet anlayışının gerekliliklerini yerine getirmek ve planlamalar yapmak, gerekse vergi toplamak, ülke bütünlüğünü, toplumsal düzeni ve bireylerin güvenliğini sağlamak, istihbarat

[1] **Elif Küzeci**, Kişisel Verilerin Korunması, 4. Bası, On İki Levha Yayıncılık, 2020, s. 19.

faaliyetleri yürütmek, politikalar oluşturmak gibi amaçlar başta olmak üzere daha birçok amacı yerine getirebilmek için kişisel verilere, bilgiye ihtiyaç duymaktadır[2]. Diğer bir ifadeyle modern devlet; ticari hayatın oluşturulması ve sürdürülmesi, toplumun düzen içinde varlığını devam ettirmesi, devletin siyasi, askeri ve diplomatik düzenini geliştirebilmesi ve daha da ötesinde devlet düzeninin sağlanması için bilgiye daima ihtiyaç duymuştur[3].

Sanayi Devrimi'nin bir diğer sosyal sonucu olan kentleşmenin yükselişi ile insanların kalabalık şehirlerde yoğunlaşması ve çalışma hayatında daha çok kendini göstermesi bireylerde özel yaşamın gizliliği hakkının daha çok tartışılmasına sebep olmuştur[4]. Aynı dönemde güçlü bir gelişim ivmesi yakalayan teknoloji, kişisel verilerin hem gerçek kişiler hem de kurumlar, şirketler ve devletler tarafından elde edilmesini, saklanmasını, işlenmesini ve transfer edilmesini daha da kolaylaştırmıştır. Bu durum, bireylerin özel hayatlarının dahi gözetlenebileceği ve kaydedilebileceği bir teknolojik seviyeye ulaştığından artık kişisel verilerin kontrol altına alınmadığı bir dünyada bireyler tehlikede olacaktır[5]. Zira son yüzyıl içerisinde teknolojinin geldiği nokta itibariyle, çok büyük sayıda veriler farklı veri depolama aygıtları ile saklanabilmekte, elektronik ortamlara aktarılabilmekte, internet vasıtasıyla da tek bir tıklama ile dünyanın bir ucundan diğer ucuna transfer edilebilmektedir[6].

Bireylerin kişisel verilerinin kolayca, kontrolsüzce ve hatta ilgilisinin izni dahi olmadan başka kişi ve kurumlar tarafından toplanması, işlenmesi, saklanması ve/veya transfer edilmesi tehlikesine karşın kişisel verilerin korunması gerekliliğine ilişkin ilk tartışmalar 1960'lı yıllarda başlamış, ilk yasal düzenleme ise 1970 yılında Almanya'nın Hessen eyaletinde kabul edilen "Hessen Veri Koruma Kanunu"dur

---

[2] **Küzeci**, s. 22.
[3] **Aydın Akgül**, Danıştay ve Avrupa İnsan Hakları Mahkemesi Kararları Işığında Kişisel Verilerin Korunması, Beta, İstanbul 2014, s.33.
[4] **Küzeci**, s. 21.
[5] **Murat Volkan Dülger**, Kişisel Verilerin Korunması Hukuku, 2. Baskı, Hukuk Akademisi Yayınları, İstanbul 2019, s.6.
[6] **Murat Volkan Dülger**, Kişisel Verilerin Korunması Kanunu ve Türk Ceza Kanunu Bağlamında Kişisel Verilerin Ceza Normlarıyla Korunması, İstanbul Medipol Üniversitesi Hukuk Fakültesi Dergisi, C.3, S.2, 2016, s. 101-167.

(Hessisches Datenschutzgesetz). Bu federe devlet düzeyindeki yasal düzenlemeden sonra kişisel verilerin korunması hakkında dünyadaki ilk ulusal düzeydeki yasal düzenleme 1973 yılında İsveç'te kabul edilen İsveç Veri Yasası'dır. Her ne kadar 1970 tarihli Hessen Veri Koruma Kanunu federe düzeyde bir düzenleme olsa da Almanya'da ülke çapında ses getiren bu düzenleme, 1977 yılında "Federal Almanya Veri Koruma Kanunu"nun kabul edilmesinin önünü açmış ve federal düzeyde koruma getirilmiştir. Bunu takip eden kişisel verilerin korunması hukukundaki ulusal düzeyde kanunlaşma hareketleri olarak 1978 yılında Fransa'da 78-17 sayılı "Bilgi Teknolojileri, Veri Dosyaları ve İnsan Hakları Kanunu[7]" ve aynı yılda Avusturya'da da "Avusturya Veri Koruma Kanunu" öne çıkmaktadır.

1980 yılı itibariyle Almanya, İsveç ve Fransa dışında neredeyse Avrupa Ekonomik Topluluğu'nun üyelerinin tamamının kişisel verilerin korunması konusunda bir çalışma yapmış veya hazırlıklarına başlamıştır[8].

Her ne kadar 1970 ve 1980'li yıllarda Batı Avrupa'da kişisel verilerin korunmasına ilişkin yasama faaliyetleri yoğunlaşsa da aynı tarihlerde Amerika Birleşik Devletleri'nde (ABD) de veri koruması hukukuna ilişkin ilk yasama faaliyetlerinin yapıldığı görülmektedir. Bu kapsamda ABD Kongresi, bankacılık sisteminin etkili şekilde devam edebilmesi ve bu sistemin etkili devamının tesisi sırasında bireylere kendi kredi raporlarını görme, güncelliğini yitirmiş veya yanlış bilgilerin çıkarılmasını talep etme hakkı veren 15 U.S.C. § 1681 numaralı Adil Kredi Raporlama Yasası'nı (*Fair Credit Reporting Act*)[9] 1970 yılında çıkarmıştır. Bu kanun; tüketicilerin kredi ve sigorta bilgilerini, tüketici raporlama kuruluşları tarafından belirli ölçütlere göre toplanması ve bireylere ait kredi bilgilerinin belli şartlar altında kullanılması ve açıklanması gerektiğini düzenlemişken, kanun kapsamındaki tüketici raporlama kuruluşlarına faaliyetlerini sürdürürken

---

[7] 1978 tarihli ve 78-17 sayılı Bilgi Teknolojileri, Veri Dosyaları ve İnsan Hakları Kanunu'nun orijinal metnine ve İngilizce çevirisine şu kaynaktan erişilebilir: https://www.ssi.ens.fr/textes/a78-17-text.html Erişim Tarihi: 1 Şubat 2020.

[8] **Andrew Charlesworth**, "The Governance of the Internet in Europe", The Internet, Law and Society, Hazırlayanlar: Yaman Akdeniz, Clive Walker, David Wall, Pearson Education Limited, İngiltere 2000, s.63.

[9] 15 U.S.C. § 1681 numaralı Adil Kredi Raporlama Yasası'nı (*Fair Credit Reporting Act*)'in orijinal metnine şu kaynaktan erişilebilir: https://www.law.cornell.edu/uscode/text/15/1681 Erişim Tarihi: 1 Şubat 2020.

tüketicilerin özel hayatlarının gizliliğine gerekli özeni gösterme sorumluluğu yüklemiştir. Kanunun çıkışını izleyen yıllarda ABD Kongresi tarafından 1974 yılında 5 U.S.C. §552a sayılı Özel Hayatın Gizliliği Yasası (*The Privacy Act*)[10] kabul edilmiştir. İçeriğinde kişilere ilişkin verilerin hangi kapsamda kullanılabileceği ve açıklanabileceğine ilişkin kurallar, sınırlamalar ve istisnalar barındıran bu kanun, özellikle kurumlara tanıdığı ayrıcalıklı veri kullanım hakları sebebiyle amacını tam olarak yerine getirememiştir.

Avrupa'ya tekrar dönecek olursak kişisel verilerin korunması hukukunda yargı kararı 1983 yılında Almanya Federal Anayasa Mahkemesi tarafından verilmiştir. Söz konusu karara, 1983 yılında yapılması planlanan nüfus sayımı için 1982 yılında Federal Alman Meclisi tarafından çıkarılan Nüfus Sayımı Yasası (*Volkszählungsgesetz 1982*) konu olmuştur. Alman hükümeti bu yasa ile ülke çapında yapılacak nüfus sayımı sırasında vatandaşlardan nüfus sayımının amacının ötesinde bazı bilgileri toplamayı hedeflemiş, bu hedefi gerçekleştirmek adına vatandaşlara birçok kişisel veri açıklama yükümlülüğü getirilmiş ve nüfus sayımı için gelen memurlarla söz konusu verileri paylaşmayan vatandaşlara ise belirli yaptırımlar öngörmüştür[11]. Hükümet nüfus sayımı sırasında 160 soruluk bir formun vatandaşlar tarafından cevaplanmasını ve bu formların uzun bir süre boyunca saklanılmasını hedeflemiştir[12]. Cevaplanması istenilen sorular arasında bireylerin çok çeşitli tercihlerinin öğrenilmesine imkân verecek kişinin dininin, mesleğinin, çalışma şartlarının, gelirinin ne olduğu gibi sorular bulunmaktaydı[13]. Ulaşılmak istenen amaç itibariyle nüfus sayımının sınırlarını aşan bu kanun her ne kadar kamuoyunda devlet tarafından ölçüsüzce kişisel veri toplanacağı sebebiyle tepkiyle

---

[10] 5 U.S.C. § 552a sayılı Özel Hayatın Gizliliği Yasası (*The Privacy Act*)'in orijinal metnine şu kaynaktan erişilebilir: https://www.law.cornell.edu/uscode/text/5/552a Erişim Tarihi: 1 Şubat 2020.

[11] **Gerrit Hornung, Chrsitoph Schnabel**, "Data Protection in Germany I: The Population Census Decision and The Right to Informational Self-Determination", Computer Law & Security Review, Cilt 25, Sayı 1, s. 84-88, Ocak 2009, s.85; **Oğuz Şimşek**, Anayasa Hukukunda Kişisel Verilerin Korunması, Beta, İstanbul 2008, s. 114-119.

[12] **Furkan Güven Taştan**, Türk Sözleşme Hukukunda Kişisel Verilerin Korunması, 2. Baskı, On İki Levha Yayınları, İstanbul 2017, s.5.

[13] **Paul Schwartz**, "Computer in German and American Constitutional Law: Towards an American Right of Informational Self-Determination", American Journal of Comparative Law, Cilt 37, s. 675-702, 1989, s. 687.

karşılansa da Alman parlamentosunun her iki kanadı tarafından oy birliği ile kabul edilmiştir[14]. Ancak ciddi eleştirilere maruz kalan yasa, Federal Alman Anayasa Mahkemesi tarafından bireylerin temel hak ve özgürlüklerinin ihlal edileceği gerekçesi detaylı şekilde açıklanarak anayasaya aykırı bulunmuş ve iptal edilmiştir. Bu kararın uluslararası boyutta ses getirmesinin yanında bir diğer önemli husus ise mahkemenin Federal Almanya Cumhuriyeti Anayasası'nın insan onurunun korunması hakkı (m. 1/1) ile bireyin kişiliğini serbestçe geliştirme hakkı (m. 2/1) hükümlerini sentezleyerek "bireyin bilginin geleceğini belirleme hakkı"nı (Almancası "*informationelle Selbstbestimmung*", İngilizcesi "*Informational Self-Determination*") yeni bir hak olarak türetmiştir[15]. Bugün Almanya'da belki de Avrupa Birliği'nin en katı veri koruma yasalarının olmasının[16] altında bu tarihi olayın yattığı söylenebilir[17].

Veri koruma hukuku, hızla gelişen teknoloji karşısında yeni sınırlar çizmek, gelişmelere ayak uydurmak ve ilerlemek için sürekli ve hızlı değişikliklerin yaşanacağı bir hukuk dalı olmaya devam edecektir. Özellikle bilişim teknolojilerinin gelişme hızı düşünüldüğünde veri koruma hukukunda belki de devrim niteliğinde sayılabilecek yeni konseptlerin ve yasal düzenlemelerin yakın tarihlerde hayatlarımıza gireceği bir gerçektir.

2. KİŞİSEL VERİLERİN KORUNMASI HAKKININ HUKUKİ NİTELİĞİ

Doktrinde, kişisel verilerin korunması hakkının hukuki niteliğine ilişkin çeşitli görüşler mevcuttur. Bu görüşler genel olarak kişisel verilerin korunması hakkının dayandığı temel menfaatlerden hareketle birbirlerinden ayrılmaktadırlar. Özellikle Avrupa'da ve ABD'de kişisel verilerin korunması ile aslında hangi menfaatin gözetildiği konusunda tarihi akışta iki farklı yaklaşım gelişmiştir.

---

[14] **Hornung/Schnabel**, s. 85; **Küzeci**, s.70.
[15] **Eva Fialova**, Data Portability and Informational Self-Determination", Masaryk Univerity Journal of Law and Technology, Cilt 8, Sayı 1, s. 45-55, 2014, s.47; **Schwartz**, s. 687.
[16] **Samantha Diorio**, "Data Protection Laws: Quilts versus Brackets", Syracuse Journal of International Law and Commerce, Cilt 42, s. 485-513, 2014, s.502.
[17] **Taştan**, s. 6.

Bunlardan bir tanesi korunan esas menfaatin insan haklarına ilişkin olduğunu ileri süren Avrupa yaklaşımı, diğeri ekonomik haklara ilişkin olduğunu ileri süren ABD yaklaşımıdır.

2.1. Ekonomik Hak Olduğu Görüşü

Kişisel verilerin korunmasını hakkını daha çok ekonomik bir hak olarak ele alan ve hakkın dayandığı menfaati insan hakları ile yakından ilişkilendirmeyen bir yaklaşımdır. Kendi içinde ikiye ayrılan bu görüş daha çok ABD'de savunulan bir görüştür.

2.1.1. Mülkiyet Hakkı Olduğu Görüşü

Mülkiyet hakkı; kişinin sahip olduğu şey üzerinde kullanma (*usus*), yararlanma, semerelendirme (*fructus*) ve tasarrufta bulunma (temlik etme, üzerinde hak tesis etme, yok etme) (*abusus*) yetkilerinin tümüne sahip olmasını ifade eder[18].

Bu görüşün savunucuları kişisel verilerin adeta bir eşya olduğundan hareketle, veri sahibinin bu veriler üzerinde tasarruf yetkisinin olduğunu ifade ederler. Dolayısıyla kişisel veri, verilerin sahibi olan ilgili kişinin malvarlığının bir parçasıdır ve kişi malik olduğu diğer şeyler üzerinde sahip olduğu mülkiyete ilişkin kullanma, yararlanma ve tasarrufta bulunma yetkilerine kişisel verileri üzerinde de sahiptir. Örneğin bu görüşe göre kişisel verinin sahibi bu kişisel verilerin mülkiyetini para karşılığında satabilecektir[19].

Kişisel verilerin korunması hakkının mülkiyet hakkına dayandığını savunan bu görüşe göre kişisel veriler, temel bir hak ve özgürlük olarak değil, kapitalist ekonomik sistem altında korunmaktadır. Nitekim bu görüşün yaygın olduğu ABD'de kişisel veriler anayasal koruma ile temel hak ve özgürlükler olarak düzenlenmemiş, daha çok sektörel bazda düzenlemeler yapılarak çeşitli korumalar getirilmiştir[20].

---

[18] **Şeref Ertaş**, Eşya Hukuku, 10. Baskı, Barış Yayınları, İzmir 2012, s. 13; **Lale Sirmen**, Eşya Hukuku, Yetkin Yayınları, Ankara 2013, s. 261.
[19] **Taştan**, s. 55.
[20] **Dülger**, s. 17.

Bu görüşle ilgili doktrinde ve Avrupa Birliği Adalet Divanı kararlarında, bu görüşün kabul edildiği düzenlemelerde yeterli ölçüde güvencelerin olmaması sebebiyle bireylerin haklarının ihlal edildiği[21], mülkiyet hakkı ile kişisel verilerin korunması kavramlarının birbiriyle uyumsuz konseptler olduğu gibi sebeplerle çeşitli eleştiriler bulunmaktadır[22].

2.1.2. Fikri Mülkiyet Hakkı Olduğu Görüşü

Bireyin kendi fikri ürünleri üzerinde sahip olduğu haklara fikri haklar denmektedir[23]. ABD'de yaygın olan bu görüşün savunucuları kişisel verilerin korunması ile fikri mülkiyet hakkını benzer ve bağlantılı bulmakta ve kişisel verilerin telif hakkına benzer bir sistemle korunabileceğini ileri sürmektedirler[24]. Burada kişisel veri sahibi olan ilgili kişi, adeta bir eser sahibi gibi düşünülmekte ve kişinin kendi eseri üzerindeki fikri mülkiyet hakkı kapsamında sahip olduğu manevi haklar gibi haklara sahip olduğu ileri sürülmektedir. Bu görüşe göre kişisel veri sahibi bu veriler üzerindeki manevi haklarını saklı tutarak mülkiyetini üçüncü kişilere veya şirketlere devredebilecektir.

Bu görüşle ilgili eleştirilerle bir önceki başlıkta anlattığımız mülkiyet hakkına ilişkin yapılan eleştiriler birbiriyle benzerlik göstermektedir[25].

2.2. İnsan Hakkı Olduğu Görüşü

Kişisel verilerin korunması hakkının temel bir insan hakkı olduğunu savunan görüşün esasen çıkış noktası Avrupa'dır[26]. Bu görüşü savunanlar fikirlerini bireyin özel hayatının gizliliği ve mahremiyetinin korunması çerçevesine oturtmaktadır[27].

Her ne kadar bilgi önceki dönemlere nazaran bugün çok daha önemli bir ekonomik değer ifade etse de günümüzde kişisel verilerin korunmasının temel bir

---

[21] **Sinem Göçmen Uyarer**, Kişisel Verilerin Korunması Kanunu ve Türk Ceza Kanunu Kapsamında Kişisel Verilerin Korunması, Seçkin Yayınevi, 2019, s.25.
[22] **Pamela Samuelson**, "Privacy as Intellectual Property?", Stanford Law Review, Cilt 52, s. 1125-1173, 2000, s. 1138.
[23] **Taştan**, s. 57.
[24] **Küzeci**, s. 66.
[25] **Uyarer**, s.28.
[26] **Küzeci**, s. 69.
[27] **a.g.e.**

insan hakkı (veya doktrindeki bazı yazarların ifadesiyle "kişilik hakkı") olduğu görüşü baskındır[28].

3. KİŞİSEL VERİLERİN KORUNMASI ALANINDAKİ ULUSLARARASI MEVZUAT

3.1. OECD

Kişisel verilerin korunması alanındaki ilk uluslararası düzenleme Ekonomik İş Birliği ve Kalkınma Örgütü (OECD)[29] tarafından 23 Eylül 1980 tarihinde kabul edilen Özel Yaşamın Gizliliğinin ve Sınır Ötesi Kişisel Veri Dolaşımının Korunmasına İlişkin Rehber İlkeler'dir[30] (İngilizcesi "*Protection of Privacy and Transborder Flows of Personal Data*").

Kişisel verilerin korunmasına ilişkin asgari gerekliliklerin düzenlendiği Rehber İlkeleri bir tavsiye kararı niteliğinde olduğundan, OECD'ye üye olan devletler için herhangi bir bağlayıcılığı bulunmamaktadır[31].

Rehber İlkeler, üye ülkelere kişisel verilerin korunması kapsamında yasal düzenlemelerde ve politikalarda dikkat edilmesi gereken asgari ölçütlere ilişkin tavsiyeleri ve bu konuda aşağıda sayılan sekiz ilkeyi içermektedir:

- "1. İlke: *Veri toplamanın sınırlı olması ilkesi* (m. 7),
- 2. İlke: *Verilerin belirli bir nitelikte olması (veri kalitesi) ilkesi* (m. 8),
- 3. İlke: *Amacın belirliliği ilkesi* (m. 9),
- 4. İlke: *Sınırlı kullanım ilkesi* (m. 10),

---

[28] **a.g.e.**

[29] The Organisation for Economic Co-operation and Development (OECD) - Ekonomik İş Birliği ve Kalkınma Örgütü 1961 yılında, üye ülkelerde demokrasinin, insan haklarının ve ekonominin gelişimine, küresel ticaretin büyütülmesine, yaşam standartlarının yükseltilmesine, işsizliğin azaltılmasına katkı sağlamak amacıyla Türkiye'nin de arasında olduğu yirmi kurucu ile kurulmuştur. Bkz. http://www.oecd.org/ Erişim Tarihi: 2 Şubat 2020.

[30] 23 Eylül 1980 tarihli "OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data"nın orijinal metnine şu kaynaktan erişilebilir: https://www.oecd.org/internet/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm Erişim Tarihi: 2 Şubat 2020. Bundan sonra "Rehber İlkeler" olarak anılacaktır.

[31] **Nilgün Başalp**, Kişisel Verilerin Korunması ve Saklanması, Yetkin Yayınları, Ankara 2004, s. 24; **Küzeci**, s. 120.

- 5. İlke: *Veri güvenliği ilkesi* (m. 11),
- 6. İlke: *Açıklık ilkesi* (m. 12),
- 7. İlke: *Bireyin katılımı ilkesi* (m. 13),
- 8. İlke: *Hesap verilebilirlik ilkesi* (m. 14)"

Her ne kadar tavsiye niteliğinde olması itibariyle üye devletler açısından bağlayıcılığı olmasa da ülkelerin kişisel verilerin korunmasına ilişkin mevzuatında Rehber İlkeler'in dikkate alındığı görülmektedir. 2016 yılında çıkan 6698 sayılı Kişisel Verilerin Korunması Kanunu'nun hazırlanma evresinde de Rehber İlkeler dikkate alınmış, Kanun'un genel gerekçesinde de Rehber İlkeler'e atıflarda bulunulmuştur.

Gelişen teknoloji ve değişen ihtiyaçlar doğrultusunda veri koruma ihtiyacındaki dünya çapındaki artış sebebiyle Rehber İlkeler, 2013 yılında OECD tarafından revize edilmiştir[32]. Bu kapsamda ulusal gizlilik stratejileri, gizlilik yönetimi programları ve veri güvenliğini ihlal bildirimi konularında yeni bazı fikirler benimsenmiştir.

3.2. Birleşmiş Milletler

II. Dünya Savaşı'ndan sonra, dünyadaki barış ve güvenliğin tesis edilmesi, insan hakları ile temel hak ve özgürlüklerin güvence altına alınarak geliştirilmesi, sürdürülebilir kalkınmanın desteklenmesi amaçlarının gerçekleştirilmesi için 24 Ekim 1945 tarihinde Türkiye Cumhuriyeti'nin de arasında olduğu 51 devletin üyeliğiyle kurulan Birleşmiş Milletler'in[33] (BM) günümüz itibariyle 193 üyesi bulunmaktadır.

[32] The OECD Privacy Framework. 2013 yılında OECD tarafından yapılan revizyondan sonra Rehber İlkeler'in İngilizce metnine şu kaynaktan erişilebilir: https://www.oecd.org/sti/ieconomy/oecd_privacy_framework.pdf Erişim Tarihi: 2 Şubat 2020.

[33] Birleşmiş Milletler (*United Nations*) hakkında daha detaylı bilgiye şu kaynaktan erişilebilir: https://www.un.org/en/about-un/ Erişim Tarihi: 2 Şubat 2020.

3.2.1. İnsan Hakları Evrensel Bildirisi

BM, 10 Aralık 1948 tarihinde "İnsan Hakları Evrensel Bildirisi"ni[34] kabul ederek insan haklarının korunması alanında dünya çapında ses getiren ve kısa bir zaman diliminde yaygın bir coğrafyada benimsenen bir uluslararası düzenleme yapmıştır. Çalışma konumuz itibariyle Bildiri'nin özel hayatın gizliliği hakkını düzenlediği 12. maddesi içerik itibariyle önem arz etmektedir. Bildiri 12. maddesinde; "*Hiç kimse özel hayatı, ailesi veya haberleşmesine yönelik keyfi müdahalelere ya da onur ve şöhretine karşı saldırılara maruz bırakılamaz. Herkesin bu müdahale veya saldırılara karşı kanun yolu ile korunma hakkı vardır.*" hükmünü düzenlemiştir. Kişisel verilerin korunması hukukunun tarihsel gelişiminde yaşanan olayların çıkış noktaları genellikle bireylerin özel hayatlarının gizliliğinin müdahale edilerek devletlerce ihlal edilmesi olmuştur. Bu durum devletlerce bireyin özel hayatın gizliliği hakkını tanımasını, korumasını ve geliştirmesini talep etmesi sonucunu doğurmuştur.

3.2.2. Birleşmiş Milletler Medeni ve Siyasi Haklar Uluslararası Sözleşmesi

BM genel kurulunca 1966 yılında kabul edilmesinin ardından, 1976 yılında yürürlüğe giren Medeni ve Siyasi Haklar Uluslararası Sözleşmesi'nin[35] çalışma konumuz itibariyle önem arz eden "Mahremiyet Hakkı" başlıklı 17. maddesinde, Bildiri'nin bir üst başlık altında alıntıladığımız 12. maddesini neredeyse birebir tekrar ederek düzenlemiştir. Ek olarak, BM İnsan Hakları Komitesi, bahsi geçen 17. maddenin kapsamını açıkladığı 16. Genel Yorum'unda, bireylerin kişisel verilerinin korunması hakkının bireyin özel hayatının gizliliği hakkı kapsamında gördüğünü açıklamıştır.

---

[34] İnsan Hakları Evrensel Bildirisi'nin (İngilizcesi *Universal Declaration of Human Rights*) günümüz itibariyle 523 dildeki tercümesinin bulunduğu internet sayfasına şu uzantıdan erişilebilir: https://www.ohchr.org/EN/UDHR/Pages/Language.aspx?LangID=trk Erişim Tarihi: 2 Şubat 2020. Bundan sonra "Bildiri" olarak anılacaktır.

[35] Medeni ve Siyasi Haklar Uluslararası Sözleşmesi'nin (İngilizcesi *International Covenant on Civil and Political Rights*) İngilizce metninin bulunduğu sayfaya şu uzantıdan erişilebilir: https://www.ohchr.org/en/professionalinterest/pages/ccpr.aspx Erişim Tarihi: 4 Şubat 2020.

3.2.3. Bilgisayara Geçirilmiş Kişisel Veri Dosyalarına İlişkin Rehber İlkeler

BM'nin doğrudan doğruya kişisel verilerin korunmasına ilişkin yaptığı ilk düzenleme 14 Aralık 1990 tarihinde BM Genel Kurulu tarafından kabul edilen "Bilgisayara Geçirilmiş Kişisel Veri Dosyalarına İlişkin Rehber İlkeler"dir[36]. Teknolojinin gelişmesiyle beraber internet ve bilgisayarların kişisel veri ihlallerine daha kolay bir zemin hazırlıyor olması sebebiyle metin içerisinde aşağıdaki ilkeler kabul edilmiştir:

- "Verilerin meşru ve dürüst yollarla toplanması ve işlenmesi ilkesi
- Verilerin doğruluğu ilkesi
- Amacın belirliliği ilkesi
- İlgili kişinin erişimi ilkesi
- Ayrımcılık yasağı ilkesi
- Veri güvenliği ilkesi
- Denetim ve yaptırım ilkesi
- Verilerin sınır ötesi akışı ilkesi"

Bahsi geçen düzenleme, Denetim ve Yaptırım başlıklı A.8. maddesi ile kişisel verilerin korunmasına ilişkin rehber ilkelere uyulup uyulmadığını denetlemek için kanunla oluşturulacak yetkili ve bağımsız bir veri koruma otoritesinin kurulması gerektiğini işaret eden ilk uluslararası düzenleme olmuştur[37]. Ancak hukuken bir tavsiye kararı niteliğinde olan ve üye devletler açısından bağlayıcılığı olmayan bu ilkelerin BM'nin uluslararası etki seviyesine rağmen OECD Veri Koruma İlkeleri ve AK Sözleşmesi'ne kıyasla çok daha kısıtlı bir etkisi olmuştur[38].

---

[36] Bilgisayara Geçirilmiş Kişisel Veri Dosyalarına İlişkin Rehber İlkeler'in (İngilizcesi *Guidelines for the Regulation of Computerized Personal Data Files*) İngilizce metninin bulunduğu sayfaya şu uzantıdan erişilebilir: https://www.refworld.org/pdfid/3ddcafaac.pdf Erişim Tarihi: 4 Şubat 2020.
[37] **Lee A. Bygrave**, Data Protection Law (Approaching Its Rationale, Logic and Limits), Kluwer Law International, Hollanda 2002, s. 73, 350.
[38] **Küzeci**, s. 127.

3.3. Avrupa Konseyi

II. Dünya Savaşı'ndan sonra kurulan ve kişisel verilerin korunması alanında uluslararası düzenlemeler yapan bir diğer kuruluş da Avrupa Konseyi'dir (AK)[39]. 5 Mayıs 1949 tarihinde AK Statüsü'nün[40] Londra'da imzaya açılmasının ardından Türkiye'nin de hemen imza atmak suretiyle üyesi olduğu Konsey, insan hakları ve özgürlüğünü, hukukun üstünlüğünü koruyup güçlendirmeyi ve bu değerlere sahip olan üye ülkeler arasında sıkı bir birlik geliştirmeyi amaçlamaktadır.

3.3.1. 108 Sayılı Kişisel Verilerin Otomatik İşleme Tabi Tutulması Karşısında Bireylerin Korunması Sözleşmesi (108 Sayılı Sözleşme) ve 181 Sayılı Ek Protokol

Kişisel verilerin korunması alanındaki uluslararası düzenlemeler içerisinde imzalayan devletler açısından bağlayıcılığı bulunan ilk hukuki belge 28 Ocak 1981 tarihinde AK tarafından Strazburg'da imzaya açılan ve beş devletin imzalaması ile 1 Ekim 1985 tarihinde yürürlüğe giren 108 Sayılı Kişisel Verilerin Otomatik İşleme Tabi Tutulması Karşısında Bireylerin Korunması Sözleşmesi'dir[41].

Türkiye, her ne kadar 108 Sayılı Sözleşme'yi imzaya açılma tarihi olan 28 Ocak 1981 tarihinde imzalamış ise de onay kanunu[42] ancak 17 Mart 2016 tarihli ve 29656 sayılı Resmî Gazete'de yayımlanabilmiş[43] ve bu tarih itibariyle 108 Sayılı Sözleşme Türkiye Cumhuriyeti'nde bağlayıcı hale gelmiştir. Böylece Türkiye

---

[39] Bundan sonra "AK" veya "Konsey" olarak anılacaktır.

[40] Avrupa Konseyi Statüsü (İngilizcesi *Statute of the Concil of Europe*) ile ilgili detaylı bilgi ve İngilizce metninin bulunduğu sayfaya şu uzantıdan erişilebilir: https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/001 Erişim Tarihi: 5 Şubat 2020.

[41] 108 Sayılı Kişisel Verilerin Otomatik İşleme Tabi Tutulması Karşısında Bireylerin Korunması Sözleşmesi (İngilizcesi *Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data*) ile ilgili detaylı bilgi ve İngilizce metninin bulunduğu sayfaya şu uzantıdan erişilebilir: https://www.coe.int/en/web/conventions/search-on-treaties/-/conventions/treaty/108 Erişim Tarihi: 6 Şubat 2020. Bundan sonra "108 Sayılı Sözleşme" olarak anılacaktır.

[42] 6669 sayılı ve 30 Ocak 2016 tarihli "Kişisel Verilerin Otomatik İşleme Tabi Tutulması Karşısında Bireylerin Korunması Sözleşmesinin Onaylanmasının Uygun Bulunduğuna Dair Kanun"a şu uzantıdan erişilebilir: https://www.resmigazete.gov.tr/eskiler/2016/02/20160218-2.pdf Erişim Tarihi: 6 Şubat 2020.

[43] 108 Sayılı Sözleşme'nin Resmî Gazete'de yayımlanan Türkçe metninin bulunduğu sayfaya şu uzantıdan erişilebilir: https://www.resmigazete.gov.tr/eskiler/2016/03/20160317-2.pdf Erişim Tarihi: 6 Şubat 2020.

sözleşmeyi ilk imzalayan devletlerden biri olurken, onaylayarak iç hukukunda yürürlüğe koyan son ülke olmuştur[44]. Sözleşme AK üye devletlerine ek olarak üye olmayan devletlerin de imzasına açıktır.

108 Sayılı Sözleşme'de kişisel verilerin korunması hakkı özel hayatın gizliliğinden ayrı bir hak olarak koruma altına alınmış ve sözleşmenin "Veri Korumasına İlişkin Temel İlkeler" başlıklı II. Bölümünde taraf devletlerin uymaları gereken aşağıdaki ilkeler düzenlenmiştir:

- Veri kalitesi (verilerin belirli bir nitelikte olması) (m. 5)
- Özel veri kategorileri (hassas nitelikteki kişisel verilerin özel olarak korunması) (m. 6)
- Veri güvenliği (verilere erişim yetkilerinin belirlenmesi ve saklama alanlarına ilişkin tedbirlerin alınması) (m. 7)
- İlgili kişinin hakları (ilgili kişiye bilgi alma, verilerinin düzeltilmesini, silinmesini talep etme, yasal yollara başvurma hakkı verilmesi) (m. 8)

108 Sayılı Sözleşme'nin V. Bölümü uyarınca sözleşmenin yürürlüğe girmesinin akabinde bir Danışma Komitesi oluşturulmuştur. Bu komitenin sözleşme maddelerini yorumlamak, değişiklik tekliflerinde bulunmak, sözleşmenin kapsamına giren uygulamaları geliştirmek gibi fonksiyonları bulunmaktadır[45].

Danışma Komitesi 8 Kasım 2001 tarihinde 181 Sayılı Ek Protokol'ü[46] imzaya açmış ve bu Ek Protokol beş devlet tarafından onaylandıktan sonra 1 Temmuz 2004 tarihinde 108 Sayılı Sözleşme'nin ek bir protokolü olarak yürürlüğe girmiştir. 181 Sayılı Ek Protokol, taraf devletler için 108 Sayılı Sözleşme'de bulunmayan veri işleme ve koruma faaliyetlerini denetlemek üzere bağımsız bir veri koruma otoritesinin kurulmasını öngörmüş, ayrıca ülkeler arasında yapılan kişisel veri transferlerine ilişkin birtakım kurallar belirlemiştir.

---

[44] **Dülger**, s. 28.
[45] Bkz. 108 Sayılı Sözleşme'nin 18. maddesi.
[46] 181 Sayılı Ek Protokol'ün (İngilizce tam ismi *Additional Protocol to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, regarding Supervisory Authorities and Transborder Data Flows*) İngilizce metninin bulunduğu sayfaya şu uzantıdan erişilebilir: https://www.coe.int/en/web/conventions/full-list/-/conventions/rms/0900001680080626 Erişim Tarihi: 7 Şubat 2020.

108 Sayılı Sözleşme, 18 Mayıs 2018 tarihinde AK Bakanlar Komitesi tarafından Kişisel Verilerin Otomatik İşleme Tabi Tutulması Karşısında Bireylerin Korunması Sözleşmesinde Değişiklik Yapılmasına Dair Protokol'ün[47] kabul edilmesiyle yenilenmiş[48] ve bilişim teknolojilerinin getirdiği yeniliklere uyumlanmak için daha etkili veri koruma kuralları getirdiğini işaret etmek adına bu değişikliklerden sonra 108 Sayılı Sözleşme "Convention 108+" veya "108+" ismiyle anılmıştır[49].

3.3.2. Avrupa İnsan Hakları Sözleşmesi

Avrupa Konseyi tarafından 4 Kasım 1950 tarihinde kabul edilerek Roma'da imzaya açılan Avrupa İnsan Hakları Sözleşmesi[50] (AİHS) günümüzde hala insan hakları alanındaki en önemli uluslararası düzenlemelerin başında gelmektedir[51]. Özellikle 1959 yılında Avrupa İnsan Hakları Mahkemesi'nin (AİHM) Strazburg'da uluslararası mahkeme statüsünde kurulmasıyla birlikte ile AİHS'in insan hakları alanındaki en etkili uluslararası sözleşme olduğu söylenebilir[52].

Her ne kadar AİHS bünyesinde kişisel verilerin korunmasına ilişkin müstakil bir düzenleme bulunmasa da çalışma konumuz açısından önemli gördüğümüz özel hayatın gizliliği hakkının korunduğu AİHS'in "Özel ve Aile Hayatına Saygı" başlıklı 8. maddesinde şu hüküm düzenlenmiştir[53]:

---

[47] Kişisel Verilerin Otomatik İşleme Tabi Tutulması Karşısında Bireylerin Korunması Sözleşmesinde Değişiklik Yapılmasına Dair Protokol (İngilizcesi *Protocol amending the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data)* İngilizce metninin bulunduğu sayfaya şu uzantıdan erişilebilir: https://www.coe.int/en/web/conventions/full-list/-/conventions/rms/09000016808ac918 Erişim Tarihi: 7 Şubat 2020.

[48] **Dülger**, s.29; bkz. https://www.coe.int/en/web/data-protection/-/modernisation-of-convention-108 Erişim Tarihi: 7 Şubat 2020.

[49] Bkz. https://rm.coe.int/convention-108-convention-for-the-protection-of-individuals-with-regar/16808b36f1 Erişim Tarihi: 7 Şubat 2020.

[50] Avrupa İnsan Hakları Sözleşmesi'ne (İngilizce tam ismi *Convention for the Protection of Human Rights and Fundamental Freedoms*) ilişkin detaylı bilgilerin bulunduğu sayfaya şu uzantıdan erişilebilir: https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/005 Erişim Tarihi: 9 Şubat 2020. Bundan sonra "AİHS" olarak alınacaktır.

[51] **Küzeci**, s.138.

[52] **Dülger**, s. 30.

[53] Avrupa İnsan Hakları Sözleşmesi'nin İngilizce metnine şu uzantıdan erişilebilir: https://www.coe.int/en/web/conventions/full-list/-/conventions/rms/0900001680063765 Erişim Tarihi: 9 Şubat 2020.

"(*1) Herkes özel ve aile hayatına, konutuna ve yazışmasına saygı gösterilmesi hakkına sahiptir.*

(2) Bu hakkın kullanılmasına bir kamu makamının müdahalesi, ancak müdahalenin yasayla öngörülmüş ve demokratik bir toplumda ulusal güvenlik, kamu güvenliği, ülkenin ekonomik refahı, düzenin korunması, suç işlenmesinin önlenmesi, sağlığın veya ahlakın veya başkalarının hak ve özgürlüklerinin korunması için gerekli bir tedbir olması durumunda söz konusu olabilir."[54]

AK bünyesinde kişisel verilerin korunmasına ilişkin ilk düzenleme böylece AİHS'in yukarıda alıntılanan 8. maddesi tahtında gerçekleştirilmiştir[55]. Nitekim AİHM, 8. madde ile ilgili verdiği birçok kararında bireyin kişisel verilerinin korunması hakkının AİHS'in 8. maddesi başlığı altında korunduğunu belirtmiştir[56].

3.4. Avrupa Birliği

II. Dünya Savaşı'nın olumsuz etkilerinin silinmesi ve kalıcı barışın sağlanması için kurulan bir diğer uluslararası oluşum Avrupa Birliği'dir[57]. İlk olarak 1951 yılında imzalanan Paris Antlaşması ile Avrupa Ekonomik Kömür ve Çelik Topluluğu adıyla kurulsa da daha sonra 1957 yılında imzalanan Roma Antlaşması ile Avrupa Ekonomik Topluluğu'na dönüşmüştür. Son olarak AB, 1992 yılında imzalanan Maastricht Antlaşması (diğer adıyla Avrupa Birliği Antlaşması) ile Avrupa Ekonomik Topluluğu, ekonomik ve parasal birlik ile ortak dışişleri ve güvenlik politikalarını tesis etmek üzere, Avrupa Birliği adını almıştır.

---

[54] Avrupa İnsan Hakları Sözleşmesi'nin Türkçe metnine şu uzantıdan erişilebilir: https://www.danistay.gov.tr/upload/avrupainsanhaklarisozlesmesi.pdf Erişim Tarihi: 9 Şubat 2020.

[55] **Başalp**, s.25.

[56] **Taştan**, s. 13; Konuyla ilgili başlıca AİHM kararlarına ilişkin künyeleri inceleyebilirsiniz: AİHM, Klass ve Diğerleri v. Almanya, 5029/71 sayılı ve 6 Eylül 1978 tarihli; AİHM, Malone v. Birleşik Krallık, 8697/79 sayılı ve 2 Ağustos 1984 tarihli; AİHM, Leander v. İsviçre, 9248/81 sayılı ve 26 Mart 1987 tarihli; AİHM, Gaskin v. Birleşik Krallık, 10454/83 sayılı ve 7 Temmuz 1989 tarihli; AİHM, Amann v. İsviçre, 27798/95 sayılı ve16 Şubat 2000 tarihli; AİHM, Rotaru v. Romanya, 28341/95 sayılı ve 4 Mayıs 2000 tarihli; Segerstedt-Wiberg ve Diğerleri v. İsveç, 62332/00 sayılı ve 6 Haziran 2006 tarihli kararlar, https://hudoc.echr.coe.int/ . Erişim Tarihi: 9 Şubat 2020.

[57] Avrupa Birliği'nin resmi internet sitesi ve detaylı bilgi için şu adresi ziyaret edebilirsiniz: https://europa.eu/european-union/index_en Erişim Tarihi: 9 Şubat 2020. Bundan sonra "AB" olarak anılacaktır.

Kişisel verilerin korunmasını temel insan haklarının kapsamında gören Batı Avrupa ülkeleri, veri koruması hukukunun lokomotifi konumundadır[58].

3.4.1. 95/46/EC Sayılı Kişisel Verilerin İşlenmesi ve Serbest Dolaşımı Bakımından Bireylerin Korunmasına İlişkin Avrupa Parlamentosu ve Avrupa Konseyi Direktifi

Avrupa Birliği tarafından hazırlıklarına 1990'lı yıllarda başlanan ve 24 Ekim 1995 tarihinde Avrupa Konseyi tarafından yayınlanan "95/46/EC Sayılı Kişisel Verilerin İşlenmesi ve Serbest Dolaşımı Bakımından Bireylerin Korunmasına İlişkin Avrupa Parlamentosu ve Avrupa Konseyi Direktifi"[59] kişisel verilerin korunması hukukundaki en önemli düzenlemelerden biridir. Direktif ile birlikte kişisel verilerin AB içerisinde korunmasına ve bu verilerin sınır ötesi serbest dolaşımına ilişkin kurallar belirlenmiştir[60].

Direktif'in "Veri Kalitesine İlişkin İlkeler" başlıklı 6. maddesindeki ilkeler aşağıdaki gibidir:

- "Hukuka ve dürüstlük kurallarına uygun olma,
- Belirli, açık ve meşru amaçlar için işlenme,
- İşlendikleri amaçla bağlantılı, sınırlı ve ölçülü olma,
- Doğru ve gerektiğinde güncel olma,
- İlgili mevzuatta öngörülen veya işlendikleri amaç için gerekli olan süre kadar muhafaza edilme."

Yukarıda özetlenen ve ileride ayrı bir başlık altında detaylı açıklayacağımız ilkelerin neredeyse aynıları 6698 sayılı Kanun'un (kişisel verilerin işlenmesinde) "Genel İlkeler" başlıklı 4. maddesinde de düzenlenmiştir. Kanun'un, sadece bu

---

[58] **Dülger**, s.32.

[59] 95/46/EC Sayılı Kişisel Verilerin İşlenmesi ve Serbest Dolaşımı Bakımından Bireylerin Korunmasına İlişkin Avrupa Parlamentosu ve Avrupa Konseyi Direktifi'nin (İngilizcesi, *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*) İngilizce metni için şu adresi ziyaret edebilirsiniz: https://eur-lex.europa.eu/eli/dir/1995/46/oj?eliuri=eli:dir:1995:46:oj Erişim Tarihi: 11 Şubat 2020. 95/46/EC Sayılı Direktif bundan sonra "Direktif" olarak anılacaktır.

[60] **Başalp**, s. 26; **Leyla Keser, Mahir Ülgü, Cüneyd Er**, Elektronik Sağlık Kayıtları ve Özel Hayatın Gizliliği, İstanbul Bilgi Üniversitesi Yayınları, İstanbul 2009, s. 115.

madde özelinde değil genel itibariyle Direktif'in diğer düzenlemeleri ile de ciddi anlamda benzerlikleri bulunmaktadır. Bu ilkelerin benzerleri 108 Sayılı Sözleşme'de düzenlenen ilkelerle benzerlik göstermektedir.

Avrupa Birliği'nin İşleyişi Hakkında Antlaşma'nın[61] 288. maddesi uyarınca direktiflerin üye ülkeler tarafından doğrudan uygulanması söz konusu değildir. Direktifler, üye ülkelere belirli bir konuda ulaşılmak istenen amacı, birlik içinde tüm üye devletlerin uyumlu hale gelmesini istedikleri hedefi belirlemektedir. Bu kapsamda direktifler ulaşılması istenen sonuçlar itibariyle muhatap her üye devleti bağlamaktadır. Üye devletlerin, direktiflerde yer alan düzenlemeleri iç hukuklarına adapte ederken şekil ve yöntem açısından takdir yetkileri bulunmaktadır. Bu durum zamanla üye devletlerin mevzuatında hedeflenen yeknesaklığı sağlayamamasına ve üye devletler arasındaki uygulamaların birbirinden farklılık göstermesine sebep olmuştur. Sonuç itibariyle Direktif getiriliş amacını tam anlamıyla gerçekleştirememiş ve AB içinde daha etkili, güncel ihtiyaçlara çözüm getiren ve üye devletlerin uygulamalarını birbiriyle uyumlu hale getirecek bir düzenleme yapılması ihtiyacı doğmuştur[62].

3.4.2. Avrupa Birliği Temel Haklar Şartı

Avrupa Birliği Temel Haklar Şartı, 7 Aralık 2000 tarihinde Fransa'nın Nice şehrinde kabul edilmiş ve Lizbon Antlaşması'nın yürürlüğe girdiği tarih olan 1 Aralık 2009'da tam anlamıyla yürürlüğe girmiştir[63]. Düzenlemenin amacı Avrupa vatandaşları ve AB'de yaşayan tüm insanların temel hak ve özgürlüklerini, siyasal ve ekonomik haklarını tek bir hukuki düzenleme altında toplamaktır.

Şartın "Özgürlükler" başlıklı İkinci Bölümünün "Özel ve Aile Hayatına Saygı" başlıklı 7. maddesi şöyledir:

---

[61] Avrupa Birliği'nin İşleyişi Hakkında Antlaşma'nın Türkçe metnine şu uzantıdan ulaşabilirsiniz: https://www.ab.gov.tr/files/pub/antlasmalar.pdf Erişim Tarihi: 11 Şubat 2020.

[62] **Nilgün Başalp**, "Avrupa Birliği Veri Koruması Genel Regülasyonu'nun Temel Yenilikleri", Marmara Üniversitesi Hukuk Araştırmaları Dergisi, Cilt 21, Sayı 1, s. 77-105, 2015, s. 82.

[63] Avrupa Birliği Temel Hakları Şartı'nın (İngilizcesi, *Charter of the Fundamental Rights of the European Union*) İngilizce metnine şu uzantıdan ulaşabilirsiniz: https://www.europarl.europa.eu/charter/pdf/text_en.pdf Erişim Tarihi: 11 Şubat 2020.

"*(1) Herkes özel ve aile yaşamına, evine ve iletişimine saygı gösterilmesi hakkına sahiptir.*"

Görüleceği üzere yukarıdaki maddede AİHS m. 8/1'den farklı olarak "haberleşme" ifadesi yerine "iletişim" ifadesi kullanılmış, böylece koruma alanı genişletilmiş ve her türlü yeni iletişim aracının da kapsanması konusunda herhangi bir soru işareti bırakılmamıştır[64].

Avrupa Birliği Temel Haklar Şartı'nın "Kişisel Verilerin Korunması" başlıklı 8. maddesi şöyledir:

> "*(1) Herkes, kendisine ilişkin kişisel bilgilerinin korunmasını isteme hakkına sahiptir.*
>
> *(2) Bu tür bilgiler, belirtilen amaçlar için ve ilgili kişinin rızasına veya kanunda öngörülen diğer meşru bir temele dayalı olarak işlenebilir. Herkes kendisi hakkında toplanmış bu verilere erişme ve bunları düzelttirme hakkına sahiptir.*
>
> *(3) Bu kurallara uyulması bağımsız bir makam tarafından denetlenecektir.*"

Bu iki maddenin birbirinden bağımsız hükümler olarak yazılmasının bireyin kişisel verilerin korunması hakkına, özel hayatın gizliliği hakkından ayrı bir koruma sağlanması bakımından önemi bulunmaktadır.

3.4.3. 2002/58/EC Sayılı Haberleşme Sektöründe Özel Yaşamın Korunması ve Kişisel Verilerin İşlenmesi Direktifi

95/46/EC Sayılı Direktif, AB içinde o zamana kadar kişisel verilerin korunması konusunda hazırlanan en geniş kapsamlı düzenleme olmuş ise de zamanla sektörel bazda özel ihtiyaçlar belirmiştir. Bu kapsamda 15 Aralık 1997 yılında haberleşme sektörünün veri koruma hukukundaki ihtiyaçlarının karşılanması için 97/66/EC Sayılı Haberleşmenin Gizliliği Direktifi[65] çıkarılmıştır.

---

[64] **Küzeci**, s. 163.

[65] 97/66/EC Sayılı Haberleşmenin Gizliliği Direktifi'nin (İngilizcesi, *Directive 97/66/EC of the European Parliament and of the Council of 15 December 1997 concerning the processing of personal data and the protection of privacy in the telecommunications sector*) İngilizce metnine şu uzantıdan ulaşabilirsiniz: https://eur-lex.europa.eu/eli/dir/1997/66/oj Erişim Tarihi: 13 Şubat 2020.

Bu direktif incelendiğinde özellikle telekomünikasyon sektöründe hizmet verenlere kullanıcıların haberleşmelerinin gizliliğini sağlamaları için bir dizi sorumluluklar getirildiği görülmektedir.

Teknolojik gelişmeler neticesinde elektronik haberleşmenin yaygınlaşması ve yeni ihtiyaçlar doğrultusunda 12 Temmuz 2002 tarihinde elektronik haberleşme sektöründe rekabetin arttırılması ve kullanıcıların gizliliklerinin korunması amacıyla "Avrupa Parlamentosu ve Konseyi'nin 2002/58/EC Sayılı Haberleşme Sektöründe Özel Yaşamın Korunması ve Kişisel Verilerin İşlenmesi Direktifi" kabul edilerek 97/66/EC Sayılı Haberleşmenin Gizliliği Direktifi ilga edilmiştir. Bu direktif kapsamında üye devletlere elektronik iletişim araçlarındaki iletişim trafiği ile konum bilgilerini kayıt altında tutma yükümlülüğü getirilmiştir, ayrıca iletişim araçlarıyla yapılan haberleşmelerde elde edilen kişisel verilerin meşru şekilde işlenmesi düzenlenmiştir[66].

2002/58/EC Sayılı Direktif'in metninin içerisinde 95/46/EC Sayılı Direktif'e çok sayıda atıfta bulunulduğunu ve esasen 95/46/EC Sayılı Direktif'i tamamlayıcı nitelikte olduğunu[67] belirtmek isteriz.

3.4.4. 2016/680 Sayılı Emniyet Teşkilatında Kişisel Verilerin Korunmasına İlişkin Direktif

95/46/EC Sayılı Direktif'in yürürlüğünün devam ettiği dönemde emniyet teşkilatı için de bir ek düzenleme yapılması ihtiyacı doğmuştur. Bu konudaki ilk yasal düzenleme bir çerçeve kararı ile yapılmıştır. AB Konseyi'nin 27 Kasım 2008 tarihli ve 2008/977/JHA Sayılı Çerçeve Kararı'nda[68] cezai konularda kolluk teşkilatının adli iş birliği yapmasına ilişkin kurallar düzenlenmiştir. Bu kararda kolluk teşkilatı ve adli teşkilatın verileri yalnızca üye devletler arasında paylaşılabilmesi ve buna ilişkin çeşitli diğer kurallar düzenlenirken, emniyet

[66] **Şimşek**, s. 57.
[67] **Dülger**, s. 36.
[68] 2008/977/JHA Sayılı Çerçeve Kararı'nın İngilizce metnine şu uzantıdan ulaşabilirsiniz: http://data.europa.eu/eli/dec_framw/2008/977/oj Erişim Tarihi: 13 Şubat 2020.

teşkilatı tarafından ülke içindeki kişisel verileri işleme faaliyetleri kararın kapsamına dahil edilmemiştir[69].

AB üye devletlerinin emniyet ve kolluk teşkilatlarındaki iş birliğinin güçlendirilmesi, terör ve önemli suçlarla mücadele edilmesi ve bu amaçları gerçekleştirirken bireylerin temel haklarının korunmasının temini amacıyla Genel Veri Koruma Tüzüğü'ne paralel olarak 27 Nisan 2016 tarihli ve 2016/680 sayılı "Yetkili Makamlar Tarafından Suçun Önlenmesi, Soruşturulması, Tespiti veya Kovuşturulması veya Cezai Süreçlerin Yürütülmesi Amacıyla İşlenen Kişisel Verilere İlişkin Gerçek Kişilerin Korunmasına ve Bu Tür Verilerin Serbest Dolaşımına Dair Direktif" çıkarılmıştır[70].

3.4.5. 2006/24/EC Sayılı İletişim Trafik Verilerinin Saklanmasına Dair Direktif

7 Temmuz 2005 tarihinde Londra metrosunda gerçekleştirilen bombalı terör saldırısının akabinde, terörle mücadele kapsamında *ciddi bir suç şüphesinin varlığı halinde* kamuya açık elektronik haberleşme hizmetlerini kullanan kişilerin haberleşme içeriği dışındaki bilgilerinin, iletişim trafiğinin, konum bilgileri gibi çeşitli kişisel verilerinin saklanabileceğini öngören 15 Mart 2006 tarihli ve 2006/24/EC sayılı "İletişim Trafik Verilerinin Saklanmasına Dair Direktif"[71] kabul edilmiştir. Ancak bu direktif, "ciddi suç" deyiminin çok geniş bir kavram olması ve içeriğinin net olmaması sebebiyle eleştirilmiştir. Ayrıca, Avrupa Birliği Adalet

---

[69] **Dülger**, s. 37.

[70] 2016/680 Sayılı Direktif'in (İngilizce tam başlığı, *Directive (EU) 2016/680 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 by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA*) İngilizce metnine şu uzantıdan ulaşabilirsiniz: https://eur-lex.europa.eu/eli/dir/2016/680/oj Erişim Tarihi: 13 Şubat 2020.

[71] 2006/24/EC Sayılı Direktif'in (İngilizce tam başlığı, *Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC*) İngilizce metnine şu uzantıdan ulaşabilirsiniz: http://data.europa.eu/eli/dir/2006/24/oj Erişim Tarihi: 13 Şubat 2020.

Divanı (ABAD), 8 Nisan 2014 tarihli kararında[72] direktifin korumak istediği menfaat ile uyguladığı yöntemler arasındaki ölçülülük ilkesinin aşılması, direktifin kötüye kullanılabilme olasılığına karşılık getirilen güvencelerin eksik olması sebepleriyle 2006/24/EC Sayılı Direktif'i geçersiz kılmıştır.

3.4.6. 45/2001 ve 2018/1725 Sayılı Avrupa Birliği Kurumları Veri Koruma Tüzükleri

AB'nin kurum ve organları tarafından yapılacak kişisel veri işleme faaliyetlerine ilişkin kuralların belirlenmesi amacıyla 18 Aralık 2000 tarihli ve 45/2001 sayılı Avrupa Birliği Kurumları Veri Koruma Tüzüğü[73] kabul edilmiştir. Tüzük, gerçek kişilerin kişisel verilerinin işlenmesi eksenindeki temel hak ve özgürlükleri ile mahremiyet haklarına topluluğun kurum ve organları tarafından saygı gösterildiğinin gözetimi amacıyla bağımsız bir denetim otoritesi olan Avrupa Veri Koruma Denetçisi'nin (*European Data Protection Supervisor*) kurulmasını öngörmüştür.

Bahsi geçen tüzük, 23 Ekim 2018 tarihli ve 2018/1725 sayılı Avrupa Birliği Kurumları Veri Koruma Tüzüğü'nün kabul edilmesiyle ilga edilmiştir[74]. 2018/1725 sayılı Tüzük ile AB kurum ve organlarının kişisel verileri işleme faaliyetleri 2018 yılında tam anlamıyla yürürlüğe giren Genel Veri Koruma Tüzüğü ile uyumlanmış, böylece AB veri koruma reformunun önemli bir aşamasının daha tamamlandığı

---

[72] ABAD'ın 8 Nisan 2014 tarihli, C-293/12 ve C-594/12 sayılı karara şu uzantıdan erişilebilir: https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX:62012CJ0293 Erişim Tarihi: 13 Şubat 2020.

[73] 45/2001 Sayılı Direktif'in (İngilizce tam başlığı, *Regulation (EC) No 45/2001 of the European Parliament and of the Council of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data*) İngilizce metnine şu uzantıdan ulaşabilirsiniz: https://eur-lex.europa.eu/eli/reg/2001/45/oj Erişim Tarihi: 15 Şubat 2020.

[74] 2018/1725 Sayılı Direktif'in (İngilizce tam başlığı, *Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC (Text with EEA relevance.)*) İngilizce metnine şu uzantıdan ulaşabilirsiniz: https://eur-lex.europa.eu/eli/reg/2018/1725/oj Erişim Tarihi: 15 Şubat 2020.

belirtilmelidir[75]. 2018/1725 sayılı Tüzük'te de mülga tüzükte belirtilen bağımsız denetim otoritesi (Avrupa Veri Koruma Denetçisi) varlığını korumaktadır.

3.4.7. 2016/679 Sayılı Avrupa Birliği Genel Veri Koruma Tüzüğü (GDPR)

Veri koruma hukukunu doğrudan etkileyen teknolojik gelişmelerin çok hızlı şekilde ilerlemesi AB veri koruma hukukunda yeni bir düzenleme yapılması ihtiyacını doğurmuştur. Ek olarak, yukarıda açıkladığımız üzere 95/46/EC Sayılı Direktif üye devletlerin mevzuatları arasında hedeflenen uyum yakalanamamış, üye devletler arasındaki veri koruması uygulamaları birbirinden farklılık göstermiştir. Bu sebeplerle, Direktif'in veri koruma hukukunda yaratamadığı hukuki yeknesaklığın sağlanması[76] ile uygulama birliğinin hayata geçirilmesi ve yeni ihtiyaçların karşılanması adına AB Parlamentosu ve Konseyi tarafından 27 Nisan 2016 ve 2016/679 sayılı Genel Veri Koruma Tüzüğü (*General Data Protection Regulation*, "GDPR") kabul edilmiştir[77].

4 Mayıs 2016 tarihli Avrupa Birliği Resmî Gazetesi'nde (*Official Journal of the European Union*) yayımlanan Tüzük, 99. maddesi uyarınca 25 Mayıs 2016 tarihinde yürürlüğe girmiş ancak aynı maddenin ikinci fıkrası gereği tüzük hükümlerinin uygulanmasına 25 Mayıs 2018'den itibaren başlanmıştır. Tüzüğün 94. maddesi uyarınca 95/46/EC sayılı Direktif, 25 Mayıs 2018 tarihinden itibaren geçerli olmak üzere ilga edilmiştir.

Avrupa Birliği'nin İşleyişi Hakkında Antlaşma'nın 288. maddesi uyarınca tüzükler üye devletler açısından genel uygulama alanına sahiptir ve tamamen bağlayıcıdır. Ayrıca tüzükler üye devletlerde doğrudan uygulanabilir olduklarından iç hukuka uyumun sağlanması için ayrıca bir hukuki düzenleme yapılmasına gerek bulunmamaktadır.

---

[75] **Dülger**, s. 38.
[76] **Başalp**, "Avrupa Birliği Veri Koruması Genel Regülasyonu'nun Temel Yenilikleri", s. 82.
[77] 2016/679 Genel Veri Koruma Tüzüğü'nün (İngilizce tam başlığı, *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)*) İngilizce metnine şu uzantıdan ulaşabilirsiniz: https://eur-lex.europa.eu/eli/reg/2016/679/oj Erişim Tarihi: 16 Şubat 2020. Bundan sonra "GDPR" veya "Tüzük" olarak anılacaktır.

Tüzüğün "Bölgesel Kapsam" başlıklı 3. maddesi incelendiğinde kapsamın 95/46/EC sayılı Direktif'e göre genişletildiği görülmektedir. Buna göre Tüzük; AB hukukuna bağlı olan kuruluşlara ek olarak, AB sınırları içerisindeki veri sahiplerine mal veya hizmet sunan ve AB içerisindeki veri sahiplerinin davranışlarını izleyen kuruluşlara da uygulanacaktır. Örneğin AB sınırları içerisinde de faaliyet gösteren Facebook, Amazon, Microsoft, Google gibi Amerikan şirketleri ile AB içerisindeki kişisel veri sahipleri arasında herhangi bir hukuki ihtilafın çıkması durumunda GDPR'ın uygulanacağını söyleyebiliriz. Nitekim Fransa, 2019 yılında Amerikan şirketi olan Google'a GDPR'ın aydınlatma yükümlülüğü, açık rıza ve şeffaflık ile ilgili hükümlerine aykırı faaliyetleri nedeniyle 50 milyon Euro tutarında para cezası kesmiştir[78].

Tüzükle getirilen yeniliklere ve başlıca değişikliklere aşağıdaki başlıklar altında kısaca değinilecektir:

- İlgili Kişinin Rızası: Tüzükle birlikte kişisel veri sahibinden alınması gereken açık rızaya ilişkin düzenlemeler detaylandırılmıştır. Bu konuda ilk göze çarpan yenilik; veri işleme faaliyetinin rızaya dayandığı durumlarda veri sorumlularının veri sahibinden bu rızayı aldığını ispat etme yükümlülüğü getirilmesidir (GDPR m. 7/1). Ayrıca kişisel veri sahibine verisinin işlenmesi için verdiği rızayı dilediği zaman geri çekebilmesi hakkı tanınmıştır (GDPR m. 7/3).
- Veriye Erişim Hakkı: Veri süjesine kişisel verisinin işlenip işlenmediğini öğrenme, eğer işleniyorsa bu verilere ilişkin kapsamlı bilgi edinme hakkı düzenlenmiştir (GDPR m. 15).
- Unutulma Hakkı: Veri süjesine kişisel verisini işleyen taraflardan bu verilerin silinmesini talep etme hakkı verilmiştir (GDPR m. 17)[79].

[78] CNIL ("Commission nationale de l'informatique et des libertés", İngilizcesi "National Commission on Informatics and Liberty") Fransız bağımsız idari otoritesinin Google'a kestiği idari para cezasına ilişkin İngilizce karar metnine şu uzantıdan ulaşabilirsiniz: https://www.cnil.fr/sites/default/files/atoms/files/san-2019-001.pdf Erişim Tarihi: 16 Şubat 2020.

[79] ABAD'ın 95/46/EC sayılı Direktif döneminde unutulma hakkına ilişkin verdiği 13 Mayıs 2014 tarihli Google kararının Türkçe çevirisi için bkz. **Mehmet Bedii Kaya**, "Avrupa Birliği Adalet Divanı'nın 13 Mayıs 2014 Tarihli Google Unutulma Hakkı Kararı (Karar Çevirisi)", 2015

- Veri Taşıma Hakkı: Veri süjesinin kendisine ait kişisel verilerini daha önce aktarmış olduğu veri sorumlusuna başvurarak bu kişisel verilerini yaygın kullanılan ve aletler tarafından okunabilen formatta almayı talep etme hakkı ve bu alınan verilerin veri süjesi tarafından başka bir veri sorumlusuna aktarma hakkı getirilmiştir (GDPR m. 20).
- Tasarıma Dayalı ve Varsayılan Ayarlarla Veri Koruma: Kişisel verilerin korunmasına ilişkin faaliyetlerin veri sorumluları tarafından veri işleme amaçlarının belirlendiği andan itibaren teknik ve idari tedbirlerin alınması gerektiği düzenlenmiştir (GDPR m. 25). "Varsayılan ayarlarla veri koruma" kavramı ise; veri işleme faaliyetinin amacı doğrultusunda işlenecek kişisel verilerin en yüksek gizlilik seviyesinde, amaca uygun olarak en az kişisel verinin işlenmesi gerektiğini ifade etmektedir[80].
- Kişisel Veri İhlali Bildirimi: Kişisel verilere ilişkin ihlallerin veri sorumluları tarafından 72 saatten geç olmamak üzere ilgili veri koruma otoritesine bildirilmesi, bu ihlallerin gerçek kişilerin temel hak ve özgürlükleri üzerinde yüksek risk yaratması durumunda ise bu durumun veri süjesine en kısa zaman içinde bildirilmesi gerektiği düzenlenmiştir (GDPR m. 33-34).
- Veri Koruma Görevlisi (*Data Protection Officer*): Veri sorumluları ve veri işleyenlerin veri işleme faaliyeti yapan (mahkemeler hariç) kamu kurumlarında, yüksek miktarda veri işleme faaliyetini işin doğası gereği düzenli ve sistematik şekilde gözetim faaliyeti gerçekleştirerek yapan kuruluşlarda, esas faaliyet konusu yüksek miktarda özel nitelikli kişisel verileri, ceza mahkumiyetine veya suça ilişkin verileri işlemek olan kuruluşlarda veri sorumluları ve veri işleyenler

(Çevrimiçi) https://www.mbkaya.com/hukuk/ab-unutulma-hakki-kararceviri.pdf Erişim Tarihi: 28 Nisan 2020.

[80] **Leyla Keser Berber**, Çevrimiçi Davranışsal Reklamcılık (Online Behavioral Advertising) Uygulamaları Özelinde Kişisel Verilerin Korunması, İstanbul 2014, s. 24; **Başalp**, "Avrupa Birliği Veri Koruması Genel Regülasyonu'nun Temel Yenilikleri", s. 92.

tarafından bir Veri Koruma Görevlisi atanması gerektiği düzenlenmiş, ayrıca bu görevlinin sahip olması gereken nitelikler ve görevlerine ilişkin ayrıntılı düzenlemeler getirilmiştir (GDPR m. 37 vd.).

- İdari Para Cezaları: Tüzük kişisel verilerin korunması alanında daha önce görülmemiş boyutlarda para cezaları düzenlemiştir. Buna göre GDPR kapsamında kişisel veri ihlali yapan kuruluşlara üst sınırı kuruluşun bir önceki yıla ait dünya çapındaki yıllık cirosunun %4'üne veya 20 milyon Euro'ya kadar idari para cezası kesilmesi düzenlenmiştir (GDPR m. 83).

4. KİŞİSEL VERİLERİN KORUNMASI ALANINDAKİ ULUSAL MEVZUAT

4.1. 1982 Anayasası

Kişisel verilerin korunmasına ilişkin bir hukuki düzenleme yapılması ihtiyacı ülkemizde de geçtiğimiz yıllarda giderek artmıştır. Ayrıca özellikle Avrupa Birliği'nin son yıllarda konuyla ilgili yaptığı çeşitli düzenlemeler, Türkiye'nin de bu konuda hukuki düzenlemeler yapmaya yönelik motivasyonunu arttırmıştır. Bu kapsamda Türkiye'de kişisel verilerin korunmasına ilişkin ilk hukuki düzenleme, günümüz itibariyle yürürlükte olmayan, "Telekomünikasyon Sektöründe Kişisel Bilgilerin İşlenmesi ve Gizliliğinin Korunması Hakkında Yönetmelik" ile 2004 yılında yapılmıştır[81]. Bu düzenlemeden sonra, çalışmamızın ayrı bir başlığı altında ele alacağımız, 5237 sayılı Türk Ceza Kanunu içinde çeşitli düzenlemeler yapılmıştır.

1982 Anayasası'nda kişisel verilerin korunması ile ilgili ilişkilendirilebilecek özel hayatın gizliliği, haberleşme hürriyeti, din ve vicdan hürriyeti, düşünce ve kanaat hürriyeti gibi çeşitli düzenlemeler[82] olsa da Anayasa'da kişisel verilerin korunmasına ilişkin doğrudan yapılan ilk düzenleme 12 Eylül 2010 tarihli

[81] **Taştan**, s. 23.
[82] **Şimşek**, s. 111.

referandum ile yapılmıştır[83]. Bu kapsamda "Özel Hayatın Gizliliği" başlıklı 20. Maddesine üçüncü bir ek fıkra eklenmiştir. İlgili hüküm aşağıdaki gibidir:

"*IV. Özel hayatın gizliliği ve korunması*

A. Özel hayatın gizliliği

Madde 20 – (1) Herkes, özel hayatına ve aile hayatına saygı gösterilmesini isteme hakkına sahiptir. Özel hayatın ve aile hayatının gizliliğine dokunulamaz. (Mülga üçüncü cümle: 3/10/2001- 4709/5 md.) (Değişik fıkra: 3/10/2001-4709/5 md.)

(2) Millî güvenlik, kamu düzeni, suç işlenmesinin önlenmesi, genel sağlık ve genel ahlâkın korunması veya başkalarının hak ve özgürlüklerinin korunması sebeplerinden biri veya birkaçına bağlı olarak, usulüne göre verilmiş hâkim kararı olmadıkça; yine bu sebeplere bağlı olarak gecikmesinde sakınca bulunan hallerde de kanunla yetkili kılınmış merciin yazılı emri bulunmadıkça; kimsenin üstü, özel kâğıtları ve eşyası aranamaz ve bunlara el konulamaz. Yetkili merciin kararı yirmidört saat içinde görevli hâkimin onayına sunulur. Hâkim, kararını el koymadan itibaren kırksekiz saat içinde açıklar; aksi halde, el koyma kendiliğinden kalkar.

(3) (Ek fıkra: 7/5/2010-5982/2 md.) 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 veriler, ancak kanunda öngörülen hallerde veya kişinin açık rızasıyla işlenebilir. Kişisel verilerin korunmasına ilişkin esas ve usuller kanunla düzenlenir."

Anayasa'daki düzenleme ile kişilere kendisi hakkında işlenen kişisel verilere erişme, bunlar hakkında bilgilendirilme, bu verilerin silinmesini veya

[83] Türkiye Cumhuriyeti Anayasasının Bazı Maddelerinde Değişiklik Yapılması Hakkında Kanun'un yayımlandığı 13 Mayıs 2010 tarihli ve 27580 sayılı Resmî Gazete'ye şu uzantıdan ulaşabilirsiniz: https://www.resmigazete.gov.tr/eskiler/2010/05/20100513-1.htm Erişim Tarihi: 17 Şubat 2020. Ayrıca bkz: **Sultan Tahmazoğlu Üzeltürk**, Kişisel Verilerin Korunması Hakkında Anayasa Değişikliği, Legal Hukuk Dergisi, S. 93, s. 3151-3156, 2010, s. 3151.

düzeltilmesini talep etme, bu verilerin toplanma amaçları doğrultusunda işlenip işlenmediğini öğrenme hakları verilmiştir. Ek olarak kişisel verilerin yalnızca kanunda bu konuda bir düzenleme olması veya kişisel verinin sahibi tarafından verilmiş bir açık rızanın bulunması halinde işlenebileceği düzenlenmiştir. Ayrıca kişisel verilerin korunmasına ilişkin düzenlemelerin kanunla yapılacağı belirtilmiş, böylece bu hakla ilgili keyfi düzenlemeler yapılmasının önüne geçilmeye çalışılmıştır.

Yukarıda alıntılanan maddenin üçüncü fıkrası ile birlikte kişisel verilerin korunması hukuku Türkiye'de anayasal bir hak olarak düzenlenmiş ve teminat altına alınmıştır[84].

4.2. 6698 Sayılı Kişisel Verilerin Korunması Kanunu

Ülkemizde kişisel verilerin korunması alanında kanun yapma çalışmalarının 1989 yılında başladığı bilinmekte ise de bu konuda bir kanun hazırlamak üzere ilk komisyon 13 Eylül 1995 tarihinde kurulmuştur[85]. Komisyon çalışmaları çeşitli sebeplerle tamamlanamamış ve 2000 yılında yeni bir komisyon oluşturulmuştur. Bu komisyon tarafından hazırlanan ve 2003 yılında açıklanan Kişisel Verilerin Korunması Kanunu Tasarısı da yasalaşamamıştır[86]. 2008 ve 2014 yıllarında TBMM'ye sevk kişisel verilerin korunmasına ilişkin hazırlanan kanun tasarıları çeşitli sebeplerle hükümsüz kalmıştır. Nihayet bugün yürürlükte olan 6698 sayılı Kişisel Verilerin Korunması Kanunu'nun komisyon görüşmeleri 12 Şubat 2016 tarihinde tamamlanmış, kanun tasarısı 24 Mart 2016 tarihinde TBMM tarafından kabul edilmiş, kabul edilen bu kanun 29677 sayılı ve 7 Nisan 2016 tarihli Resmî Gazete'de yayımlanmıştır[87]. Kanun'un "Yürürlük" başlıklı 32. maddesi uyarınca Kanun'un 8., 9., 11., 13., 14., 15., 16., 17. ve 18. maddeleri yayımı tarihinden altı ay sonra, diğer maddeleri ise yayımı tarihinde yürürlüğe gireceği düzenlenmiştir. Çalışmamızın yazılma tarihi itibariyle Kanun tüm hükümleriyle yürürlüktedir.

---

[84] **Küzeci**, s. 288.
[85] **Küzeci**, s. 311.
[86] **Başalp**, s. 107-108.
[87] 7 Nisan 2016 Tarihli ve 29677 Sayılı Resmî Gazete, https://www.resmigazete.gov.tr/eskiler/2016/04/20160407.htm Erişim Tarihi: 17 Şubat 2020.

Kanun'un getiriliş sebebi olarak Genel Gerekçe incelendiğinde aşağıdaki sebepler öne çıkmaktadır:

- 2010 Anayasa değişikliği ile Anayasa'nın 20. maddesinin üçüncü fıkrası uyarınca kişisel verilerin korunması temel bir insan hakkı olarak düzenlenmesi ve kişisel verilerin korunmasına ilişkin usul ve esasları göstermek üzere bir kanun çıkarılması gerekliliği,
- 5237 sayılı TCK'nın 135 ila 140. maddeleri arasında belirlenen suç tiplerinde belirtilen fiilin hukuka aykırılığının ne zaman gerçekleştiğinin belirlenebilmesi noktasında özel bir kanuni düzenleme bulunmaması,
- AB üyelik sürecindeki müzakere fasıllarından dördünün, direkt olarak kişisel verilere ilişkin olması, bu fasıllarla ilgili sürecin ilerleyebilmesi için ülkemizde kişisel verilerin korunmasına ilişkin temel bir kanunun hazırlanması gerekliliği,
- Ülkemizin emniyet ve yargı teşkilatları ile AB'deki EUROPOL (Avrupa Polis Teşkilatı) ve EUROJUST (AB üye devletleri arasında yargı teşkilatının cezai işlere ilişkin iş birliği faaliyetini yürüten kurum) arasında ülkemizde kişisel verilerin korunmasına ilişkin kanuni bir düzenleme olmaması sebebiyle veri paylaşımı yapılamıyor olması,
- Ülkemizdeki sağlık kuruluşlarında, herhangi bir kanuni düzenleme olmamasına ve yeterli güvenlik tedbirlerinin alınmamasına rağmen, çok sayıda özel nitelikli kişisel verinin tutulması, bu verilerin yetkisiz kişilerce ifşa edilmesi ve bu uygulamaların AİHM tarafından özel hayatın gizliliğine müdahale olarak yorumlanması ve ülkemiz aleyhine birçok dosyada ihlal kararı vermesi,
- 64. Hükümet'in 2016 yılına ilişkin Eylem Planında üç ay zarfında yapılacak reformlar arasında kişisel verilerin korunması hakkındaki yasal düzenlemelerin gerçekleştirileceğinin bulunması,
- Yabancı sermayenin ülkemizde yatırım yapması ve ülkemizdeki yatırımlarını etkili bir şekilde yönetebilmesi için ihtiyaç duyduğu veri

aktarımının, ülkemizde bu konuda bir kanuni düzenleme olmaması sebebiyle gerçekleştirilememesi ve bu durumun yabancı sermayenin ülkemizde yatırım yapması açısından caydırıcı bir etken olması.

Kanun'un hazırlık aşamasında AB'nin hazırladığı 95/46/EC sayılı Direktif'ten ciddi ölçüde yararlanılmıştır, bu sebeple iki düzenleme arasında büyük oranda benzerlik bulunmaktadır.

Kanun içeriğinde; genel ve özel nitelikli kişisel verilerin işlenme şartlarına, kişisel verilerin silinmesi, yok edilmesi veya anonim hâle getirilmesine, yurt içinde ve yurt dışına aktarılmasına, veri sorumlularının yükümlülükleri ve ilgili kişinin haklarına, veri güvenliğine ilişkin yükümlülüklere, veri sorumlularına başvuru ve Kişisel Verileri Koruma Kuruluna yapılacak şikayet usullerine, Kanun kapsamında halihazırda kurulmuş olan Kişisel Verileri Koruma Kurumu'nun teşkilatı ve görevlerine ilişkin bilgilere, Kanun'un ihlali halinde uygulanacak idari para cezalarına ilişkin çeşitli düzenlemelere yer verilmiştir[88].

4.3. 5237 Sayılı Türk Ceza Kanunu

Kişisel verilerin korunması hakkının bireyin temel bir hakkı olduğuna daha önce değinmiştik. Bu hakkın korunmasını temin etmek adına kanun koyucu tarafından bazı suç tipleri yaratılmıştır. Kişisel verilerin korunmasına ilişkin suç tiplerine 26 Eylül 2004 tarihli ve 5237 sayılı Türk Ceza Kanunu'nun (TCK) özel hükümlerinin düzenlendiği ikinci kitabının "Kişilere Karşı Suçlar" başlıklı ikinci kısmının "Özel Hayata ve Hayatın Gizli Alanına Karşı Suçlar" başlıklı dokuzuncu bölümünde yer verilmiştir[89].

TCK'nın 135. maddesinde "kişisel verilerin kaydedilmesi suçu", 136. maddesinde "verileri hukuka aykırı olarak verme veya ele geçirme suçu", 137.

---

[88] Kişisel verilerin korunması hukuku alanındaki ulusal ve uluslararası mevzuat, içtihat ve bibliyografya derlemesi için bkz. **Mehmet Bedii Kaya, Furkan Güven Taştan**, Kişisel Veri Koruma Hukuku (Mevzuat - İçtihat - Bibliyografya), On İki Levha Yayınları, 2. Baskı İstanbul 2019, (Çevrimiçi) https://www.mbkaya.com/hukuk/veri-koruma-hukuku.pdf Erişim Tarihi: 20 Şubat 2020.

[89] 5237 sayılı Türk Ceza Kanunu'nun metnine şu uzantıdan ulaşabilirsiniz: https://www.resmigazete.gov.tr/eskiler/2016/04/20160407.htm Erişim Tarihi: 20 Şubat 2020.

maddesinde sayılan bu suçların "nitelikli halleri", 138. maddesinde "verileri yok etmeme" suçu, 140. maddesinde ise kişisel verilere ilişkin suçların bir tüzel kişilik tarafından işlenmesi durumunda bu tüzel kişiler hakkında güvenlik tedbirlerinin uygulanacağı hususu düzenlenmiştir.

6698 sayılı Kanun'un "Suçlar ve Kabahatler" başlıklı beşinci bölümünün "Suçlar" başlıklı 17. maddesinin birinci fıkrasında kişisel verilere ilişkin suçlara TCK'nın 135 ila 140. maddelerinin uygulanacağı belirtilmiş ve böylece 6698 sayılı Kanun ile 5237 sayılı TCK arasında direkt bir ilişkilendirme yapılmıştır[90].

[90] **Dülger**, s. 537.

İKİNCİ BÖLÜM
KİŞİSEL VERİLERİN KORUNMASI HUKUKUNUN TEMEL KAVRAMLARI VE VERİ SORUMLUSUNUN GENEL YÜKÜMLÜLÜKLERİ

1. KİŞİSEL VERİLERİN KORUNMASI HUKUKUNUN TEMEL KAVRAMLARI

Bu başlık altında kişisel verilerin korunması hukukunun ulusal ve uluslararası düzenlemelerdeki temel kavramları ele alınacaktır. Açıklamalarımızı yaparken Kanundaki düzenlemelerinin üzerinde daha ayrıntılı şekilde duracağız ve gerekli gördüğümüz yerlerde konuyu GDPR ve 95/46/EC Sayılı Direktif'teki düzenlemelerle karşılaştırmalı olarak ele alacağız.

1.1. Kişisel Veri

Kişisel verinin tanımına ilişkin keskin sınırları olan bir tanım bulunmasa da hem ulusal hem de uluslararası mevzuatta yapılan tanımlamalar ışığında; kimliği belirli ya da belirlenebilir nitelikteki kişilere ait her türlü bilginin kişisel veri olduğu söylenebilir. Bu tanımdan yola çıkarak ortada bir kişisel veriden bahsedebilmemiz için asgari iki gereklilik bulunmaktadır: Bunlardan birincisi bir kişiye ilişkin bilginin bulunması, ikincisi ise bu bilginin ya kimliği belirli bir kişiye ait olması ya da kişinin kimliğinin belirlenebilir olmasıdır.

OECD'nin yayımladığı Rehber İlkeler'de ve AK'nin yayımladığı 108 Sayılı Sözleşme'de birbiriyle aynı doğrultuda düzenleme yapılarak; kişisel veri, kimliği belirli ya da belirlenebilir nitelikteki kişilere ait her türlü bilgi olarak tanımlanmıştır. AB'nin 95/46/EC Sayılı Mülga Direktifi ile yürürlükteki GDPR'da kişisel veri, kimliği belirli ya da belirlenebilir nitelikteki gerçek kişilere (ilgili kişi veya veri süjesi) ait her türlü bilgi olarak tanımlanmıştır. Bu tanıma ek olarak mülga Direktif ve GDPR'da belirlenebilir nitelikteki gerçek kişiye ilişkin ek neredeyse birbirleri ile aynı bir tanımlama da yapılmıştır. Mülga Direktif ile GDPR'daki düzenlemenin OECD Rehber İlkeleri ile 108 Sayılı Sözleşme'den temel farkı;

OECD Rehber İlkeleri ile 108 Sayılı Sözleşme'deki tanım içerisinde kullanılan "kişi" kelimesi yerine, Direktif ile GDPR'daki tanım içerisinde "gerçek kişi" tanımı yapılmıştır. Dolayısıyla, Direktif ve GDPR'da tüzel kişiler kapsam dışında tutulmuştur.

6698 sayılı Kanunda da güncel uluslararası mevzuatlara uyumlu şekilde bir kişisel veri tanımlaması yapılmıştır. Kanunun "Tanımlar" başlıklı 3. maddesinin 1. fıkrasının d bendinde kişisel veri, "kimliği belirli veya belirlenebilir gerçek kişiye ilişkin her türlü bilgi" olarak tanımlanmıştır. Direktif ve GDPR'da olduğu gibi Kanundaki kişisel veri tanımında da tüzel kişiler kapsam dışında bırakılmıştır. Kanunda kişisel verilerin neler olduğuna ilişkin sınırlı sayıda sayım yapılmamıştır. Kanunun gerekçesinde kişisel verilerin yalnızca ad, soyad, doğum tarihi, doğum yeri gibi direkt olarak kişiyi işaret eden bilgileri değil, kişinin fiziki, ailevi, ekonomik, sosyal ve diğer özelliklerine ilişkin bilgileri de kapsayacağı belirtilmiştir. Ek olarak gerekçede; "*Bir kişinin belirli veya belirlenebilir olması, mevcut verilerin herhangi bir şekilde bir gerçek kişiyle ilişkilendirilmesi suretiyle, o kişinin tanımlanabilir hale getirilmesini ifade eder. Yani verilerin; kişinin fiziksel, ekonomik, kültürel, sosyal veya psikolojik kimliğini ifade eden somut bir içerik taşıması veya kimlik, vergi, sigorta numarası gibi herhangi bir kayıtla ilişkilendirilmesi sonucunda kişinin belirlenmesini sağlayan tüm halleri kapsar. İsim, telefon numarası, motorlu taşıt plakası, sosyal güvenlik numarası, pasaport numarası, özgeçmiş, resim, görüntü ve ses kayıtları, parmak izleri, genetik bilgiler gibi veriler dolaylı da olsa kişiyi belirlenebilir kılabilme özellikleri nedeniyle kişisel verilerdir.*" şeklinde yapılan açıklamayla kişisel kavramının ne kadar geniş bir perspektiften ele alınması gerektiği anlaşılmaktadır.

Kişinin belirlenebilir olmasına ilişkin Kanunun gerekçesine ek olarak, GDPR'ın başlangıç bölümünün 26. maddesinde de yol gösterici düzenlemeler vardır. Buna göre bir kişinin belirlenebilir olmasındaki ölçüt, yardımcı ve makul vasıtaların kullanılmasıyla ilgili kişinin kimliğinin ortaya çıkarılabilir olup olmamasındadır. Kişinin belirlenebilir olması, o kişinin henüz diğer insanlardan ayırt edilmiş olmamasıyla birlikte, yardımcı ve makul vasıtaların yardımıyla ayırt edilmesinin mümkün olduğunu ifade eder. Kişinin yaşı, cinsiyeti, mesleği, mezun

olduğu okul, anne adı gibi veriler, kişinin belirlenmesinde yardımcı olan bilgilerdir, zira bu bilgiler tek başlarınayken neredeyse çoğu zaman ilgili kişiyi doğrudan işaret etmezler.

Tüm bu birbirine benzer tanımlamalara bakıldığında çok geniş kapsamlı bir tanımı olan kişisel verinin aşağıda sayılı üç temel unsuru bulunmaktadır[91]:

- Bir verinin bulunması
- Verinin kişiyi belirli veya belirlenebilir kılması
- Bilginin, kimliği belirli veya belirlenebilir bir gerçek kişiye ilişkin olması

Kişisel veri, kişiye ait her türlü bilgileri kapsamakta olduğu için kişisel verilerin kişinin yalnızca özel hayatına ilişkin verilerden ibaret olmadığını veya verinin öznel, nesnel, doğru veya yanlış olmadığının kişisel verinin varlığının tespitinde herhangi bir önem arz etmediğini belirtmek isteriz.

1.2. Özel Nitelikli (Hassas) Kişisel Veriler

Kişisel verilerin korunmasına ilişkin yapılan düzenlemeler incelendiğinde bazı kişisel verilerin diğerlerine göre daha "*hassas*" nitelikte olduğu belirtilmiş ve bu veri türüne ilişkin özel düzenlemeler getirilmiştir. Avrupa Konseyi'nin 108 Sayılı Sözleşmesi, BM'nin Bilgisayara Geçirilmiş Kişisel Veri Dosyalarına İlişkin Rehber İlkeleri, 95/46/EC Sayılı Direktif ve GDPR incelendiğinde ayrı bir düzenleme yoluna gidilen özel nitelikli kişisel verileri görmekteyiz. Böyle bir ayrıma gidilmesinde özel (hassas) nitelikli kişisel verilerin diğer verilere oranla diğer kişiler tarafında öğrenilmesi veya kötüye kullanılması durumunda ilgili kişiye daha büyük bir zarar verebilecek olması veya ilgili kişinin ayrımcılığa maruz kalabilecek olması[92] gibi haklı kaygılar sebep olmuştur.

---

[91] Kişisel veri kavramına ilişkin daha ayrıntılı bir değerlendirme için bkz. **Article 29 Data Protection Working Party**, Opinion 4/2007 on the Concept of Personal Data, 20 Haziran 2007, 01248/07/EN, WP 136, (Çevrimiçi) https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2007/wp136_en.pdf Erişim Tarihi: 22 Şubat 2020.

[92] **Başalp**, s. 43; **Akgül**, s. 13.

Kanunun 6. maddesinde tanımı ve işlenme şartları düzenlenen özel nitelikli kişisel veri türleri aşağıdaki gibidir:

- "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
- Biyometrik ve genetik verileri"

Sayılan özel nitelikli kişisel veri türlerinin birçoğunun ne ifade ettiği kavramın kendisinden anlaşılmakta ise de biyometrik verilerin neyi ifade ettiğini açıklamak yerinde olacaktır. Kanunda biyometrik verilerin tanımına ilişkin bir tanımlama bulunmamaktadır. GDPR'ın m. 4/14 hükmü uyarınca biyometrik veri; özel teknik yöntemlerle kişiyi ayırt edici şekilde belirlemeye yarayan kişinin fiziksel, psikolojik veya karakterine ilişkin özellikleridir. Bu tanım doğrultusunda parmak izi, retina modeli, yüz modeli, imza modeli, yürüyüş şekli kişinin biyometrik verilerindendir.

Ses ve görüntü verilerinin hangi durumlarda biyometrik veri olarak değerlendirileceği hususunu ayrıca incelemek gerekmektedir. Kurulun internet sitesinde 7 Nisan 2020 tarihinde yayınlanan Uzaktan Eğitim Platformları Hakkında Kamuoyu Duyurusu[93] uyarınca; "*(...) Uzaktan eğitim platformlarında, öğrencilerin ad ve soyadları gibi kişisel verileri ile* ***ses ve görüntü gibi biyometrik veri kapsamında değerlendirilebilecek bazı özel nitelikli kişisel verilerinin*** *işlendiği görülmektedir. (...)*" ifadesine yer verilmiştir.

[93] Kişisel Verileri Koruma Kurulu'nun 7 Nisan 2020 yayınlanma tarihli ve "Uzaktan Eğitim Platformları Hakkında Kamuoyu Duyurusu" metnine şu uzantıdan ulaşabilirsiniz: https://www.kvkk.gov.tr/Icerik/6723/Uzaktan-Egitim-Platformlari-Hakkinda-Kamuoyu-Duyurusu Erişim Tarihi: 05.06.2020.

Ancak ses ve görüntü verilerinin yalnızca belirli bazı durumlarda biyometrik veri kategorisinde (özel nitelikli kişisel veri) sayılabileceği kanaatindeyiz. Ses ve görüntü verileri, biyometrik yöntemler kullanılarak ilgili kişinin kimliğini saptama, teyit etme, tanımlama veya doğrulama gibi işlemlere tabi tutulduğu durumlarda; bu ses ve görüntü verilerinin özel nitelikli kişisel veri olarak kabul edilmesi gerekecektir[94]. Diğer bir ifadeyle ses ve görüntü verilerinin ilgili kişiyi belirli şekilde kimliğinin tespit edilmesine imkân veren biyometrik yöntemler aracılığıyla işlenmemesi durumunda bu verilerin biyometrik veri olarak kabul edilmesi ve özel nitelikli kişisel veri hükümlerine tabi olmaması gerektiği kanaatindeyiz.

Kanundaki özel nitelikli kişisel veri türleri yasa koyucu tarafından sınırlı sayıda sayılmıştır ve dolayısıyla kıyas yoluyla genişletilmesi mümkün değildir.

Yukarıda sayılan özel nitelikli kişisel veriler üzerinde yapılacak veri işleme faaliyetlerine ilişkin Kanunda öngörülen kurallar, özel nitelikli olmayan verilere ilişkin veri işleme kurallarından ciddi farklılıklar göstermektedir. Bunun yanı sıra özel nitelikte kişisel verilerin tabi olduğu işleme kuralları da ilgili hükmün içinde farklılaşmaktadır. Sağlık verileri ve diğer özel nitelikli veriler özelinde işleme kuralları bakımından hükmün dikkatle incelenmesi gerekmektedir. Bu amaçla ilgili farklılıklar ileride "Kişisel Verilerin İşlenme Şartları" başlıklı bölüm altında ele alınacaktır.

1.3. Veri Sorumlusu

Veri sorumlusu (*data controller*) kavramı Kanuna göre "*kişisel verilerin işleme amaçlarını ve vasıtalarını belirleyen, veri kayıt sisteminin kurulmasından ve yönetilmesinden sorumlu olan gerçek veya tüzel kişi*" olarak tanımlanmıştır. Tanımdaki düzenleme ışığında gerçek kişilerin dışında, ticaret şirketleri, dernekler, vakıflar, kamu kurumları gibi tüzel kişiliği bulunan diğer kuruluşların da veri sorumlusu olmaları mümkündür.

---

[94] Aynı görüşte bkz. **Mücahit Ünal**, "Ses ve Görüntü Verilerinin Paylaşılmasının Kişisel Verilerin Korunması Kanunu Açısından Değerlendirilmesi", Lexpera Blog, 02.06.2020, (Çevrimiçi) https://blog.lexpera.com.tr/ses-ve-goruntu-verilerinin-paylasilmasinin-kisisel-verilerin-korunmasi-kanunu-acisindan-degerlendirilmesi/ Erişim Tarihi: 05.06.2020.

Kişisel Verileri Koruma Kurumu'nun yayınladığı "Veri Sorumlusu ve Veri İşleyen[95]" isimli rehbere göre veri sorumlusunun kim olduğu tespit edilirken aşağıdaki konulara kimin karar verdiğine dikkat edilmelidir:

- Kişisel verilerin işlenip işlenmeyeceği
- Kişisel verilerin işlenme amacı ve toplanma yöntemi
- Hangi tür kişisel verilerin işleneceği
- Kimlerin kişisel verilerinin işleneceği
- Kişisel verilerin üçüncü kişilere transfer edilip edilmeyeceği
- Verilerin ne kadar süreyle saklanacağı
- Kişisel verileri silme, yok etme ve anonim hale getirme faaliyetlerinden hangilerinin uygulanacağı

Yukarıda belirtilen konularda karar yetkisi bulunan kişi veri sorumlusudur. Zira kişisel verinin işlenip işlenmeyeceğinden başlayıp, verileri silme, yok etme ve anonim hale getirme işlemlerine kadar kişisel verilere ilişkin tüm konularda karar verme yetkisine sahiptir. Diğer bir ifadeyle veri sorumlusunu belirlerken kişisel verilerin üzerindeki genel kontrol ve karar verme yetkisinin kimde olduğu konusu önem arz etmektedir.

Veri işleme faaliyetinin bir tüzel kişilik tarafından yapılması durumunda burada veri sorumlusu tüzel kişiliğin kendisi olacaktır. Diğer bir ifadeyle veri işleme faaliyetini tüzel kişiliğin içinde yapan gerçek kişilerin veya departmanların (örneğin insan kaynakları departmanı müdürünün veya herhangi bir beyaz yakalı çalışanın) Kanun kapsamında veri sorumlusu olmaları veya anonim şirketin yönetim kurulu üyelerinden bir kişinin veri sorumlusu olarak seçilmesi mümkün değildir. Kanun içeriğindeki veri sorumlusuna ilişkin yükümlülükler tüzel kişiliğin üzerinde doğacaktır. Bu yükümlülüklerin tüzel kişilik içerisinde yerine getirilmesinden ise tüzel kişiliği temsil ve ilzama yetkili organlar ya da kişiler olacaktır.

---

[95] Kişisel Verileri Koruma Kurumu'nun yayınladığı "Veri Sorumlusu ve Veri İşleyen" isimli rehbere şu uzantıdan ulaşabilirsiniz: metnine şu uzantıdan ulaşabilirsiniz: https://www.kvkk.gov.tr/SharedFolderServer/CMSFiles/f63e88cd-e060-4424-b4b5-f6413c602060.pdf Erişim Tarihi: 24 Şubat 2020.

Tüzel kişiliği bulunan bir anonim şirket veya üniversite veri sorumlusu olabilecekken; avukatlar, mali müşavirler, noterler belirli bir mesleğin icra edilmesi çerçevesinde diğer şahıslara verdikleri hizmet sırasında kendi meslek kurallarının gerektirdiği şekilde işledikleri veriler bakımından veri sorumlusu sayılmaktadırlar. Zira bu meslek grupları her ne kadar müvekkil, mükellef veya müşterilerinden aldıkları talimatlar doğrultusunda hareket ettikleri düşünülse de mensubu oldukları meslek grubunun kanunları uyarınca gerekli olduğunda edindikleri bu kişisel verileri ilgili kurum ve kuruluşlara açıklamak gibi çeşitli yükümlülükleri bulunmaktadır. Bu durum da bu meslek mensuplarına kişisel veriler üzerinde yetki ve kontrol sahibi olduklarını göstermekte ve onları veri sorumlusu yapmaktadırlar[96]. Bu meslek gruplarının tüzel kişiliği bulunmadığından belirli bir noterlik için noterin kendisi, hukuk bürosunda avukatın kendisi, muhasebe bürosunda muhasebecinin kendisi olan gerçek kişiler veri sorumlularıdır[97].

95/46/EC Sayılı Direktif uyarınca oluşturulmuş ve Avrupa Birliği'nin ulusal veri koruma otoritelerini temsil eden ve bağımsız çalışan kilit danışma organı olan ve 25 Mayıs 2018 tarihi itibariyle yerine geçen Avrupa Veri Koruma Kurulu (European Data Protection Board) ile faaliyetlerine son verilen Madde 29 Çalışma Grubu (Article 29 Working Party[98]) tarafından veri sorumlusu kavramına ilişkin örneklerle birlikte detaylı bir inceleme yapılmıştır[99]. Bu kapsamda örneğin; bir şirketin yönetim kurulu üyesinin, şirket tarafından bu doğrultuda bir karar alınmamasına rağmen çalışanları gizli şekilde kamera vasıtasıyla izlemesi

---

[96] **Dülger**, s. 120.

[97] Kurulun 02.04.2018 tarihli ve 2018/32 sayılı kararı uyarınca avukatların, noterlerin, serbest mali müşavirlerin ve muhasebecilerin veri sorumlusu olduğu açıkça belirtilmiştir. Esasen Veri Sorumluları Sicili'ne kayıt olma yükümlülüğünden istisna tutulan meslek gruplarının belirtildiği bu karar bazı meslek gruplarının açıkça veri sorumlusu olduğunun belirtilmesi açısından önem arz etmektedir. Kararın metnine şu uzantıdan ulaşabilirsiniz: https://www.kvkk.gov.tr/Icerik/4233/2018-32 Erişim Tarihi: 24 Şubat 2020.

[98] Bundan sonra "Working Party" olarak anılacaktır.

[99] **Article 29 Data Protection Working Party**, Opinion 1/2010 on the Concepts of "Controller" and "Processor", 16 Şubat 2010, 00264/10/EN, WP 169, (Çevrimiçi) https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2010/wp169_en.pdf , Erişim Tarihi: 24 Şubat 2020.

durumunda şirketin veri sorumlusu olmasından hareketle olası bir uyuşmazlıkta şirketin sorumluluğu gündeme gelecektir[100].

1.4. Veri İşleyen

Veri işleyen kavramı Kanunda; "veri sorumlusunun verdiği yetkiye dayanarak onun adına kişisel verileri işleyen gerçek veya tüzel kişi" olarak tanımlanmıştır. GDPR'daki veri işleyen (*processor*) kavramı ise; "veri sorumlusu (*controller*) adına kişisel verileri işleyen gerçek veya tüzel kişi, kamu kurum veya kuruluşu ya da diğer herhangi bir kuruluş" olarak tanımlanmıştır[101]. Yani veri sorumlularından ayrı bir tüzel veya gerçek kişiliği bulunan veri işleyenler, veri sorumlusundan aldıkları talimatlarla veri işleme faaliyetini yürütmektedir.

Kanunun 3. maddesinin gerekçesinde bahsedildiği gibi bir gerçek veya tüzel kişi aynı anda hem veri sorumlusu hem de veri işleyen olabilir. Örneğin tüzel kişiliği bulunan bir ticaret şirketinin başka bir şirketten çağrı merkezi hizmeti satın almak üzere sözleşme yapması halinde böyle bir durum oluşacaktır. Bu örnekte çağrı merkezi hizmeti veren şirket hizmet sunduğu şirketin talimatlarıyla ve o şirket adına hareket ederek kişisel veri işleme faaliyetini yerine getirir[102]. Bu kapsamda veri işleyen konumunda olacaktır. Oysa çağrı merkezi hizmet sunan şirketin kendi çalıştırdığı personelle ilgili tuttuğu özlük dosyaları bakımından ise hukuki statüsü veri sorumlusuna karşılık gelecektir. Aynı şekilde bir bulut depolama hizmeti veren şirket kendi çalışanlarıyla ilgili kişisel verileri işlerken veri sorumlusu olacakken, hizmet sunduğu şirketlerin verilerini depolarken veri işleyen olacaktır.

Kişisel Verileri Koruma Kurumu'nun yayınladığı "Veri Sorumlusu ve Veri İşleyen Rehberi" [103] isimli belgede veri sorumlularının yapacakları kişisel veri işleme sözleşmesi ile;

---

[100] **Working Party**, Opinion 1/2010 on the Concepts of "Controller" and "Processor", s. 17.
[101] Veri işleyen kavramı hakkında daha detaylı açıklamalar için lütfen bkz. **Working Party**, Opinion 1/2010 on the Concepts of "Controller" and "Processor", Erişim Tarihi: 24 Şubat 2020.
[102] **Working Party**, Opinion 1/2010 on the Concepts of "Controller" and "Processor", s. 28.
[103] Veri Sorumlusu ve Veri İşleyen Rehberi" isimli belgeye şu bağlantı üzerinden erişebilirsiniz: https://www.kvkk.gov.tr/SharedFolderServer/CMSFiles/f63e88cd-e060-4424-b4b5-f6413c602060.pdf Erişim Tarihi: 24 Şubat 2020.

- "Kişisel verilerin toplanması için hangi bilgi teknolojileri sistemlerinin veya diğer metotların kullanılacağı,
- Kişisel verilerin hangi yöntemle saklanacağı,
- Kişisel verilerin korunması için alınacak güvenlik önlemlerinin detayları,
- Kişisel verilerin aktarımının hangi yöntemle yapılacağı,
- Kişisel verilerin saklanmasına ilişkin sürelerin doğru uygulanabilmesi için kullanılacak metot,
- Kişisel verilerin silinmesi, yok edilmesi ve anonim hale getirilmesi yöntemi"

gibi hususlarda karar verme yetkisini veri işleyene bırakabileceğinden bahsedilmiştir.

Veri sorumlusunu veri işleyenden ayıran temel nokta; veri işleyenin veri sorumlusu adına hareket etmesi, veri işleme faaliyetinden herhangi bir çıkarı olmaması ve veri sorumlusundan aldığı talimatlar doğrultusunda veri işleme faaliyetini gerçekleştirmesidir.

1.5. Açık Rıza

1.5.1. Genel Olarak

Kişisel verileri işlenen birey, kendi verilerinin işlenme süreçlerine aktif şekilde katılma ve veri işleme faaliyetlerinin ne şekilde ilerleyeceği hususunda söz alma haklarına sahiptir[104]. Kişisel verilerin korunması hukukunun en önemli kavramlarından biri olan açık rıza kavramı kişisel verilerin işlenmesine ilişkin bir hukuka uygunluk sebebidir. İlgili kişi tarafından açık rıza beyanında bulunulması, ilgili kişiye veri işleme sürecine doğrudan dahil olma fırsatı vermektedir. İlgili kişiye kişisel verileri üzerinde bir denetim tesis etmesine imkân veren rıza kavramı, kişisel verilerin geleceğini tayin etme hakkı (*informational self-determination*) düşüncesinin de bir yansımasıdır[105]. Ayrıca 12 Eylül 2010 tarihinde yapılan

[104] **Ozan Selek**, "Genel Veri Koruma Tüzüğü Işığında Kişisel Verilerin İşlenmesinde Rıza Açıklaması", DergiPark/Dokuz Eylül Üniversitesi Hukuk Fakültesi Dergisi, C. 21, S. 2, s. 911-951, 2019, s. 915.
[105] **Küzeci**, s. 238.

referandum ile Anayasanın 20. Maddesine eklenen 3. fıkra uyarınca; "*kişisel verilerin yalnızca kanunda öngörülen hallerde veya kişinin açık rızasıyla işlenebileceği*" hususu düzenlenmiştir.

Açık rıza kavramı Kanunun 3. maddesinde; "*belirli bir konuya ilişkin, bilgilendirilmeye dayanan ve özgür iradeyle açıklanan rıza*" olarak tanımlanmıştır. Kanunda genel veya özel nitelikli kişisel verilerin işlenebilmesi, bu verilerin yurtiçinde üçüncü kişilere veya yurtdışına aktarılabilmesi için, Kanunda öngörülen istisnalar dışında, açık rızanın varlığı aranmaktadır.

Rıza kavramı 95/46/EC Sayılı Direktifin 2. maddesinde "ilgili kişinin (veri süjesinin) rızası" terimiyle ifade edilmiş ve "*kendisiyle ilgili kişisel verilerin işlenmesi için ilgili kişinin kabulüne işaret eden, özgürce ve bilgilendirme yapıldıktan sonra alınan rıza*" olarak tanımlanmıştır. Direktifte kişisel veriler ile özel nitelikli kişisel verilerin işlenmesi için gereken rızanın içeriğinde ayrıma gidilmiş ve Direktifin "Özel nitelikli kişisel verilerin işlenmesi" başlıklı 8. Maddesinde bu türdeki verilerin işlenmesi için ilgili kişi (*data subject*) tarafından açık rıza (*explicit consent*) verilmesi gerektiği düzenlenmiştir.

Kanun ile Direktifteki tanımın karşılaştırılmasından hareketle Kanundaki açık rıza kavramının Direktife çok benzer şekilde düzenlendiğini söylemek mümkündür. Nitekim Kanunun açık rıza kavramına ilişkin gerekçesinde de açık rıza kavramının Direktif dikkate alınarak tanımlandığı belirtilmiştir. Ek olarak Kanunun gerekçesinde açık rıza kavramından anlaşılması gerekenin; "ilgili kişinin kendisiyle ilgili veri işlenmesine, hür bir iradeyle, konuyla ilgili yeterli bilgi sahibi olarak, tereddüde yer bırakmayacak açıklıkta ve yalnızca o işlemle sınırlı olarak verdiği onay beyanı" olması gerektiği belirtilmiştir.

GDPR'ın 4. maddesinde rıza kavramı; "*ilgili kişinin bir beyan yoluyla ya da açık bir onay eylemiyle kendisine ait kişisel verilerin işlenmesine onay verdiğini gösteren özgür bir şekilde verilmiş spesifik, bilinçli ve açık gösterge*" olarak tanımlanmıştır. Direktifteki gibi GDPR'da da özel nitelikli kişisel verilerin işlenmesinde ilgili kişi (*data subject*) tarafından verilecek rızanın açık rıza (*explicit consent*) şeklinde olması gerektiği düzenlenmiştir. GDPR'ın başlangıç kısmındaki 40. madde uyarınca kişisel verilerin işlenmesine ilişkin alınacak rızanın izin

şeklinde yani veri işleme faaliyetinden önce alınması gerekmektedir. Dolayısıyla veri işleme faaliyeti başladıktan sonra ilgiliden icazet şeklinde sonradan alınan rıza GDPR bağlamında geçerli değildir.

Herhangi bir hukuka uygunluk sebebi olmaksızın yapılan kişisel verileri işleme faaliyeti hukuka aykırı ve ilgili kişinin kişilik hakkına yapılmış bir müdahale olup, söz konusu kişisel veri işleme faaliyetine ilgili kişinin rıza göstermesi bir hukuka uygunluk sebebi oluşturacaktır[106]. Kişisel veri işleme faaliyetinin hukuka aykırı olmaması ve ilgili kişinin kişilik hakkına müdahale etmemesi için, açık rıza gerekmeden veri işlemeye izin veren başkaca bir hukuka uygunluk sebebinin olmaması durumunda, ilgili kişinin veri işleme faaliyetinden (yani kişilik hakkına müdahale edilmesinden) önce[107] ve en geç veri işleme faaliyeti esnasında[108] rıza vermesi gerekmektedir. Diğer bir ifadeyle kişisel verilerin hukuka uygun şekilde işlenmesi için ilgili kişi tarafından verilecek rıza yalnızca izin şeklinde verilebilecek olup, icazet şeklinde verilemeyecektir[109]. Zira kişilik hakkına yapılan hukuka aykırı müdahaleye sonradan verilecek rıza, hukuka aykırılığı ortadan kaldırmayacaktır[110].

GDPR'da çocuklara ait kişisel verilerin işlenmesine ilişkin özel bir düzenleme yapılmıştır. Bu kapsamda GDPR'ın m. 8/1 hükmü uyarınca bilgi toplumu hizmetlerinin bir çocuğa doğrudan sunulmasının teklif edilmesi halinde, çocuğun en az 16 yaşında olması durumunda kişisel veri işleme faaliyetinin hukuka uygun olacağı, çocuğun 16 yaşından küçük olması durumunda velayet hakkına sahip olan yasal temsilcinin vereceği rıza veya çocuğun rızasını onaylaması ile çocuğa ait kişisel verilerin işlenebileceği düzenlenmiş ve üye devletlere bahsi geçen 16 yaş sınırının 13 yaşa kadar indirilmesi konusunda bir takdir alanı bırakmıştır.

---

[106] **Cihan Avcı Braun**, Kişisel Verilerin İşlenmesinde Rıza, Yeditepe Üniversitesi Hukuk Fakültesi Dergisi, Cilt 15, Sayı 1, s. 13-33, 2018, s. 15; **Hüseyin Can Aksoy**, Medeni Hukuk ve Özellikle Kişilik Hakkı Yönünden Kişisel Verilerin Korunması, Çakmak Yayınevi, Ankara 2010, s. 82-83.
[107] **Ian J. Lloyd**, Information Technology Law, Eighth Edition, Oxford University Press, Oxford 2017, s. 97-98; **A. Çiğdem Ayözger**, Kişisel Verilerin Korunması Elektronik Haberleşme Sektörüne İlişkin Özel Düzenlemeler Dahil, Beta Yayınevi, İstanbul 2016, s. 125-127; **Braun**, s. 15; **Kişisel Verileri Koruma Kurumu**, Açık Rıza Rehberi, (Çevrimiçi) https://www.kvkk.gov.tr/SharedFolderServer/CMSFiles/66b2e9c4-223a-4230-b745-568f096fd7de.pdf Erişim Tarihi: 1 Mart 2020, s. 5.
[108] **Taştan**, s. 159; **Braun**, s. 15.
[109] **Braun**, s. 16.
[110] **a.g.e.**

Yukarıdaki temel düzenlemelerdeki rıza kavramına ilişkin yapılan tanımlamalar birbirleriyle karşılaştırıldığında Kanun, Direktif ve GDPR'da rıza için aranan şartlar birbirinden farklılık göstermektedir. Kanunda genel veya özel nitelikli kişisel verilerin işlenebilmesi için açık rıza kavramı kullanılmışken, GDPR'da ve Direktifte ikili ayrıma gidilerek genel nitelikli kişisel verilerin işlenmesi için rıza (*consent*), özel nitelikli kişisel verilerin işlenmesi için açık rıza (*explicit consent*) kavramları kullanılmıştır. Ancak burada dikkat edilmesi gereken husus rıza kavramı için seçilen kelimeler değil, rıza veya açık rıza terimleri ile hangi unsurların arandığıdır.

1.5.2. Açık Rızanın Unsurları

1.5.2.1. Belirli Bir Konuya İlişkin Olma

Kişisel verilerin işlenmesine yönelik verilen rızanın geçerli olabilmesi için öncelikle ilgili kişinin hangi kişisel verilerinin ne amaçlarla işleneceğinin saptanması ve rızanın belirli bir konuya ilişkin olması (*specific*) gereklidir[111]. Dolayısıyla sınırları belirlenmemiş, konusu belli olmayan veya muğlak olan alanlarda ilgili kişi tarafından verilen rıza geçerli değildir[112]. Diğer bir ifadeyle kişisel veri işleme konusunun açıkça belirlenmiş olmasına ek olarak ilgili kişi, vereceği açık rıza beyanında genel ifadelerden kaçınması gerekmektedir[113]. Zira ilgili kişi tarafından çok geniş kapsamdaki konuların tamamına ilişkin ve doktrinde torba rıza veya battaniye rıza olarak adlandırılan rıza beyanında bulunulması da geçersizdir[114].

---

[111] **Mesut Serdar Çekin**, "6698 sayılı Kişisel Verilerin Korunması Hakkında Kanun'un Big Data (Büyük Veri) ve İrade Serbestisi Açısından Değerlendirilmesi", İstanbul Üniversitesi Hukuk Fakültesi Mecmuası, Cilt 74, Sayı 2, s. 629-644, 2016, (Çevrimiçi) http://static.dergipark.org.tr/article-download/ade8/9dcb/8112/58e4bb01ca41c.pdf? Erişim Tarihi: 1 Mart 2020, s. 636; **Braun**, s. 23.

[112] **Kemal Atasoy**, Kişilik Hakkı Kapsamında Sosyal Medyada Kişisel Verilerin Korunması ve Veri Sahibinin Rızası, Marmara Üniversitesi Hukuk Araştırmaları Dergisi, Cilt 22, Sayı 3, s. 269-301, 2016, s. 292.

[113] **Murat Volkan Dülger**, "AB Genel Veri Koruma Tüzüğü ve KVKK'da Rıza Kavramı", s. 4, (Çevrimiçi) Makalenin metnine şu uzantıdan ulaşabilirsiniz: http://dulger.av.tr/wp-content/uploads/2019/05/AB_Genel_Veri_Koruma_Tuzugu_GDPR_ve_KVKK.pdf Erişim Tarihi: 20 Nisan 2020.

[114] **Taştan**, s. 158.

İlgili kişi tarafından verilen rızanın birden fazla kişisel verilerin kategorisine veya konuya ilişkin işlenmesine ilişkin alınacak açık rıza beyanında, tüm bu kişisel veri kategorileri, veri işleme konuları, hangi verilerin ne amaçla işleneceği ve veri işleme faaliyetlerinin hangi noktalarda farklılaşacağı hususlarının da belirtilmesi gerekmektedir[115].

İlgili kişiden açık rıza beyanı alındıktan sonra, veri işleme amaçlarının kısmen veya tamamen değişmesi durumunda, konu da değişeceğinden veri sorumlusu tarafından yeni amaç ve konuya ilişkin olarak ilgili kişiden yeniden açık rıza alınması gerekmektedir[116].

1.5.2.2. Bilgilendirmeye Dayanma

İlgili kişi tarafından verilen açık rıza beyanının geçerli olabilmesi için ilgili kişinin neye rıza gösterdiğini biliyor olması, bu konuda bilgilendirilmiş olması ("*informed consent"*) gerekmektedir. Açık rızanın bilgilendirmeye dayalı olması veya ilgili kişinin aydınlatılmış olması kavramları, veri işleme faaliyetinin amacı, kapsamı, süresi ve ilgili kişiyi etkileyebilecek diğer tüm hususlar hakkında rızası talep edilen ilgili kişinin bilgilendirilmesini ifade etmektedir[117].

Rızanın bilgilendirmeye dayalı olduğundan bahsedebilmek için ilgili kişiye bazı bilgilerin açıklanması gerekmektedir. Bu konuda Working Party tarafından hazırlanan bir çalışma belgesinde ilgili kişiye açıklanması gereken asgari bilgiler şu şekilde sıralanmıştır[118]:

- "Veri sorumlusunun kimliği
- Rıza talep edilen her bir veri işleme faaliyetinin amacı
- Hangi verilerin toplanacağı ve kullanılacağı
- Rızayı geri alma hakkının mevcut olduğu

---

[115] **Dülger**, s. 141.
[116] **Çekin**, "6698 sayılı Kişisel Verilerin Korunması Hakkında Kanun'un Big Data (Büyük Veri) ve İrade Serbestisi Açısından Değerlendirilmesi", s. 637; **Dülger**, s. 142.
[117] **Taştan**, s. 158.
[118] **Article 29 Data Protection Working Party**, Guidelines 05/2020 on Consent Under Regulation 2016/676, 4 Mayıs 2020, Version 1.1, s. 15-16, (Çevrimiçi) https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_202005_consent_en.pdf , Erişim Tarihi: 22 Mayıs 2020; **Dülger**, s. 143.

- Otomatik karar almaya konu olacaksa buna ilişkin bilgi
- Verinin yurtdışına aktarılması halinde uygunluk kararının olmaması ve gerekli önlemlerin bulunmaması durumunda gündeme gelebilecek olası riskler"

Açık rıza kavramının bir unsuru olan bilgilendirmeye dayanma şartı aynı zamanda Kanunun "Veri sorumlusunun aydınlatma yükümlülüğü" başlıklı 10. maddesinde veri sorumlularına ait bulunan bir yükümlülük olarak düzenlenmiştir. Kanunun 10. maddesi uyarınca;

- "Veri sorumlusunun ve varsa temsilcisinin kimliği,
- Kişisel verilerin hangi amaçla işleneceği,
- İşlenen kişisel verilerin kimlere ve hangi amaçla aktarılabileceği,
- Kişisel veri toplamanın yöntemi ve hukuki sebebi,
- Kanunun 11. maddesinde sayılan diğer hakları"

içerecek şekilde kişisel verilerin elde edilmesi sırasında veri sorumlusu veya yetkilendirdiği kişi tarafından ilgili kişilere açıklaması gerektiği, aydınlatma yükümlülüğü başlığı altında düzenlenmiştir.

İlgili kişinin Kanunun 11. Maddesinde sayılan diğer hakları konusu çalışmamızın Üçüncü Bölüm'ünde 3.2. numaralı başlık altında daha detaylı şekilde anlatıldığından burada ilgili kişinin diğer haklarının neler olduğunun üzerinde durulmayacaktır.

GDPR'ın "Rızanın Şartları" başlıklı 7. maddesinin 2. fıkrasında ve gerekçenin 32. Maddesinde ilgili kişiden alınacak bilgilendirmeye dayalı rıza için çeşitli koşullar düzenlenmiştir. Bu koşullar uyarınca bilgilendirmenin mutlaka kolayca anlaşılır bir dilde ve açık bir ifade ile yapılması, rızanın yazılı bir şekilde alınması durumunda rıza talebinin diğer konu veya varsa belgelerden ayrı ve kolayca erişilebilir olacak şekilde ilgili kişiye sunulması gerekmektedir.

Ek olarak Working Party'nin rıza kavramı üzerine hazırladığı rehber ilkelerinde; geçerli bir bilgilendirmeden söz edebilmek için aydınlatma metninde açık ve sade bir dilin kullanılması, ortalama bir insan tarafından kolayca anlaşılır olması, yalnızca hukukçuların anlayabileceği ve sıkça teknik terimlerin bulunduğu bir dilin kullanılmaması, ayrıca yapılacak bilgilendirmenin açık, diğer konulardan

kolayca ayrıştırılabilir, anlaşılır ve kolayca erişilebilir olması gerektiğinden bahsedilmiştir[119].

1.5.2.3. Özgür İradeye Dayanma

Kişisel verilerin işlenmesine yönelik verilecek açık rıza özgür iradeyle (*freely given*) açıklanmalıdır. Rızanın özgür iradeye dayanması kavramı, ilgili kişiye veri işleme faaliyetine rıza verip vermemek noktasında gerçek anlamda bir seçenek sunulması gerektiğini ifade etmektedir[120].

Bir irade beyanı olan rıza, ilgili kişinin yaptığı bu davranışının bilincinde olması, kendi kararını kendisinin verebilecek durumda olması ve cebir, tehdit, hile gibi kişinin iradesini sakatlayıcı fiillerin olmaması durumunda geçerli olacaktır[121]. İlgili kişinin özgür iradesinin sakatlanıp sakatlanmadığı hususu her somut olayda ayrıca incelenmesi gereken bir durumdur.

İşçi-işveren ilişkisi veya özellikle sigorta ve kredi sözleşmelerinde şirket-müşteri ilişkilerinde tarafların çeşitli sosyal ve ekonomik sebeplerle eşit güce ve söz hakkına sahip olmadıkları söylenebilir. Bu tarz ilişkilerde görece güçsüz birey, örneğin müşteri hizmet alabilmek için veya işçi istihdam ilişkisinde olumsuz bir sonuçla karşılaşmamak için kişisel verilerinin işlenmesine rıza göstermek zorunda hissediyorsa ve güçsüz konumdaki bireye kişisel verilerinin işlenmesine rıza göstermeme hakkı etkin bir şekilde tanınmıyorsa, burada özgür iradeden ve dolayısıyla geçerli bir rıza beyanından bahsedilmesi olası değildir[122].

GDPR'ın başlangıç kısmının 43. maddesinde özellikle kamu kurumları ve işverenlerde olduğu gibi veri sorumlusu ve ilgili kişi arasındaki bariz güç dengesizliklerinin varlığı halinde bu veri sorumlularının sözleşme içinde "paket halinde" veya "bağlı" şekilde istedikleri rızaların özgür iradeye dayanmasının mümkün olmadığından hareketle bu şekilde dayatılan rızaların geçersiz olduğu belirtilmiştir[123].

---

[119] **Working Party**, Guidelines 05/2020 on Consent Under Regulation 2016/676, s. 16.
[120] **Taştan**, s. 160.
[121] **Kişisel Verileri Koruma Kurumu**, Açık Rıza Rehberi, s. 5-6.
[122] **Avcı Braun**, s. 21.
[123] **Dülger**, s. 145.

1.5.2.4. Tereddüde Yer Bırakmayacak Açıklıkta İfade Edilme

Açık rızanın tereddüde yer bırakmayacak açıklıkta olması (*unambiguously*) gerektiği hususu Kanunun açık rıza tanımının yapıldığı 3. maddede veya Kanunun diğer maddelerinde ifade edilmese de Kanunun 3. maddesinin gerekçesinde bulunmaktadır. Bu yüzden açık rızanın unsurları arasında sayılması gereken bir diğer kavram da açık rızanın tereddüde yer bırakmayacak açıklıkta olması gerekliliğidir. Rıza beyanı herhangi bir tereddüde yer bırakmayacak şekilde olduğu müddetçe açık veya örtülü şekilde verilebilir[124]. Burada önem arz eden hususun rıza beyanının herhangi bir şüpheye yer bırakmayacak ve karışıklığa sebep olmayacak şekilde anlaşılıyor olması gerekliliğidir.

İlgili kişi tarafından verilecek açık rıza beyanının tereddüde yer bırakmayacak açıklıkta olması ilgili kişi tarafından rızanın aktif bir eylemle açıklanmasını ifade etmektedir. Bu bağlamda, kişisel verinin işlenmesine yönelik ilgili kişinin bir rıza verip vermediği hususunda her türlü şüphenin önüne geçmek ve beyanın açıklığında herhangi bir tereddüde yer bırakmamak için ilgili kişinin mutlaka aktif bir davranışta bulunması gerekmektedir[125]. Bu durumda ilgili kişi tarafından aktif bir eylemde bulunulmadan elde edilen açık rıza beyanları geçersiz kabul edilecektir. Örneğin bir internet sitesine girdiğinizde sizden aktif şekilde bir eylemde bulunmanızı gerektirmeden veri işlenmesine yönelik onay almak için kutucukların önceden işaretlenmiş olması durumunda toplanan rızanın herhangi bir geçerliliği bulunmamaktadır.

1.5.3. Açık Rızanın Alınma Şekli

Kanunda veya Kanunun gerekçesinde açık rızanın geçerlilik şekline ilişkin herhangi bir düzenleme yapılmamıştır. Burada önemli olan konu açık rızanın Kanunda belirtilen şartları taşıması ve ispatlanabilir olmasıdır. Bu sebeple, herhangi bir zorunluluk veya şekil şartı olmasa da ilgili kişiden alınacak açık rızanın yazılı

[124] **Başalp**, s. 40.
[125] **Taştan**, s. 161.

olmasında ispat açısından fayda vardır. Açık rıza yazılı alınabileceği gibi sözlü veya elektronik ortamda da alınabilir. Açık rıza beyanının yazılı olarak alınacağı durumlarda açık rıza metinlerinin içerisinde açık, sade ve anlaşılır bir dil kullanılması gerekmektedir. Açık rıza beyanı hangi formatta alınırsa alınsın ilgili kişinin şüpheye mahal vermeyecek şekilde, açık rıza vermeye yönelik ve özgür iradesine dayalı niyetini açıkça ortaya koyduğunu işaret eden biçimde aktif bir davranış ile olumlu bir irade beyanını içermelidir[126]. Susma, aktif bir davranış olarak kabul edilemeyeceği için susma tek başına açık rıza olarak kabul edilemez[127]. Açık rızanın ilgili kişiden alındığına ilişkin ispat külfeti veri sorumlusuna aittir[128].

Açık rızanın alınmasına sebep olan konular belirlenmeli, daha önce değindiğimiz gibi "torba rıza" veya "battaniye rıza" olarak da tabir edilen sınırları belli olmayan konularda genel nitelikli bir rıza şeklinde olmamalıdır. Ayrıca veri işleme faaliyetine ilişkin hangi verilerin ne kadar süre ile işleneceği, açık rızaya bağlanan sonuçlar gibi hususların da açık rıza metninde bulunması gereklidir[129].

GDPR'da ise özel nitelikli kişisel veriler, kişisel verilerin yurtdışına transferi ve otomatik karar alma süreçlerine tabi tutulacak veriler açısından ilgili kişilerden "açık rıza" alınması gerektiği, bunlar dışındaki verilerin işlenebilmesi için ise "rıza" alınması gerektiği düzenlenmiştir. GDPR uyarınca sıradan "rıza" alınırken "*bir beyan veya onaylayıcı eylem*"in varlığı yeterli olabilecekken, Working Party'nin hazırladığı Rıza Hakkındaki Rehber İlkeler'de "açık rıza" almanın en etkili yolunun

---

[126] **Leyla Keser Berber, Ayça Atabey, Melis Mert**, E-Gizlilik Tüzük Taslağının Son Versiyonu Üzerine Düşünceler, Kişisel Verileri Koruma Dergisi, Cilt 1, Sayı 2, s. 66-74, 2019, (Çevrimiçi) https://www.verbis.com.tr/makaleler/mk9.pdf , s.73; **ABAD**, 1 Ekim 2019 tarihli ve C-673/17 sayılı Bundesverband der Verbraucherzentralen und Verbraucherverbände — Verbraucherzentrale Bundesverband eV v. Planet49 GmbH kararı (Planet49 Kararı), (Çevrimiçi) http://curia.europa.eu/juris/document/document.jsf;jsessionid=E1263B9218236FAB0174B7EB1208B0E7?text=&docid=218462&pageIndex=0&doclang=en&mode=lst&dir=&occ=first&part=1&cid=609404 Erişim Tarihi: 3 Mart 2020.

[127] **Avcı Braun**, s. 29; **Nafiye Yücedağ**, "Medeni Hukuk Açısından Kişisel Verilerin Korunması Kanunu'nun Uygulama Alanı ve Genel Hukuka Uygunluk Sebepleri", İstanbul Üniversitesi Hukuk Fakültesi Mecmuası, Cilt 75 Sayı 2, s. 765-790, 2017, s. 775; **Hale Akdağ**, Türk Ceza Kanunu Kapsamında Kişisel Verilerin Korunması, Adalet Yayınevi, Ankara, 2013, s. 113-114.

[128] **Kişisel Verileri Koruma Kurumu**, 100 Soruda Kişisel Verilerin Korunması Kanunu, (Çevrimiçi) https://www.kvkk.gov.tr/SharedFolderServer/CMSFiles/7d5b0a2f-e0ea-41e0-bf0b-bc9e43dfb57a.pdf Erişim Tarihi: 3 Mart 2020, s.28.

[129] **Dülger**, s. 152-153.

ıslak imzalı beyan olduğu belirtilmiştir. Working Party ayrıca ıslak imzalı beyanın açık rıza almak konusunda tek yol olmadığını telefon veya internet üzerinden de açık rıza alınabileceğini ancak bu yöntemlerin kullanılması durumunda ilgili kişinin kimlik doğrulama prosedürüne tabi tutulması ve ilgili kişinin eyleminin açık bir şekilde rıza vermeye yönelik olması gerektiğini belirtmiştir[130].

1.5.4. Açık Rızanın Geri Alınması

GDPR'da "Rızanın Şartları" başlıklı 7. maddesinin 3. fıkrasında ilgili kişinin dilediği zamanda rızasını geri alma hakkına sahip olduğu açıkça düzenlenmiştir. Ayrıca aynı fıkrada rızanın geri alınması eyleminin ilgili kişinin rızasını geri çekmesinden önce veri sorumlusu tarafından yapılan veri işleme faaliyetlerinin hukuka uygunluğuna etki etmeyeceği ve rızanın geri alınması işleminin en az rıza verme işlemi kadar kolay olması gerektiği de düzenlenmiştir.

Kanunda ise ilgili kişi tarafından kişisel verilerin işlenmesine yönelik verilen rızanın geri alınabilmesine ilişkin açık bir düzenleme yoktur. Ancak Kanunda açık düzenleme olmaması rızanın geri alınabilmesi hakkının olmadığı anlamına gelmemelidir. Zira Kanunun ruhundan, sistematiğinden ve gerekçesinden, ek olarak Kişisel Verileri Koruma Kurumu'nun yayımladığı rehberlerden[131] verilen rızanın her zaman geri alınabileceği sonucuna ulaşılmaktadır[132]. Her şeyden öte kişisel verilerin işlenmesine yönelik verilen rızanın geri alınabilmesi hususu, kişilik hakkının kanun koyucu tarafından üstün tutulmasından ileri gelen bir sonuçtur. Bilindiği üzere 4721 sayılı Türk Medeni Kanunu'nun 23. maddesi[133] kişilik hakkını ihlal eden kendi işlemlerine karşı dahi kişiyi korumaktadır. Bu çerçevede sadece yaptığı işlemlerin geçersiz olması değil, aynı zamanda kişilik hakkına müdahale oluşturacak her türlü hukuki işleme ilişkin verdiği rızayı da dilediği zaman geri alabilmesi bu kabulün doğal bir uzantısıdır. Ayrıca dolaylı bir ifade ile de olsa

---

[130] **Working Party**, Guidelines 05/2020 on Consent Under Regulation 2016/676, s. 20-21.
[131] Bkz. **Kişisel Verileri Koruma Kurumu**, 100 Soruda Kişisel Verilerin Korunması Kanunu, s. 29.
[132] **Taştan**, s. 165; **Avcı Braun**, s. 17.
[133] TMK m. 23; "*(1) Kimse, hak ve fiil ehliyetlerinden kısmen de olsa vazgeçemez. (2) Kimse özgürlüklerinden vazgeçemez veya onları hukuka ya da ahlâka aykırı olarak sınırlayamaz.* (…)"

Kanunun 11. maddesi ile ilgili kişiye kişisel verilerinin silinmesini, yok edilmesini isteme hakkı tanınarak ilgili kişiye adeta açık rıza beyanını geri alma hakkı tanındığı söylenebilir[134]. Kaldı ki Kurumun yayınladığı "100 Soruda Kişisel Verilerin Korunması Kanunu" isimli rehberde de açık rızanın ilgili kişi tarafından dilediği zamanda geri alınabileceği açıkça düzenlenmiştir. Buna gerekçe olarak açık rızanın geri alınmasının kişiye sıkı sıkıya bağlı haklardan olduğu belirtilmiştir. Ancak rızanın geri alınmasının sonuçlarını ileriye etkili olarak (*ex nunc*) doğuracağı ve TMK 23. maddesi uyarınca açık rızanın geri alınması hakkından önceden feragat edilmesi mümkün değildir[135]. İlgili kişinin rızasını geri alma beyanı veri sorumlusuna ulaştığı andan itibaren hüküm doğuracağı için söz konusu geri alma beyanı veri sorumlusuna ulaştığı andan itibaren veri sorumlusu ilgili kişinin önceden almış olduğu açık rızasına binaen gerçekleştirdiği veri işleme faaliyetlerini durdurmak zorundadır[136].

1.6. İlgili Kişi

İlgili kişi veya yabancı mevzuattaki karşılığıyla veri süjesi (*data subject*) kavramı en temel ifadeyle kişisel verisi işlenen kişi anlamına gelmektedir. GDPR ve Kanun ilgili kişi kapsamına yalnızca gerçek kişileri almaktadır. Nitekim Kanundaki ilgili kişi tanımı da "*kişisel verisi işlenen gerçek kişi*" olarak yapılmıştır.

Kanunda yer alan ve daha öncede açıkladığımız üzere kişisel verinin tanımı uyarınca, tüzel kişiye ait bir verinin herhangi bir gerçek kişiyi işaret etmesi, belirli veya belirlenebilir kılması durumlarında, bu verilerin Kanun kapsamında koruma altında olacağını belirtmek isteriz. Ancak, bu durumda dahi tüzel kişinin hukuki menfaati değil, kanunen tanınan öncelik gereği tüzel kişiye ait verinin işaret ettiği belirli ya da belirlenebilecek gerçek kişinin hukuki menfaati korunacaktır.

---

[134] **Taştan**, s. 165.
[135] **Avcı Braun**, s. 17.
[136] **Kişisel Verileri Koruma Kurumu**, 100 Soruda Kişisel Verilerin Korunması Kanunu, s. 29.

1.7. Kişisel Verilerin İşlenmesi

Kişisel verilerin işlenmesi kavramı oldukça geniş bir kavramdır. GDPR'ın 4. Maddesindeki tanıma göre kişisel verilerin işlenmesi "*otomatik yöntemlerle olsun veya olmasın, kişisel veri veya kişisel veri setleri üzerinde gerçekleştirilen toplama, kaydetme, düzenleme, yapılandırma, saklama, uyarlama veya değiştirme, elde etme, danışma, kullanma, iletim yoluyla açıklama, yayma veya kullanıma sunma, uyumlaştırma ya da birleştirme, kısıtlama, silme veya imha etme gibi herhangi bir işlem veya işlemler dizisi*" olarak tanımlanmıştır.

Kanunda ise 3. maddede yapılan açıklamaya göre kişisel verilerin işlenmesi "*kişisel verilerin tamamen veya kısmen otomatik olan ya da herhangi bir veri kayıt sisteminin parçası olmak kaydıyla otomatik olmayan yollarla elde edilmesi, kaydedilmesi, depolanması, muhafaza edilmesi, değiştirilmesi, yeniden düzenlenmesi, açıklanması, aktarılması, devralınması, elde edilebilir hâle getirilmesi, sınıflandırılması ya da kullanılmasının engellenmesi gibi veriler üzerinde gerçekleştirilen her türlü işlem*" olarak tanımlanmıştır.

Diğer bir ifadeyle kişisel verilerin işlenmesi kavramı; otomatik araçlar kullanılarak veya kullanılmaksızın kişisel veriler üzerinde yapılan verinin toplanması, elde edilmesi, aktarılması, değiştirilmesi, sınıflandırılması, saklanması, yeniden düzenlenmesi, anonim hale getirilmesi, silinmesi veya yok edilmesi gibi her türlü işlemi veya işlemler dizisini ifade etmektedir [137].

Yukarıdaki iki tanım birbiriyle karşılaştırılarak incelendiğinde iki düzenlemede de detaylı bir örnekleme yöntemiyle sayım metodu izlenmiştir. Dolayısıyla sınırlı sayıda bir sayım yapılmadığından kişisel verilerin işlenmesi faaliyetine örnekler çoğaltılabilir. Kanundaki tanımın GDPR ile uyumlu olduğu söylenebilir, zira çok ufak farklar dışında iki düzenleme birbirine benzemektedir.

---

[137] **Eda Manav**, "İş İlişkisinde İşçinin Kişisel Verilerinin Korunması" Gazi Üniversitesi Hukuk Fakültesi Dergisi, C. XIX, S. 2, s. 95-136, 2015, s. 98.

1.7.1. Otomatik İşleme

Kişisel verilerin otomatik yollarla işlenmesi kavramının tam olarak ne ifade ettiğine ilişkin Kanunda net bir tanım bulunmasa da OECD'nin tanımına göre otomatik işleme; "*insan müdahalesi ya da yardımı konusundaki ihtiyacı asgari seviyeye indiren, kendi aralarında bağlantılı ve etkileşimli elektrikli veya elektronik bir sistem tarafından gerçekleştirilen veri işleme faaliyeti*" olarak tanımlanmıştır. Dolayısıyla otomatik işleme faaliyetinden daha çok bilişim sistemleri vasıtasıyla işleme, otomatik olmayan işleme faaliyetinden daha çok insan faaliyetiyle ve manuel olarak, bir bilişim sistemi vasıtası olmadan işleme faaliyeti olarak anlam çıkarmak mümkündür.

1.7.2. Otomatik Olmayan Yollarla İşleme

Kanunun 3. maddesindeki "*kişisel verilerin işlenmesi*" tanımına göre, otomatik olmayan (bilişim sistemleri kullanılmadan ve manuel) yollarla gerçekleştirilen veri işleme faaliyetleri, işlenen verilerin bir veri kayıt sisteminin parçası olmaması durumunda veri işleme faaliyetinin Kanun kapsamında değerlendirilme imkânı olmayacaktır. GDPR'da böyle bir ayrıma gidilmemiştir, otomatik olmayan yollarla veri işleme faaliyeti bir veri kayıt sistemine dahil olup olmadığına bakılmaksızın GDPR kapsamında bir veri işleme faaliyeti olmaya devam edecektir.

1.8. Veri Kayıt Sistemi

Kanunun 3. maddesindeki tanıma göre veri kayıt sistemi; "*kişisel verilerin belirli kriterlere göre yapılandırılarak işlendiği kayıt sistemi*" olarak tanımlanmıştır. Veri kayıt sistemi kavramı GDPR'da ise "*dosyalama sistemi*" kavramı ile düzenlenmiştir. GDPR'ın 4. maddesindeki tanıma göre dosyalama sistemi; "*işlevsel veya coğrafi bir temelde merkezi, merkezi olmayan veya dağınık olarak belirli kriterlere göre erişilebilen yapılandırılmış herhangi bir kişisel veri dizisi*" olarak tanımlanmıştır. Dolayısıyla verinin belirli bir düzen içinde tutulması,

ona erişimin belirli kriterlere göre yapılandırılmış olması veri kayıt sistemini ifade edecektir. Bu durumda dağınık veriler bu tanım kapsamında yer almayacaktır[138].

Dosyalama sistemi olarak da tanımlanan veri kayıt sistemleri elektronik veya fiziki ortamlarda oluşturulabilir.

Veri kayıt sisteminin varlığı kişisel veri işleme faaliyetinin otomatik olmayan yollarla işlenmesi durumunda önem arz etmektedir, zira otomatik olmayan yollarla işleme faaliyetlerinde eğer işlenen veriler bir veri kayıt sisteminin parçası değiller ise bu durumda veri işleme faaliyeti Kanunun kapsamına girmeyecektir. Örneğin, bir çalışanın alelade bir kâğıda, veri kayıt sistemine dahil olmadan, işyerindeki çalışanların ad ve soyadlarını yazması Kanun kapsamında işleme faaliyeti olarak kabul edilmeyecektir. Zira kişinin diğerlerinin isimlerini kâğıda yazması otomatik olmayan yollarla veri işleme faaliyeti olsa da işlenen verilerin herhangi bir veri kayıt sistemine dahil olmaması sebebiyle buradaki veri işleme faaliyeti Kanun kapsamında değerlendirilmeyecektir. Ancak bu durum ortada bir kişisel verinin bulunmadığı anlamına gelmemektedir. Eğer ortada "Kişisel Veri" başlığı altında değindiğimiz kişisel verinin unsurları var ise o halde kişisel verinin var olduğu ancak bu kişisel verinin otomatik yolla işlenmemesi veya otomatik yollarla işlenmesine karşın bir veri kayıt sistemine dahil olmaması sebebiyle bu kişisel verilerin tutulması GDPR veya Kanun kapsamında herhangi bir sonuç doğurmayacaktır. Ancak bu durumda dahi kişisel verinin unsurlarının varlığı halinde KVKK veya GDPR kapsamında sonuç doğurmayacak kişisel verilere ilişkin TCK'nın cezai hükümleri uygulama alanı bulabilecektir[139].

1.9. Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi

1.9.1. Genel Olarak

Çalışmamızın bu başlığı altında kişisel verilerin silinmesi, yok edilmesi veya anonim hale getirilmesi kavramlarının yalnızca tanımlamalarının yapılması ile

[138] **Başalp**, s. 33.
[139] **Dülger**, s. 107.

yetinilecektir. Bu kavramlarla ilgili teknik düzenlemeler ve veri sorumlusunun bu konudaki yükümlülüklerine ilişkin detaylı açıklamalarımız çalışmamızın üçüncü bölümünde yapılmıştır.

Kanunun "Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi" başlıklı 7. maddesinde; "*Kanun ve ilgili diğer kanun hükümlerine uygun olarak işlenmiş olmasına rağmen, işlenmesini gerektiren sebeplerin ortadan kalkması hâlinde kişisel veriler resen veya ilgili kişinin talebi üzerine veri sorumlusu tarafından silinir, yok edilir veya anonim hâle getirilir.*" hükmü düzenlenmiştir. Ayrıca maddenin son fıkrasında kişisel verilerin silinmesine, yok edilmesine veya anonim hâle getirilmesine ilişkin usul ve esasların yönetmelikle düzenleneceği belirtilmiştir. Bu konudaki "Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi Hakkında Yönetmelik[140]" 28.10.2017 tarihli ve 30224 sayılı Resmî Gazete'de yayımlanmış ve Yönetmelik yürürlük maddesindeki düzenleme uyarınca 01.01.2018 tarihinde yürürlüğe girmiştir. Kişisel verilerin silinmesi, yok edilmesi veya anonim hale getirilmesi kavramlarının tanımlarını Yönetmeliğe atıf yaparak açıklayacağız.

1.9.2. Kişisel Verilerin Silinmesi

Kişisel verilerin silinmesi kavramı Yönetmeliğin 8. maddesi uyarınca; "kişisel verilerin ilgili kullanıcılar için hiçbir şekilde erişilemez ve tekrar kullanılamaz hale getirilmesi işlemi" olarak tanımlanmıştır.

1.9.3. Kişisel Verilerin Yok Edilmesi

Kişisel verilerin yok edilmesi kavramı Yönetmeliğin 10. maddesi uyarınca; "kişisel verilerin hiç kimse tarafından hiçbir şekilde erişilemez, geri getirilemez ve tekrar kullanılamaz hale getirilmesi işlemi" olarak tanımlanmıştır.

---

[140] Bundan sonra "Yönetmelik" olarak anılacaktır. Yönetmeliğin tam metnine şu uzantıdan ulaşabilirsiniz:
https://www.mevzuat.gov.tr/Metin.Aspx?MevzuatKod=7.5.24038&MevzuatIliski=0&sourceXmlSearch=Ki%C5%9Fisel%20verilerin%20silin Erişim Tarihi: 3 Mart 2020.

1.9.4. Kişisel Verilerin Anonim Hale Getirilmesi

Kişisel verilerin anonim hale getirilmesi kavramı Yönetmeliğin 10. maddesi uyarınca; "kişisel verilerin başka verilerle eşleştirilse dahi hiçbir surette kimliği belirli veya belirlenebilir bir gerçek kişiyle ilişkilendirilemeyecek hale getirilmesi işlemi" olarak tanımlanmıştır.

2. KİŞİSEL VERİLERİN İŞLENMESİNE İLİŞKİN TEMEL İLKELER

2.1. Genel Olarak

Kişisel verilerin korunmasına ilişkin yapılan hukuki düzenlemelerin içeriğinde veri işleme faaliyetlerine yönelik çeşitli ilkeler benimsenmiştir. Bu ilkeler veri sorumluları tarafından veri işleme faaliyetinin başından sonuna kadar olacak şekilde her aşamasında uyulması gereken ilkeler olup, kendi ifademizle veri sorumlularının genel yükümlülükleri arasındadır. Kişisel veri işleme faaliyetinin her aşamasında izlenmesi gereken kuralları belirleyen bu ilkeler ulusal ve uluslararası düzenlemelerde küçük farklılık göstermekle birlikte çoğunlukla birbirine benzemektedir.

GDPR'ın "Kişisel Verilerin İşlenmesine İlişkin İlkeler" başlıklı 5. maddesinde;

i. "hukuka ve hakkaniyete uygun olma, şeffaflık (*lawfulness, fairness and transparency*),
ii. amacın sınırlandırılması (*purpose limitation*),
iii. veri minimizasyonu (*data minimisation*),
iv. doğruluk (*accuracy*),
v. saklama süresinin sınırlandırılması (*storage limitation*),
vi. bütünlük ve gizlilik (*integrity and confidentiality*),
vii. hesap verebilirlik (*accountability*)"

olmak üzere yedi adet ilkeden bahsedilmiştir.

Kanunun "Kişisel Verilerin İşlenmesi" başlıklı ikinci bölümünün "Genel İlkeler" başlıklı 4. maddesinde;

i. "hukuka ve dürüstlük kurallarına uygun olma,

ii. doğru ve gerektiğinde güncel olma,

iii. belirli, açık ve meşru amaçlar için işlenme,

iv. işlendikleri amaçla bağlantılı, sınırlı ve ölçülü olma,

v. ilgili mevzuatta öngörülen veya işlendikleri amaç için gerekli olan süre kadar muhafaza edilme"

olmak üzere 95/46/EC Sayılı Direktif ile çok benzer doğrultuda beş farklı ilke düzenlenmiştir.

2.2. Hukuka ve Dürüstlük Kuralına Uygun Olma

Kişisel verilerin işlenmesine ilişkin ilkelerin genellikle ilk sıralarında olan "hukuka ve dürüstlük kuralına uygun olma" ilkesi çok genel ve kapsayıcı bir ilkedir. Hukuka uygun olma kavramı sadece Kanuna uygun olma şeklinde anlaşılmamalı, daha da ötesinde ilgili kişisel veri işleme faaliyetinin, bu faaliyete ilişkin kuralların yazılı olduğu tüm hukuki düzenlemelere ve bunun yanı sıra hukukun genel ve evrensel ilkelerine uygun olması gerektiği anlamına gelmektedir[141].

Veri işleme faaliyetinin dürüstlük kuralına uygun olması ilkesinin sınırlarını çizmek oldukça zordur. Bu konuda TMK'nın "Dürüst Davranma" başlıklı 2. maddesinde "*Herkes, haklarını kullanırken ve borçlarını yerine getirirken dürüstlük kurallarına uymak zorundadır.*" hükmü düzenlenmiştir. Dürüstlük kuralına uygun bir davranış, dürüst ve namuslu bir insanın yapması gereken davranış olarak ifade edilebilir. Ayrıca bir davranışın dürüstlük kuralına uygun olup olmadığı o toplumdaki ahlaki değerler, uygulanan adetler ve hakkın konusu olan ilişkilerin amaçları incelenerek tespit edilir[142]. Çalışma konumuz açısından genel anlamda dürüstlük kuralına uygun olma ilkesi; veri sorumlusunun, veri işleme amaçları doğrultusunda kişisel veri işleme faaliyeti gerçekleştirirken ilgili kişilerin

[141] **Dülger**, 173.
[142] **Kemal Oğuzman, Nami Barlas**, Medeni Hukuk, 17. Bası, Vedat Kitapçılık, İstanbul 2011, s. 245.

menfaatlerini ve makul beklentilerini göz önünde tutması gerekliliğini ifade etmektedir[143].

Hukuka ve dürüstlük kuralına uygun olma ilkesinin GDPR'daki karşılığında kişisel verilerin hukuka ve dürüstlük kurallarına uygun şekilde işlenmesine ek olarak veri işleme faaliyetinin şeffaf şekilde yapılması gerekmektedir. GDPR'ın başlangıç bölümünün 39. maddesinde şeffaflık ilkesi; kişisel verinin işlenmesiyle ilişkili bilginin kolayca erişilebilir, anlaşılabilir olması, açık ve yalın bir dille anlatılmış olması olarak açıklanmıştır.

2.3. Belirli, Açık ve Meşru Amaçlar İçin Toplanma (İşlenme)

Veri sorumluları tarafından kişisel veri işleme faaliyeti, sürecin her aşamasında belirli, açık ve meşru amaçlar doğrultusunda yapılmalıdır. Bu ilke kapsamında; hangi kişisel verilerin işleneceği, bu verilerin hangi amaçlar doğrultusunda toplanıp işleneceği gibi hususlar açık ve kesin şekilde belirlenecektir. Böylece veri işleme amacı veri sorumlusu tarafından belirli ve açık şekilde ortaya koyulacak, diğer bir ifadeyle veri işleme faaliyetinin sınırları belirlenecektir. Veri işleme faaliyetine konulan bu sınırlamalar, veri sorumlularının herhangi bir amaç belirlenmeden kişisel veri toplamasının ve işlemesinin önüne geçecektir. Veri işleme amaçlarının sınırlandırılması hususu çoğunlukla, kişisel verilerin işlenmesine ilişkin diğer ilkelerin omurgasını oluşturmaktadır[144].

Veri sorumlularının veri toplama amaçlarının meşru olması gerekmektedir. Kanunun gerekçesine göre amacın meşru olması; veri sorumlusunun işlediği verilerin, yapılan işin ya da sunulan hizmet ile bir bağlantı içerisinde ve gerekli olması anlamına gelmektedir. Meşru olma kavramı yasal olma kavramından daha geniş bir kavramdır. Yasal olma kavramı çok genel bir ifadeyle belirli bir konunun yasa tarafından öngörülmüş, düzenlenmiş olmasını ifade ederken[145]; meşru olma

[143] **Bygrave**, s. 58.
[144] **Nafiye Yücedağ**, "Kişisel Verilerin Korunması Kanunu Kapsamında Genel İlkeler", Kişisel Verileri Koruma Dergisi, Cilt 1, Sayı 1, s. 47-63, 2019, s. 52.
[145] **Dülger**, s. 185.

kavramı genel bir ifadeyle daha çok Anayasal düzen dahilinde yazılı ve yazılı olmayan kurallar bütününe uygun olmayı ifade etmektedir.

Veri toplama amaçlarının meşru olabilmesi için bu amaçların öncelikle yasal bir dayanağı olması ve ötesinde bu yasal dayanağın da hukukun genel ve evrensel prensipleriyle uyumlu olması gerekmektedir[146].

Bu ilkenin bir diğer gerekliliği de belirli, açık ve meşru amaçlar için toplanan kişisel verilerin bu toplanma amaçlarına uygun olarak işlenmesidir. Aksi halde ilgili kişinin, kişisel verileri üzerindeki denetimini kaybetmesi olasılığı gündeme gelecektir.

2.4. İşlendikleri Amaçla Bağlantılı, Sınırlı ve Ölçülü Olma

Kişisel veri işleme faaliyeti sırasında, işlenen veri kategorilerinin veri işleme amaçlarıyla uyumlu, bu amaçlarla sınırlı ve ölçülü olması gerektiği ortaya bu ilke ile ortaya konulmuştur[147]. Diğer bir ifade ile kişisel veriler ile işlenme amaçları arasında bir bağlantı olması gerekmektedir. Ayrıca "amacın sınırlandırılması" (*purpose limitation*) yöntemine gidilerek toplanması veya işlenmesi planlanan kişisel veriler yalnızca belirlenen amaçlarla veri işleme faaliyetine tabi olacaktır. İlkenin son kısmı uyarınca toplanması ve işlenmesi planlanan kişisel veriler, yalnızca veri sorumlusunun belirlediği amaçların gerçekleşmesine yeterli olacak kadarla sınırlandırılacaktır.

Kanunun m. 4/2-ç hükmünde "*işlendikleri amaçla bağlantılı, sınırlı ve ölçülü olma*" olarak düzenlenen ilke GDPR'ın m. 5/1-b hükmündeki amacın sınırlandırılması (*purpose limitation*) ve m. 5/1/c hükmündeki veri minimizasyonu (*data minimisation*) kavramları ile açıklanmıştır. Bu ilkeye göre ulaşmak istedikleri amaç doğrultusunda kişisel verilerin işlenmesinin zorunlu olduğu hallerde, amacın gereğinden fazla veri işlenmemeli, amaca ulaştırmaya yetecek en az miktardaki kişisel veriyi işlemelidir. Böylece veri sorumlusu sorumluluğundaki kişisel veri

---

[146] **Christopher Kuner**, European Data Protection Law: Corporate Compliance and Regulation, Second Edition, Oxford University Press, Oxford 2007, s. 90.
[147] **Başalp**, s. 37.

sayısı da en aza indirilmiş olacak ve gereksiz kişisel verilerin toplanmasının, saklanmasının ve işlenmesinin önüne geçilmiş olunacaktır.

Bu açıklamadan hareketle doktrinde bu ilke yeterlik ilkesi (*adequacy principle*)[148], verileri asgarileştirme[149] veya GDPR'daki şekliyle veri minimizasyonu şeklinde de anılmaktadır.

2.5. Doğru ve Gerektiğinde Güncel Olma

Kişisel verilerin doğru ve gerektiğinde güncel olması ilkesi, en genel ifadeyle kişisel verilerin gerçeğe uygun olması ve doğruyu yansıtması gerektiği olarak açıklanabilir. Bu ilke GDPR'da "doğruluk" (*accuracy*) kavramıyla düzenlenmiştir.

Kanunun gerekçesinde de belirtildiği üzere veri sorumlularının kişisel verileri doğru ve güncel tutması gerekmekte ve bu ilke ile kişisel verileri işlenen ilgili kişilerin, kendi kişisel verilerinin doğru şekilde işlenmesini, belirli aralıklarla işlenen kişisel verilerinin doğruluğunu kontrol etmesini, yanlış veya güncelliğini yitiren kişisel verilerinin düzeltilmesini talep etme haklarının birbiriyle uyum içerisinde olduğundan bahsedilmiştir.

Kişisel verilerin doğru ve gerektiğinde güncel tutulması ilkesi hem ilgili kişilerin hem de veri sorumlularının çıkarları lehine bir ilkedir[150]. Zira yanlış veya güncel olmayan kişisel veriler hem veri sorumlularının ulaşmak istedikleri amaçları gerçekleştirememelerine sebep olabilecekken, hem de ilgili kişinin temel hak ve özgürlüklerini zedeleyebilecek veya verilerinin işlenmesiyle elde etmek istediği beklentilerinin gerçekleşmemesine sebep olabilecek ya da kişi maddi ve manevi zarar görebilecektir.

Kişisel verilerin doğru ve gerektiğinde güncel tutulması veri sorumlularına yüklenen bir yükümlülüktür ve bu yükümlülüğün başkalarına devredilmesi söz konusu değildir. Ancak bu durum ilgili kişiler tarafından veri sorumlularına iletilen her kişisel verinin doğruluğunun ve güncelliğinin veri sorumluları tarafından

---

[148] **Peter Carey**, Data Protection A Practical Guide to UK and EU Law, 2. Baskı, Oxford University Press, İngiltere 2004, s. 55.
[149] **Kuner**, s. 73-74.
[150] **Küzeci**, s. 219.

incelenmesi gerektiği anlamına gelmemektedir[151]. Örneğin ilgili kişi tarafından veri sorumlusuna yanlış şekilde iletilen kişisel verinin doğruyu yansıtmaması yüzünden veri sorumlusunun sorumluluğunun gündeme geleceğini söylemek en başta hakkaniyete aykırılık teşkil edecektir. Bu sebeple, bu ilkenin işlerliğini sağlayabilmek adına öncelikle ilgili kişi, veri sorumlusuna kendi kişisel verisini iletirken en başta doğru şekilde iletmelidir ve daha sonra söz konusu kişisel verilerde bir değişiklik olması durumunda bu konuda gerekli güncellemelerin yapılması için ilgili kişi tarafından veri sorumlusu bilgilendirilmelidir[152]. Ancak veri sorumlusunun her hal ve şartta araştırma yükümlülüğünün olmadığını söylemek de ileriye giden bir yorum olur. Zira sektörel bazda yürütülen işin niteliğinin zorunlu kıldığı bir araştırma yükümlülüğü söz konusu olabilir. Bu kapsamda mali verilerin işlenmesinde finans kurumlarının araştırma yükümlülükleri akla ilk gelenler arasındadır.

2.6. İşlendiği Amaç İçin Gereken veya İlgili Mevzuatta Öngörülen Süre Kadar Muhafaza Edilme

İlke ile ilgili Kanunun gerekçesindeki açıklamalar ışığında kişisel veriler; ilgili mevzuatta kişisel verilerin saklanmasına ilişkin bir süre öngörülmüşse bu süre boyunca, eğer ilgili mevzuatta herhangi bir süre öngörülmemişse kişisel veri işleme amacı için gerekli olan süre boyunca saklanabilecektir. Dolayısıyla belirlenen amaca ulaşılması veya söz konusu amacın ortadan kalkması durumunda artık söz konusu kişisel veriler muhafaza edilmemelidir.

Veri sorumluları, veri işleme amacı için gereken sürenin veya ilgili mevzuatta öngörülen sürenin geçmesinden sonra söz konusu kişisel verileri Kanunda 7. maddesinde öngörüldüğü şekilde silmeli, yok etmeli veya anonim hale getirmelidir[153]. Bu ilke ile gelecekte ihtiyaç olabileceği ihtimaline dayanarak kişisel verilerin veri sorumlularınca uzun sürelerle saklanmasının önüne geçilmesi hedeflenmektedir.

---

[151] **Küzeci**, s. 220.
[152] **Dülger**, s. 200.
[153] **Başalp**, s. 139.

2.7. Bütünlük ve Gizlilik

GDPR'da düzenlenen bütünlük ve gizlilik ilkesi (*integrity and confidentiality*) Kanun ve 95/46/EC Sayılı Direktif'te düzenlenmemiştir.

GDPR'ın m. 5/1-f maddesindeki düzenlemeye göre bütünlük ve gizlilik ilkesi; veri sorumlularının kişisel verileri yetkisiz veya yasadışı veri işlemeye, kazara kayba, imhaya veya tahribata karşı koruma yolları dahil olmak üzere, teknik ve organizasyonel tedbirler kullanılarak uygun güvenlik düzeyini sağlayacak şekilde işlemesi anlamına gelmektedir. GDPR'da "Kişisel verilerin işlenmesine ilişkin ilkeler" başlığı altında sayılan bir ilke olsa da esasen veri güvenliğinin veri sorumluları tarafından tesis edilmesine ilişkin bir düzenlemedir[154].

2.8. Hesap Verebilirlik

Hesap verebilirlik ilkesi (*accountability*) Kanun ve 95/46/EC Sayılı Direktif'te düzenlenmeyip GDPR'ın m. 5/2'de düzenlenmiş bir ilkedir. Bu ilke ile veri sorumlularının GDPR m. 5/1'de sayılan (bu başlıktan önceki başlıklarda açıklanan) altı adet ilkeye uygun şekilde davranması gerektiği ve bu ilkelerden sorumlu oldukları ifade edilmiştir. Bu ilke ile veri sorumlularına yükümlülüklerini yerine getirip getirmediği noktasında bir ispat yükü yüklendiği söylenebilir.

Kanunun getirdiği sistematik açısından hesap verebilirlik ilkesinin veri sorumluları açısından karşılandığının göstergesi kişisel veri envanterinin hazırlanması, ayrıca usulüne uygun olarak kabul ve ilan edilmiş kişisel veri koruma politikasına sahip olunmasıdır[155]. Yine Kanundan doğan diğer yükümlülüklerin ifası amacıyla atılan adımların kayıt altında tutulması aynı amaca hizmet etmektedir.

---

[154] **Dülger**, s. 209.
[155] **Dülger**, s. 210.

3. KİŞİSEL VERİLERİN İŞLENME ŞARTLARI

Bu başlık altında kişisel verilerin işlenmesine ilişkin kurallar ve çeşitli düzenlemeler anlatılacaktır. Açıklamalarımızı yaparken ağırlıklı olarak Kanundaki düzenlemelerin üzerinde duracağız ve gerekli gördüğümüz noktalarda konuyu GDPR ve 95/46/EC Sayılı Direktif'teki düzenlemelerle karşılaştırmalı olarak açıklayacağız.

3.1. Genel Olarak

Kişisel verilerin işlenmesine ilişkin ulusal ve uluslararası düzenlemelerde yapılan çeşitli tanımlamalardan daha önceki bölümlerde bahsetmiştik[156]. Bu tanımlardan hareketle kişisel verinin ilk kez toplandığı andan başlayarak, bu toplama işlemi de dahil olmak üzere kişisel veri üzerinde yapılan her türlü işlem türlerinin bir veri işleme faaliyeti olduğu söylenebilir. Kişisel verilerin genel kural olarak, açık hükümle düzenlenmiş bir hukuka uygunluk sebebi bulunmadan işlenmesi hukuka aykırıdır[157].

3.2. Kişisel Verilerin İşlenme Şartları

Kişisel verilerin işlenmesine ilişkin şartlar, Kanunun 5. maddesinde düzenlenmiştir. Bu düzenlemeye göre aşağıda sayılı ve ilerleyen başlıklarda detaylı şekilde açıklayacağımız hallerden en az bir tanesinin bulunması durumunda ilgili kişinin kişisel verilerinin işlenmesi mümkün olacaktır:

- "*İlgili kişinin açık rızasının bulunması,*
- *Kanunlarda açıkça öngörülmesi,*
- *Fiili imkânsızlık sebebiyle rızasını açıklayamayacak durumda bulunan veya rızasına hukuki geçerlilik tanınmayan kişinin kendisinin ya da bir başkasının hayatı veya beden bütünlüğünün korunması için zorunlu olması,*

---

[156] Daha fazla bilgi için bkz. İkinci Bölüm 1.7. numaralı "Kişisel Verilerin İşlenmesi" başlığı

[157] **Işık Aslı Han**, "Kişisel Verilerin İşlenmesi Bağlamında Hukuka Uygunluk Sebebi Olarak Veri Sahibinin Rızası", Galatasaray Üniversitesi Hukuk Fakültesi Dergisi, Cilt 1, Sayı 1, s. 417-459, 2019, s. 433.

- *Bir sözleşmenin kurulması veya ifasıyla doğrudan ilişkili olması kaydıyla sözleşmenin taraflarına ait kişisel verilerin işlenmesinin gerekli olması,*
- *Veri sorumlusunun hukuki yükümlülüğünü yerine getirebilmesi için zorunlu olması,*
- *İlgili kişinin kendisi tarafından alenileştirilmiş olması,*
- *Bir hakkın tesisi, kullanılması veya korunması için veri işlemenin zorunlu olması,*
- *İlgili kişinin temel hak ve özgürlüklerine zarar vermemek kaydıyla, veri sorumlusunun meşru menfaatleri için veri işlenmesinin zorunlu olması*"

Kişisel verilerin işlenme şartları, diğer bir ifadeyle hukuka uygunluk sebepleri, Kanunda sınırlı sayıda sayıldığı için bu şartların genişletilmesi mümkün değildir[158].

Kanunun 4. maddesi uyarınca; "kişisel verilerin işlenmesinde; hukuka ve dürüstlük kurallarına uygun olma, doğru ve gerektiğinde güncel olma, belirli, açık ve meşru amaçlar için işlenme, işlendikleri amaçla bağlantılı, sınırlı ve ölçülü olma, ilgili mevzuatta öngörülen veya işlendikleri amaç için gerekli olan süre kadar muhafaza edilme ilkelerine" uyulmasının zorunlu olduğu düzenlenmiştir. Dolayısıyla sayılan bu genel ilkeler kişisel veri işleme faaliyetinin her aşamasında dikkate alınmalıdır, zira salt hukuka uygunluk sebebinin tek başına varlığı kişisel verileri işlenmesi için yeterli olmayıp Kanunun 4. Maddesi uyarınca temel ilkelere de uyulması zorunludur.

Kişisel veri işleme faaliyeti, yukarıda sayılı şartlardan açık rıza dışındaki bir şarta dayanması durumunda ilgili kişinin açık rızası olmadan kişisel veriler işlenebilecektir. Bu sebeple kişisel verilerin işlenme şartlarına ilişkin açıklamalarımızı yaparken konuyu ilgili kişinin açık rızasının bulunması hali ve açık rızanın aranmadığı haller olarak ikiye ayırarak inceleyeceğiz.

---

[158] Bkz. Anayasa m. 20/3; "*(...) Kişisel veriler, ancak kanunda öngörülen hallerde veya kişinin açık rızasıyla işlenebilir. Kişisel verilerin korunmasına ilişkin esas ve usuller kanunla düzenlenir.*"

3.2.1. İlgili Kişinin Açık Rızasının Bulunması

Kişisel verilerin işlenmesinde en temel hukuka uygunluk sebeplerinden olan rızanın varlığı halinde ilgili kişinin verilerinin hukuka uygun olarak işlenebilmesi mümkündür[159][160].

Kurumun yayınladığı "Kişisel Verilerin İşlenme Şartları Rehberi[161]"nde de belirtildiği üzere veri sorumlusu tarafından gerçekleştirilecek bir veri işleme faaliyetinden önce ilk olarak Kanunda düzenlenen veri işlemeye ilişkin şartlardan açık rıza dışındaki şartlardan birinin var olup olmadığı tespit edilmelidir. Eğer veri işleme faaliyeti Kanunda düzenlenen açık rıza dışındaki herhangi bir şarta dayandırılamıyor ise bu durumda ilgili kişinin açık rızasını alma yoluna gidilmelidir. Dolayısıyla Kanundaki açık rıza dışındaki veri işleme şartlarından biri veya birkaçının varlığı halinde, ilgili kişiden açık rıza alınmadan veri işleme faaliyeti yapılabilecekken yine de ilgili kişiden açık rıza beyanı alınması yanlış bir uygulamadır[162]. Bu durum uygulamada *rıza kirliliği* olarak da adlandırılmaktadır. Kişisel Verileri Koruma Kurulu'nun bu doğrultuda verdiği 08.07.2019 tarihli ve 2019/206 sayılı kararında konuyla ilgili olarak; "(…) *kişisel veri işleme faaliyetinin, Kanunda bulunan* ***açık rıza dışındaki şartlardan birine dayanıyorsa****, bu durumda* ***ilgili kişiden açık rıza alınmasına gerek bulunmadığı*** *ve veri işleme faaliyetinin,* ***açık rıza dışında bir dayanakla yürütülmesi mümkün iken açık rızaya dayandırılmasının, aldatıcı ve hakkın kötüye kullanımı niteliğinde olacağı****; nitekim ilgili kişi tarafından verilen açık rızanın geri alınması halinde veri sorumlusunun diğer kişisel veri işleme şartlarından birine dayalı olarak veri işleme faaliyetini sürdürmesinin hukuka ve dürüstlük kurallarına aykırı işlem yapılması anlamına geleceği* (…)" saptamalarında bulunmuştur. Ancak açık rıza dışındaki şartların var olmasına rağmen, veri sorumlusu tarafından bu şartların dışındaki

---

[159] Han, s. 434.

[160] Açık rıza kavramına ilişkin detaylı açıklamalarımız için İkinci Bölümün 1.5. numaralı ve "Açık Rıza" başlıklı kısma bakabilirsiniz.

[161] **Kişisel Verileri Koruma Kurumu**, Kişisel Verilerin İşlenme Şartları Rehberi, (Çevrimiçi) https://www.kvkk.gov.tr/SharedFolderServer/CMSFiles/8c90423f-97ea-4d81-a7c1-ace74295c2b8.pdf Erişim Tarihi: 4 Mart 2020, s. 6.

[162] **Kişisel Verileri Koruma Kurumu**, Kişisel Verilerin Korunması Hakkında Sıkça Sorulan Sorular, KVKK Yayınları, Ankara 2018, (Çevrimiçi) https://www.kvkk.gov.tr/Icerik/4196/Kisisel-Verilerin-Korunmasi-Kanunu-Hakkinda-Sikca-Sorulan-Sorular Erişim Tarihi: 27 Mart 2020, s. 25.

amaçlar doğrultusunda işlenecek veriler için ilgili kişiden açık rıza alınması gerekecektir[163].

İlgili kişiden açık rıza alınması her şart ve koşulda veri işleme faaliyetini hukuka uygun hale getirmez. Veri sorumluları, çalışmamızın önceki başlıklarında açıkladığımız kişisel verilerin işlenmesine ilişkin temel ilkelere daima uymakla yükümlüdürler. Bu sebeple örneğin ilgili kişiden açık rıza alınmasına rağmen veri sorumlusu tarafından veri işleme amacının sınırlarının net bir şekilde çizilmiş ve belirlenmiş olmaması durumu veri işleme ilkelerinden "*belirli, açık ve meşru amaçlar için işlenme*" ilkesine aykırılık teşkil edeceğinden bu veri işleme faaliyeti Kanuna aykırı olacaktır.

3.2.2. Açık Rızanın Aranmadığı Haller

3.2.2.1. Kanunlarda Açıkça Öngörülmesi

Kanun uyarınca açık rızanın aranmadığı veri işleme şartlarından ilki kanunlarda açıkça öngörülmesi şartıdır. Bu şartın varlığı için kanunlar tarafından veri sorumlusuna veri işleme faaliyeti yapması için bir yükümlülük tanımlanması veya yetki verilmesi gerekmektedir. Böylece veri sorumlusu kanunlarda açıkça öngörülen durumlarda ilgili kişinin açık rızasını almadan veri işleme faaliyeti yapabilecektir. Bu şartın var olduğu kanunlara ilişkin bazı örnekler aşağıdaki gibidir:

- 4857 sayılı İş Kanunu uyarınca işveren tarafından işçiye ilişkin özlük dosyasının tutulması
- 2559 sayılı Polis Vazife ve Salahiyet Kanunu uyarınca polis tarafından şüphelilerin parmak izlerinin alınması
- 5352 sayılı Adli Sicil Kanunu uyarınca Adalet Bakanlığı tarafından kişilere ilişkin ceza mahkûmiyet bilgilerini işlenmesi
- 5464 sayılı Banka Kartları ve Kredi Kartları Kanunu uyarınca kredi kartı çıkaran kuruluşlar, kredi kartı almak isteyen kişilerin sosyal ve

[163] **Dülger**, s. 288.

ekonomik durumlarına ilişkin verilerini dikkate alarak kişilere sağlanacak kullanım limitlerini tespit etmek zorundadır.

- 6102 sayılı Türk Ticaret Kanunu uyarınca şirket genel kurul toplantılarında hazır bulunan kişilerin listesi (*hazirun cetveli*) tutulur.

Kanunlarda açıkça öngörülmesi şartı 95/46/EC sayılı Direktif ve GDPR'da düzenlenmemiştir. Kanundaki şartın tam karşılığı olmasa da GDPR'ın m. 6/1-e hükmü uyarınca; "*işlemenin kamu yararı için gerçekleştirilen bir görevin ifası için zorunlu olması veya veri sorumlusunun resmi yetkisini kullanması bağlamında gerekli olması*" hukuka uygun bir şekilde kişisel veri işlemenin şartlarından birisi olarak düzenlenmiştir.

3.2.2.2. Fiili İmkânsızlık Nedeniyle Rızasını Açıklayamayacak Durumda Bulunan veya Rızasına Hukuki Geçerlilik Tanınmayan Kişinin Kendisinin ya da Bir Başkasının Hayatı veya Beden Bütünlüğünün Korunması İçin Zorunlu Olması

Kanunun m. 5/2-b hükmü uyarınca; veri sorumlularına açık rıza aranmaksızın kişisel veri işleme imkânı tanıyan bu şarttan söz edebilmek için öncelikle ilgili kişinin fiili imkânsızlık sebebiyle rızasını açıklayamayacak durumda olması veya rızasına hukuki anlamda geçerlilik tanınmayan kişinin, kendisinin veya bir başkasının hayatının veya beden bütünlüğünün korunması için kişisel veri işleme faaliyetinin zorunlu olması gereklidir. Örneğin; TMK m. 23 çerçevesinde üstün özel yarar olarak da adlandırabileceğimiz bu şart uyarınca hayati tehlike içinde kaybolan bir kişinin yerinin bulunarak kurtarılabilmesi amacıyla kendisine ait telefon, bilgisayar veya kredi kartının kullanım veya son bulunduğu yerin tespit edilebilmesi için konum verilerinin açık rızası olmadan işlenebilmesi mümkün olacaktır.

3.2.2.3. Bir Sözleşmenin Kurulması veya İfasıyla Doğrudan Doğruya İlgili Olması Kaydıyla, Sözleşmenin Taraflarına Ait Kişisel Verilerin İşlenmesinin Gerekli Olması

Hiç şüphesiz sözleşmelerin hem kurulması hem de ifası aşamasında birtakım kişisel verilere ihtiyaç duyulacaktır. Bu bağlamda sözleşmelerin sağlıklı ve hukuken geçerli şekilde kurulabilmeleri ve yürürlükte kaldığı müddetçe etkilerini doğurabilmesi için veri koruma mevzuatlarında sözleşmelerin kurulması ve ifasıyla ilgili olmak üzere veri işleme faaliyeti bir hukuka uygunluk sebebi olarak düzenlenmiştir. Örneğin bir banka ile kredi sözleşmesi imzalayarak kredi almayı talep eden kişi ile ilgili bankanın o kişiye ait maaş bordrolarını, tapu kayıtlarını edinmesi sırasında toplanan kişisel veriler bahsi geçen kredi sözleşmesinin kurulması ile ilgili olduğu müddetçe ilgili kişinin açık rızasının alınmasına ihtiyaç duyulmayacaktır[164]; bir emlakçının kira sözleşmesi ile ilgili olarak kiracı ve ev sahibi arasında kurulacak sözleşme kapsamında tarafların kimlik numarası, banka hesap bilgisi, adres, telefon, imza gibi kişisel verilerini elde edip işlemesi veya taraflar arasında kurulan satış sözleşmesi uyarınca satıcının satılan malı alıcıya gönderebilmek için alıcının adresini kargo şirketine vermesi gibi durumlarda ilgili kişinin kişisel verilerinin işlenebilmesi için açık rıza aranmayacaktır[165].

Kanunun m. 5/2-c hükmü uyarınca; kişisel veri işleme faaliyeti sözleşmenin kurulması veya tarafların sözleşmeden kaynaklı yükümlülüklerini yerine getirmesi (ifası) ile doğrudan doğruya ilgili olmak kaydıyla sözleşmenin taraflarına ait verilerin veri sorumluları tarafından işlenmesinin gerektiği durumlarda bu veriler, ilgili kişinin açık rızası olmadan da işlenebilecektir.

Bu şart hem Direktif hem de GDPR'da benzer şekilde yer almaktadır. GDPR'ın m. 6/1-b hükmü uyarınca; ilgili kişinin (*veri süjesi*) taraf olduğu bir sözleşmenin ifası veya bir sözleşme yapılmadan önce ilgili kişinin talebi

---

[164] Bkz. Kanunun 5. maddesinin gerekçesi.

[165] **Kişisel Verilerin Korunması Kurumu**, Örneklerle Kişisel Verilerin Korunması, KVKK Yayınları No: 29, Ankara 2019, (Çevrimiçi) https://www.kvkk.gov.tr/Icerik/5521/Orneklerle-Kisisel-Verilerin-Korunmasi-Dokumani-Kurum-Internet-Sayfasinda-Yayinlanmistir- Erişim Tarihi: 4 Mart 2020, s. 13.

doğrultusunda adımlar atılması için veri işleme faaliyetinin gerekli olması durumunda yapılacak kişisel veri işleme faaliyeti hukuka uygun olacaktır.

3.2.2.4. Veri Sorumlusunun Hukuki Yükümlülüğünü Yerine Getirebilmesi İçin Zorunlu Olması

Kanunun m. 5/2-ç hükmü uyarınca; veri sorumlusu, kendisine yüklenmiş hukuki bir yükümlülüğünü yerine getirebilmek için kişisel veri işlemek zorunda ise yalnızca bu amaca özgü olarak ilgili kişinin açık rızası olmaksızın veri işleme faaliyetini yapabilir. Bunun için yalnızca veri sorumlusu üzerine hukuki bir yükümlülük yüklenmiş olması yeterli olmayıp bu hukuki yükümlülük gereği veri işleme faaliyetinin zorunlu olması gerekmektedir. Bu hukuki yükümlülükle ilgili veri sorumlusunun veri işleme faaliyeti hususunda bir takdir hakkının olması durumunda burada zorunluluk unsurunun var olmamasından hareketle açık rıza olmaksızın veri işleme faaliyetinin yapılması mümkün olmayacaktır.

Bu şart Kanundaki veri işleme şartlarından kanunlarda açıkça öngörülmesi ve sözleşmenin kurulması veya ifası için gerekli olma şartının dışındaki hukuki yükümlülükler için açık rıza olmaksızın veri işleme imkânı getirmiştir. Böylece kanunda açıkça öngörülmeyen veya sözleşmenin kurulması veya ifası için gerekli olmayan bir sebepten dolayı örneğin, Cumhurbaşkanlığı karar ya da kararnamesi, tüzük, yönetmelikte veya tebliğ hükümleri uyarınca veya bir mahkeme kararının yerine getirilmesi kapsamında talep edilen çalışanların işyeri giriş çıkış kayıtlarının veya güvenlik kamerası kayıtlarının mahkemeye gönderilmesi gibi durumlarda ilgili kişinin açık rızası olmadan veri işleme faaliyeti yapılması mümkün kılınmıştır[166].

GDPR'ın m. 6/1-c hükmü uyarınca Kanundaki gibi bu şartla benzer bir şekilde düzenleme yapılarak veri sorumlusunun hukuki bir yükümlülüğe uymak için kişisel veri işleme faaliyetinin zorunlu olması durumunda ilgili kişinin açık rızası olmaksızın veri işlemeye izin verilmiştir.

---

[166] **Dülger**, s. 298.

3.2.2.5. İlgili Kişinin Kendisi Tarafından Alenileştirilmiş Olması

Kanunun m. 5/2-d hükmü uyarınca; bir kişisel verinin ilgili kişinin kendisi tarafından alenileştirilmesi durumunda ilgili kişinin açık rızası olmadan bu kişisel verinin işlenmesi mümkün kılınmıştır. Bu şartla ilgili olarak Kanunun 5. maddesinin gerekçesinde ilgili kişinin kendisi tarafından alenileştirilen yani kamuya açılan ve herkes tarafından bilinebilecek hale gelen bir kişisel verinin işlenmesi durumunda, korunması gereken bir hukuki menfaat mevcut olmadığının üzerinde durulmuştur. Bu şartın en yaygın örneği ilgili kişinin kendisiyle ilgili ad, soyad, fotoğraf, iletişim bilgileri gibi verilerini internet üzerinden herkese açık şekilde paylaşmasıdır.

Burada dikkat edilmesi gereken husus kişisel verinin salt alenileştirilmiş olası şartın gerçekleşmesi için yeterli olmayıp ilgili kişisel verinin doğrudan ilgili kişinin kendisi tarafından alenileştirilmiş olması ve ilgili kişinin kişisel verisinin bu alenileştirme iradesi dışındaki herhangi bir amaç için işlenmemesi gerekmektedir[167]. Kanun koyucu burada öncelikle ilgili kişinin kendi kişisel verisini alenileştirilmesi yönündeki irade beyanını aramıştır. Yani ilgili kişinin başkaları tarafından alenileştirilen kişisel verilerinin ilgili kişinin açık rızası veya diğer işleme şartlarından en az biri mevcut olmadan işlenmesi mümkün olmayacaktır.

İlgili kişinin alenileştirme amacıyla ilgili olarak; ikinci el araç satan bir kişinin internet sitesine kendi iletişim bilgilerini girmesi bu iletişim bilgilerinin pazarlama faaliyetleri çerçevesinde kullanılmasını mümkün olmayacağı örneği verilebilir[168]. Zira burada kişi kendi iletişim bilgilerini internet sitesinden aracını satmak için olası alıcıların kendisine ulaşabilmesi adına paylaşmıştır. Dolayısıyla ilgili kişinin kendi kişisel verisi olan iletişim bilgilerini satış ilanının olduğu internet sitesinde kendisinin alenileştirildiğinden hareketle bu verilerin elde edilip başka amaçlar için kullanılması hukuka aykırıdır.

---

[167] **Dülger**, s. 301.
[168] Kişisel Verilerin İşlenme Şartları Rehberi, s. 11.

GDPR kapsamında özel nitelikli kişisel veriler dışında[169] ilgili kişinin kendisi tarafından alenileştirilmiş olması gibi bir veri işleme şartı düzenlenmemiştir.

3.2.2.6. Bir Hakkın Tesisi, Kullanılması veya Korunması İçin Veri İşlemenin Zorunlu Olması

Kanunun m. 5/2-e hükmü uyarınca; kişisel verilerin işlenmesi bir hakkın tesisi, kullanılması veya korunması için zorunlu olduğu durumlarda ilgili kişinin açık rızası alınmadan işlenebilir. Burada şartın veri işlemenin hakkın tesisi, kullanılması veya korunması için zorunlu olması unsuru önem arz etmektedir. Kanunun madde gerekçesinde bu şartla ilgili olarak "*bir şirketin kendi çalışanı tarafından açılan bir davada ispat için bazı verileri kullanması veya kısıtlı bir kişinin haklarının korunması amacıyla vasinin veya kayyımın, kısıtlının mali bilgilerini tutması*" örnekleri verilmiştir. Yine, mülkiyet veya intifa hakkının tesis edilebilmesi için tapu siciline bazı kişisel verilerin işlenmesi gerekecektir. Bu durumda ilgili kişiden açık rıza alınmasına gerek olmadan kişisel verilerin işlenmesi mümkündür.

Bu şartla ilgili doktrinde yapılan eleştirilerin başında tesis edilecek, kullanılacak veya korunacak hakkın kime ait olduğu noktasında ne Kanunun ilgili maddesinde ne de gerekçesinde herhangi bir açıklamaya yer verilmemiş olması gelmektedir[170]. Dolayısıyla hakkın yalnızca veri sorumlusu veya ilgili kişiye ait bir hak olması zorunlu olmayıp üçüncü kişilerin hakları bakımından da bu veri işleme şartının uygulanabileceğini söylemek mümkündür[171].

GDPR kapsamında yalnızca özel nitelikli kişisel veriler açısından böyle bir veri işleme şartı bulunmaktadır. Bu şart GDPR'ın sistematiğinde m. 6/1-f hükmünde düzenlenen meşru menfaat şartı kapsamında değerlendirilmektedir[172].

---

[169] **Article 29 Data Protection Working Party**, Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC, 9 Nisan 2014, 844/14/EN, WP217, (Çevrimiçi) https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp217_en.pdf Erişim Tarihi: 27 Nisan 2020, s. 39.
[170] **Şehriban İpek Aşıkoğlu**, Avrupa Birliği ve Türk Hukukunda Kişisel Verilerin Korunması ve Büyük Veri, 1. Baskı, On İki Levha Yayıncılık, İstanbul 2018, s. 133.
[171] **Dülger**, s. 304.
[172] **Dülger**, s. 305.

3.2.2.7. İlgili Kişinin Temel Hak ve Özgürlüklerine Zarar Vermemek Kaydıyla Veri Sorumlusunun Meşru Menfaatleri İçin Veri İşlemenin Zorunlu Olması

Kanunun m. 5/2-f hükmü uyarınca; veri sorumlusu kendi meşru menfaatleri için veri işlemenin zorunlu olduğu durumlarda, ilgili kişilerin temel hak ve özgürlüklerine zarar vermemek kaydıyla, açık rıza almadan veri işlemeleri mümkündür. Bu şart kapsamında veri işleme faaliyeti zorunlu olmalı ve ilgili kişilerin temel hak ve özgürlüklerine zarar vermemelidir. Dolayısıyla şartın bu iki unsuru gözetilmezse veri sorumlusunun salt meşru menfaatinin bulunması veri işleme faaliyetini hukuka uygun hale getirmeyecektir. Ayrıca her türlü insan hak ve özgürlüklerinde olduğu gibi bu şartın uygulanması kapsamında yapılacak sınırlamalar dar yorumlanmalı; veri sorumlusu tarafından bu şart kapsamında veri işlenmemesi kural, işlenmesi ise istisna olmalıdır[173]. Örneğin işyerlerinde çalışanların işe giriş çıkış kayıtlarının tutulabilmesi için işverenin yönetim yetkisi dahilinde çalışanlardan işe giriş ve çıkış saatlerinde imza alınması veya kartlı takip sistemine işyeri kimlik kartlarının okutulmasının istenmesi; bir ticari işletme veya şirketin satılması, birleşmesi veya devralınması gibi işlemlerde alıcı tarafın şirket bünyesindeki çalışanlara ilişkin birtakım verileri incelemesi gibi durumlarda bu şartın var olduğu ve bu sebeple ilgili kişinin açık rıza olmaksızın veri işleme faaliyetinin yapılmasının mümkün olduğu söylenebilir.

Maalesef uygulamada herhangi başka bir veri işleme şartının bulunmadığı durumlarda veri sorumlularının sıklıkla meşru menfaat şartını kullanmaya çalıştıklarını görmekteyiz. Kişisel Verileri Koruma Kurulu'nun 25.03.2019 tarihli ve 2019/78 sayılı kararına[174] göre bu şartın var olup olmadığının tespiti yapılırken aşağıdaki hususlara dikkat edilmesi gerekmektedir:

- "*Kişisel verinin işlenmesi sonucunda elde edilecek menfaat ile ilgili kişinin temel hak ve hürriyetlerinin yarışabilir düzeyde olması,*

[173] **Şimşek**, s. 208; **Küzeci**, s. 350.
[174] Kişisel Verileri Koruma Kurulu'nun 25.03.2019 tarihli ve 2019/78 sayılı kararına şu uzantıdan ulaşabilirsiniz: https://www.kvkk.gov.tr/Icerik/5434/2019-78 Erişim Tarihi: 4 Mart 2020.

- *Söz konusu menfaate ulaşılabilmesi bakımından kişisel veri işlenmesinin zorunluluk arz etmesi,*
- *Meşru menfaatin halihazırda mevcut, belirli ve açık olması,*
- *İlgili kişinin temel hak ve hürriyetleri ile yarışabilir nitelikte olan meşru menfaatin elde edilmesi halinde bir yarar sağlanacak olması ve kişisel veri işlenmeksizin başkaca bir yol ve yöntemle bu yararın ortaya çıkmasının mümkün olmaması,*
- *Meşru menfaat belirlenirken söz konusu yararın çok sayıda kişiyi etkilemesi, yalnızca kâr elde edilmesi ya da ekonomik yararın sağlanması amacına yönelik olmaması, iş süreçlerini ya da bir işleyişi kolaylaştırması (örneğin bir birim ya da az sayıda personel nezdinde değil, kurumsal olarak geneli etkileyecek şekilde) gibi şeffaf ve hesap verilebilir nitelikleri haiz kriterlerin esas alınması,*
- *Bu açıdan ilgili kişinin başta kişisel verilerinin korunması olmak üzere temel hak ve hürriyetlerinin zarar görmesini engellemek amacıyla öngörülebilir, açık ve yakın her türlü tehlikeden uzak tutulması,*
- *Kişisel verilerin bir veri kayıt sisteminde amaçla sınırlı olarak hukuka uygun işleyişinin temini ile zararı ve ihlalleri engellemek için her türlü teknik ve idari tedbirin alınması,*
- *Kişisel verilerin işlenmesinde genel ilkelere uygunluğun sağlanması,*
- *Bu kapsamda, kişinin temel hak ve hürriyetleri ile veri sorumlusunun meşru menfaatinin karşılaştırılarak denge testinin yapılması*

hususlarının değerlendirilmesi gerektiği,

Öte yandan, kişisel verilerin ilk kez işlenmesi için gereken amaçtan farklı olarak başka bir amaca yönelik yeni bir veri işleme faaliyetinin gerçekleştirilmesinin, Kanunun 5 inci maddesinde sayılan veri işleme şartlarından en az birine dayanması ve ilk amaçtan bağımsız olarak Kanunun 4 üncü maddesinde sayılan kişisel verilerin işlenmesinde aranan ilkelerin tümüne uyumlu olması gerektiği"

Yukarıda da görüleceği üzere Kurul meşru menfaat şartının kullanılabilmesi için detaylı bir değerlendirme yapılması gerektiğini belirtmiştir. Nitekim Kurumun yayınladığı Kişisel Verilerin İşlenme Şartları Rehberi'nde meşru menfaat şartının Kanundaki diğer veri işleme şartlarının somut olayda uygulanamadığı hallerde başvurulacak bir son çare olarak algılanmaması gerektiğini, bu şartın tüm kişisel verileri kendi kapsamına dahil edebilecek bir hukuki düzenleme olmadığının altı çizilmiştir[175].

Direktif'in m. 7/1-f ve GDPR'ın m. 6/1-f hükümlerinde bu şarta benzer bir şekilde veri sorumlularının meşru menfaati bir veri işleme şartı olarak düzenlenmiştir.

3.3. Özel Nitelikli Kişisel Verilerin İşlenme Şartları

3.3.1. Genel Olarak

Özel nitelikli kişisel verilerin işlenme şartları Avrupa'daki düzenlemelere paralel şekilde, genel nitelikli yani özel nitelikli olmayan verilerden farklılık göstermektedir[176]. Buna ilişkin düzenleme Kanunun "Özel nitelikli kişisel verilerin işlenme şartları" başlıklı 6. maddesinde yapılmıştır.

Kanunun toplam dört fıkradan oluşan 6. maddesinin ilk fıkrasında özel nitelikli kişisel veriler sayıldıktan sonra maddenin diğer fıkralarında özel nitelikli kişisel verilerin işlenme şartlarına ilişkin kurallar düzenlenmiştir. Kanunun m. 6/1 hükmü uyarınca;

- "*Kişilerin ırkı, etnik kökeni*
- *Siyasi düşüncesi, felsefi inancı*
- *Dini, mezhebi veya diğer inançları*
- *Kılık ve kıyafeti*
- *Dernek, vakıf ya da sendika üyeliği*
- *Sağlığı*

---

[175] Kişisel Verilerin İşlenme Şartları Rehberi, s. 17.

[176] Özel nitelikli kişisel verilerin tanımına ilişkin açıklamalarımız için çalışmamızın İkinci Bölüm'ündeki 1.3. numaralı başlığını inceleyebilirsiniz. Bu başlık altında özel nitelikli kişisel verilerin tanımına ilişkin açıklamalar tekrara düşmemek adına yapılmamıştır.

- *Cinsel hayatı*
- *Ceza mahkûmiyeti ve güvenlik tedbirleriyle ilgili verileri*
- *Biyometrik ve genetik verileri*"

olarak sınırlı sayıda (*numerus clausus*) sayılan bu veri türleri özel nitelikli kişisel veri türleridir.

Özel nitelikli kişisel verilerin işlenme şartlarına ilişkin kuralların düzenlendiği Kanunun m. 6/2, 3 ve 4. hükümleri aşağıdaki gibidir:

> "*(2) Özel nitelikli kişisel verilerin, ilgilinin açık rızası olmaksızın işlenmesi yasaktır.*
>
> *(3) Birinci fıkrada sayılan sağlık ve cinsel hayat dışındaki kişisel veriler, kanunlarda öngörülen hâllerde ilgili kişinin açık rızası aranmaksızın işlenebilir. Sağlık ve cinsel hayata ilişkin kişisel veriler ise ancak kamu sağlığının korunması, koruyucu hekimlik, tıbbî teşhis, tedavi ve bakım hizmetlerinin yürütülmesi, sağlık hizmetleri ile finansmanının planlanması ve yönetimi amacıyla, sır saklama yükümlülüğü altında bulunan kişiler veya yetkili kurum ve kuruluşlar tarafından ilgilinin açık rızası aranmaksızın işlenebilir.*
>
> *(4) Özel nitelikli kişisel verilerin işlenmesinde, ayrıca Kurul tarafından belirlenen yeterli önlemlerin alınması şarttır.*"

Yukarıda alıntılanan düzenleme incelendiğinde ilk göze çarpan husus açık rıza kavramının özel nitelikli kişisel verilerin işlenmesinde kanun koyucu tarafından bir hukuka uygunluk sebebi olarak düzenlenmiş olmasıdır. Fıkra kapsamında ilgili kişinin açık rızası olmaksızın özel nitelikli kişisel verilerin işlenmesinin açıkça yasak olduğu düzenlenmiştir. Açık rıza kavramına ilişkin yaptığımız önceki açıklamalarımız özel nitelikli kişisel veriler açısından da geçerlidir.

Kanunun m. 6/3 hükmü uyarınca açık rıza aranmaksızın özel nitelikli kişisel verilerin işlenmesinin mümkün olduğu durumlar, sağlık ve cinsel hayata ilişkin veriler ile sağlık ve cinsel hayat dışındaki verilerin işlenme şartları olmak üzere ikili bir ayrıma gidilerek düzenlenmiştir. Böylece Kanun, sağlık ve cinsel hayata ilişkin verileri diğer grup özel nitelikli kişisel verilerden ayrı bir veri işleme rejimine tabi

kılmıştır. Bu ayrım, kanun koyucu tarafından sağlık ve cinsel hayata ilişkin verilere atfedilen önemin bir göstergesidir. Nitekim Kanunun m. 6/4 hükmü uyarınca özel nitelikli kişisel verilerin işlenmesine ilişkin, ayrıca Kişisel Verileri Koruma Kurulu tarafından belirlenen yeterli önlemlerin yerine getirilmesi şartı düzenlenmiştir. Kurul tarafından bu doğrultuda alınan 31.01.2018 tarihli ve 2018/10 numaralı karar ile birlikte "Özel Nitelikli Kişisel Verilerin İşlenmesinde Veri Sorumlularınca Alınması Gereken Yeterli Önlemler[177]" belirlenmiştir. Bu önlemler çalışmamızın Üçüncü Bölüm'ünün Veri Güvenliğine İlişkin Yükümlülükler başlığı altında detaylı şekilde açıklanmıştır[178].

3.3.2. Sağlık ve Cinsel Hayat Dışındaki Verilerin İşlenme Şartları

Kanunun m. 6/3 hükmünün birinci cümlesi uyarınca sağlık ve cinsel hayata ilişkin verilerin dışında kalan özel nitelikli kişisel veriler[179] yalnızca kanunlarda öngörülen hallerde ilgili kişinin açık rızası olmaksızın işlenebilecektir. Buna ek olarak ikinci bir veri işleme şartı ilgili kişinin açık rızasının bulunmasıdır; açık rızanın varlığı halinde sağlık ve cinsel hayat dışındaki kişisel verilerin işlenmesi mümkündür. Bu iki veri işleme şartı dışında, bahsi geçen veri türlerini hukuka uygun şekilde işlemeye izin veren başkaca bir veri işleme şartı düzenlenmemiştir.

Bu veri işleme şartı uyarınca örneğin çalışanların sendika üyelik bilgilerinin 4857 sayılı İş Kanunu uyarınca özlük dosyasında tutulması veya 2559 sayılı Polis Vazife ve Salahiyet Kanunu uyarınca polis tarafından göz altına alınan kişinin bir biyometrik verisi olan parmak izinin alınması mümkündür.

---

[177] Kurul'un "Özel Nitelikli Kişisel Verilerin İşlenmesinde Veri Sorumlularınca Alınması Gereken Yeterli Önlemler"i içeren 31.01.2018 tarihli ve 2018/10 numaralı kararına şu uzantıdan ulaşabilirsiniz: https://www.kvkk.gov.tr/Icerik/4110/2018-10 Erişim Tarihi: 5 Mart 2020.

[178] Bkz. Üçüncü Bölüm, 3.2. numaralı "Veri Güvenliğine İlişkin İdari Tedbirler" başlığı

[179] Kanunun 6. maddesinde belirtildiği üzere, sağlık ve cinsel hayata ilişkin verilerin dışında kalan özel nitelikli kişisel veriler; kişilerin ırkı, etnik kökeni, siyasi düşüncesi, felsefi inancı, dini, mezhebi veya diğer inançları, kılık ve kıyafeti, dernek, vakıf ya da sendika üyeliği, ceza mahkûmiyeti ve güvenlik tedbirleriyle ilgili verileri, biyometrik ve genetik verilerdir.

3.3.3. Sağlık ve Cinsel Hayata İlişkin Kişisel Verilerin İşlenme Şartları

Kanunun m. 6/3 hükmünün ikinci cümlesi uyarınca; "sağlık ve cinsel hayata ilişkin verilerin yalnızca kamu sağlığının korunması, koruyucu hekimlik, tıbbî teşhis, tedavi ve bakım hizmetlerinin yürütülmesi, sağlık hizmetleri ile finansmanının planlanması ve yönetimi amacıyla, sır saklama yükümlülüğü altında bulunan kişiler veya yetkili kurum ve kuruluşlar tarafından ilgilinin açık rızası aranmaksızın işlenebileceği" düzenlenmiştir. Bu sayılan hallerin dışında ilgili kişinin açık rızasını alarak da sağlık ve cinsel hayata ilişkin kişisel verilerin işlenmesi mümkün olup, bunlar dışında sağlık ve cinsel hayata ilişkin kişisel verilerinin Kanuna uygun şekilde işlenmesi mümkün değildir.

Burada önem arz eden husus sağlık ve cinsel hayata ilişkin kişisel verilere ilişkin işleme şartının bulunması durumunda bu veri işleme faaliyetini yalnızca sır saklama yükümlülüğü altında bulunan kişiler veya yetkili kurum ve kuruluşlar yapabileceklerdir. Diğer bir ifadeyle bu sayılanların dışındaki kişi, kurum veya kuruşların sağlık ve cinsel hayata ilişkin kişisel verileri işlemesi Kanuna göre hiçbir şekilde mümkün değildir.

Hukukumuzda sır saklama yükümlülüğü altındaki kişilere örnek olarak hekimler, diş hekimleri, eczacılar, avukatlar, noterler, mali müşavirler gösterilebilir. Sağlık ve cinsel hayata ilişkin kişisel verilerin işlenmesi bağlamında daha çok hekimler ve diğer sağlık çalışanları öne çıkmaktadır. Hekimlerin tabi olduğu sır saklama yükümlülükleri kendi yanlarında çalışanları ve diğer sağlık çalışanlarını da kapsamaktadır[180]. Hekimler, diş hekimleri, eczacılar, ebeler ile bu sayılanların yardımcıları ve tüm diğer tıbbi meslek veya sanat mensupları sır saklama yükümlülüğüne tabidir[181].

Bu veri işleme şartına örnek olarak hastanelerin ve doktorların hastalarına ilişkin verileri işlemesi verilebilir.

---

[180] **Dülger**, s. 316.
[181] **Faruk Erem**, "Ceza Hukukunda Meslek Sırrı", Ankara Üniversitesi Hukuk Fakültesi Dergisi, Cilt 1, No:1, 1943, s. 44.

3.4. Kişisel Verilerin Aktarılması

3.4.1. Genel Olarak

Kişisel verilerin aktarılması veya transfer edilmesi bir veri işleme şeklidir. GDPR'da ve Direktif'te kişisel verilerin üçüncü kişilere aktarılmasına ilişkin özel düzenleme yapılması yoluna gidilmeyip, diğer veri işleme faaliyetleri gibi genel veri işleme şartlarına tabi kılınmıştır. Ancak Kanunda kişisel verilerin aktarılması kavramı; kişisel verilerin yurtiçinde aktarılması ve yurt dışına aktarılması olarak iki başlık altında düzenlenmiştir.

3.4.2. Kişisel Verilerin Yurt İçinde Aktarılması

Kanunun, kişisel verilerin yurt içinde üçüncü kişilere aktarılmasını düzenleyen "Kişisel verilerin aktarılması" başlıklı 8. Maddesi aşağıdaki gibidir:

> "*(1) Kişisel veriler, ilgili kişinin açık rızası olmaksızın aktarılamaz.*
>
> *(2) Kişisel veriler;*
>
> *a) 5 inci maddenin ikinci fıkrasında,*
>
> *b) Yeterli önlemler alınmak kaydıyla, 6 ncı maddenin üçüncü fıkrasında,*
>
> *belirtilen şartlardan birinin bulunması hâlinde, ilgili kişinin açık rızası aranmaksızın aktarılabilir.*
>
> *(3) Kişisel verilerin aktarılmasına ilişkin diğer kanunlarda yer alan hükümler saklıdır.*"

Genel kural olarak ilgili kişinin açık rızası olmaksızın kişisel verilerin yurt içinde üçüncü kişilere aktarılamayacağı düzenlenmiştir. Diğer bir ifadeyle açık rızanın varlığının kişisel verilerin yurt içinde üçüncü kişilere aktarılması noktasında bir hukuka uygunluk sebebi olduğu söylenebilecektir. Madde içeriğinde görüldüğü üzere kişisel verilerin aktarılmasına ilişkin şartları belirlerken doğrudan genel nitelikli kişisel verilerin işlenme şartlarının düzenlendiği m. 5/2 ile özel nitelikli kişisel verilerin işlenme şartlarının düzenlendiği m. 6/3'e atıf yapılarak bu şartlardan birisinin bulunması halinde yurt içinde veri aktarımının ilgili kişinin açık rızası bulunmadan yapılabilmesine izin verilmiştir. Diğer bir ifadeyle aşağıdaki

seçeneklerden birinin var olması durumunda veri sorumluları, ilgili kişinin açık rızasını almadan genel nitelikli kişisel verileri ve yeterli önlemleri almak şartıyla özel nitelikli kişisel verileri yurt içinde üçüncü kişilere aktarabileceklerdir:

i. Kanunun m. 5/2 hükmü uyarınca açık rıza aranmaksızın genel nitelikli kişisel verilerin işlenmesine olanak veren hallerden en az bir tanesinin bulunması

ii. Kanunun m. 6/3-1. cümlesi uyarınca; "sağlık ve cinsel hayat dışındaki kişisel veriler için kanunlarda öngörülen bir durumun olması"

iii. Kanunun m. 6/3-2. cümlesi uyarınca; "sağlık ve cinsel hayata ilişkin kişisel veriler için ise ancak kamu sağlığının korunması, koruyucu hekimlik, tıbbî teşhis, tedavi ve bakım hizmetlerinin yürütülmesi, sağlık hizmetleri ile finansmanının planlanması ve yönetimi amacıyla, sır saklama yükümlülüğü altında bulunan kişiler veya yetkili kurum ve kuruluşlar tarafından işlenmesi"

Genel ve özel nitelikli kişisel verilerin işlenme şartlarına ilişkin önceki başlıklarda yaptığımız açıklamalarımız, kişisel verilerin yurt içinde aktarılmasına ilişkin şartlar bakımından da geçerlidir.

Kanunun m. 6/4 hükmündeki "*Özel nitelikli kişisel verilerin işlenmesinde, ayrıca Kurul tarafından belirlenen yeterli önlemlerin alınması şarttır*" düzenlemesi kapsamında Kurul'un 31.01.2018 tarihli ve 2018/10 sayılı kararı ile "Özel Nitelikli Kişisel Verilerin İşlenmesinde Veri Sorumlularınca Alınması Gereken Yeterli Önlemler[182]" düzenlenmiştir. Bu bağlamda incelediğimiz başlıkla ilgili olarak özel nitelikli kişisel veriler aktarılacaksa bahsi geçen Kurul kararı uyarınca;

> *i.* "*Verilerin e-posta yoluyla aktarılması gerekiyorsa şifreli olarak kurumsal e-posta adresiyle veya Kayıtlı Elektronik Posta (KEP) hesabı kullanılarak aktarılması,*"

[182] Kurul'un "Özel Nitelikli Kişisel Verilerin İşlenmesinde Veri Sorumlularınca Alınması Gereken Yeterli Önlemler" hakkındaki 31.01.2018 tarihli ve 2018/10 sayılı kararına şu uzantıdan ulaşabilirsiniz: https://www.kvkk.gov.tr/Icerik/4110/2018-10 Erişim Tarihi: 25 Mart 2020.

ii. "*CD, Taşınabilir Bellek, DVD gibi ortamlar yoluyla aktarılması gerekiyorsa kriptografik yöntemlerle şifrelenmesi ve kriptografik anahtarın farklı bir ortamda tutulması,*

iii. Farklı fiziksel ortamlarda bulunan sunucular arasında veri aktarımı gerçekleştiriliyorsa, sunucular arasında sFTP yöntemiyle veya VPN kurularak veri aktarımının gerçekleştirilmesi,

iv. Verilerin kâğıt ortamı yoluyla transfer edilmesi gerekiyorsa belgenin çalınması, kaybolması ya da yetkisiz kişilerce görülmesi gibi risklere karşı gerekli tedbirlerin alınması ve belgenin gizlilik dereceli belge formatında gönderilmesi"

gibi sayılan önlemlerin veri sorumluları tarafından alınması gerekmektedir.

Burada dikkat edilmesi gereken husus; özel nitelikli kişisel verilerin aktarılmasına ilişkin şartlardan (Kanun m. 6/3-1. cümle veya m. 6/3-2. cümle) birinin var olması halinde yukarıda alıntılanan önlemlere uyulması koşulu ile verilerin yurt dışındaki üçüncü kişilere aktarılması mümkün olduğudur. Diğer bir ifadeyle yeterli önlemlere uyulmadan yapılan veri aktarımları Kanuna aykırı bir veri işleme faaliyeti olarak görülecektir.

3.4.3. Kişisel Verilerin Yurt Dışına Aktarılması

3.4.3.1. Genel Olarak

Kanunun, kişisel verilerin yurt dışındaki üçüncü kişilere aktarılmasını düzenleyen "Kişisel verilerin yurt dışına aktarılması" başlıklı 9. maddesinin konuyla ilgili genel düzenlemelerin yapıldığı ilk üç fıkrası aşağıdaki gibidir:

"*(1) Kişisel veriler, ilgili kişinin açık rızası olmaksızın yurt dışına aktarılamaz.*

(2) Kişisel veriler, 5 inci maddenin ikinci fıkrası ile 6 ncı maddenin üçüncü fıkrasında belirtilen şartlardan birinin varlığı ve kişisel verinin aktarılacağı yabancı ülkede;

a) Yeterli korumanın bulunması,

b) Yeterli korumanın bulunmaması durumunda Türkiye'deki ve ilgili yabancı ülkedeki veri sorumlularının yeterli bir korumayı yazılı olarak taahhüt etmeleri ve Kurulun izninin bulunması,

kaydıyla ilgili kişinin açık rızası aranmaksızın yurt dışına aktarılabilir.

(3) Yeterli korumanın bulunduğu ülkeler Kurulca belirlenerek ilan edilir.

(...)"

Kanun koyucu tarafından kişisel verilerin ülke sınırları dışına aktarılması hususuna ayrı bir önem atfedilmiş ve bu bağlamda yurt dışına kişisel verilerin aktarılmasına ilişkin daha sıkı şartlar düzenlenmiştir.

Yukarıda alıntılanan Kanunun 9. maddesi uyarınca kişisel verilerin yurt dışına aktarımı;

i. "İlgili kişinin açık rızasının bulunması,

ii. Yeterli korumanın bulunduğu (*Kurul tarafından güvenli kabul edilen*) ülkelere veri aktarımı yapılacaksa Kanunda m. 5/2 ile m. 6/3 hükümlerinde belirtilen hallerin varlığı,

iii. Yeterli korumanın bulunmadığı ülkelere veri aktarımı yapılacaksa Kanunda m. 5/2 ile m. 6/3 hükümlerinde belirtilen hallerin varlığı, Türkiye'deki ve ilgili yabancı ülkedeki veri sorumlularınca yeterli korumanın yazılı olarak taahhüt edilmesi ve Kurulun izninin bulunması"

durumlarında yapılabilecektir.

Kişisel verilerin yurt dışına aktarılmasından bahsedebilmemiz için, kişisel verinin ülke sınırlar dışına çıkması yeterli olup verinin üçüncü kişilere aktarılması zorunlu bir şart değildir[183]. Bu kapsamda kişisel verilerin yurt dışına aktarılmasına örnek olarak; yurt dışı tabanlı bir e-mail sunucusu kullanan şirketin kişisel verileri bu e-mail sunucusunu kullanarak göndermesi durumunda kişisel veriler yurt dışında

[183] **Dülger**, s. 327.

bir üçüncü kişiye aktarılmamış olsa da kullanılan e-mail servisi yurt dışı tabanlı olduğu kişisel verilerin yurt dışına aktarılması söz konusudur[184].

Türkiye'deki veri sorumlusu ve ilgili yeterli korumanın bulunmadığı ülkedeki veri sorumluları veya veri işleyenler arasında kişisel veri aktarımı yapılabilmesi için yeterli korumanın yazılı olarak taahhüt edilmesi zorunludur. Bunun için bu kişiler Kurul tarafından "*Veri Sorumlusundan Veri Sorumlusuna Aktarım*" ve "*Veri Sorumlusundan Veri İşleyene Aktarım*" olmak üzere iki farklı taahhütname olarak hazırlanıp Kurulun internet sitesi üzerinden kullanıma sunulan[185] taahhütnamelerden uygun olanı doldurduktan sonra bu taahhütname ile birlikte Kurula başvurarak veri aktarımı için izin almalıdırlar.

Kişisel verilerin diğer kişi veya kurumlara aktarılması (transfer edilmesi) faaliyeti bir veri işleme faaliyetidir. Bu sebeple Direktif ve GDPR, kişisel verilerin üçüncü kişilere aktarılmasına ilişkin Kanundaki gibi özel şartlar düzenlememiş, tüm işleme faaliyetleri için geçerli olan genel kurallara tabi kılmıştır.

3.4.3.2. Yurt Dışına Veri Aktarımının Şartları

3.4.3.2.1. Veri İşleme Şartının Bulunması

Kişisel verilerin işlenme şartlarına ilişkin Kanunun 5. ve 6. maddesi kapsamında yaptığımız açıklamalara atıf yaparak yurt dışına aktarılacak kişisel veriler için bu şartlardan en az bir tanesinin bulunması gerekmektedir. Kişisel verinin niteliğine göre özel nitelikli olmayan (genel nitelikli) kişisel veri ise Kanunun 5. Maddesindeki şartlara veya özel nitelikli kişisel veri ise Kanunun 6. maddesindeki şartlara bakılması gerekecektir. İlgili kişinin açık rızasının bulunması halinde kişisel verinin doğrudan yurt dışına aktarılması mümkün olacaktır.

---

[184] **a.g.e.**

[185] Yurt dışına kişisel veri aktarılması kapsamında kullanılacak taahhütname örneklerine şu uzantıdan erişebilirsiniz: https://www.kvkk.gov.tr/Icerik/2053/Yurtdisina-Aktarim Erişim Tarihi: 25 Mart 2020.

3.4.3.2.2. Veri Aktarımının Yapılacağı Ülkede Yeterli Korumanın Bulunması

Kanunun m. 9/3 hükmü uyarınca yeterli korumanın bulunduğu ülkeler Kurul tarafından belirlenerek ilan edileceği düzenlenmiş ise de henüz Kurul tarafından bu yönde bir ilan yapılmamıştır.

Kişisel veri aktarımının yurt dışına yapılması durumunda veri aktarımının yapılacağı ülkede yeterli korumanın bulunup bulunmadığının belirlenmesinde Kurul tarafından Kanunun m. 9/4 hükmü uyarınca bir değerlendirme yapılacaktır. Kanunun m. 9/4 hükmü aşağıdaki gibidir:

> "*(4) Kurul yabancı ülkede yeterli koruma bulunup bulunmadığına ve ikinci fıkranın (b) bendi uyarınca izin verilip verilmeyeceğine;*
>
> *a) Türkiye'nin taraf olduğu uluslararası sözleşmeleri,*
>
> *b) Kişisel veri talep eden ülke ile Türkiye arasında veri aktarımına ilişkin karşılıklılık durumunu,*
>
> *c) Her somut kişisel veri aktarımına ilişkin olarak, kişisel verinin niteliği ile işlenme amaç ve süresini,*
>
> *ç) Kişisel verinin aktarılacağı ülkenin konuyla ilgili mevzuatı ve uygulamasını,*
>
> *d) Kişisel verinin aktarılacağı ülkede bulunan veri sorumlusu tarafından taahhüt edilen önlemleri,*
>
> *değerlendirmek ve ihtiyaç duyması hâlinde, ilgili kurum ve kuruluşların görüşünü de almak suretiyle karar verir.*"

Yukarıda alıntılanan Kanun hükmü uyarınca Kurul esasen beş kriter üzerinden değerlendirme yapacaktır. Bu temel kriterlere ek olarak Kurul tarafından Kanunun 9. maddesi uyarınca yeterli korumanın bulunduğu ülkelerin Kurulca belirlenmesinde kullanılmak üzere 02.05.2019 tarihli ve 2019/125 sayılı karar ile "Yeterli Korumaya Sahip Ülkelerin Belirlenmesinde Esas Alınacak Kriterler[186]" kabul edilmiştir. Bu kararda kabul edilen kriterler Kanunun yukarıda alıntılanan m.

[186] Kurul'un "Yeterli Korumaya Sahip Ülkelerin Belirlenmesinde Esas Alınacak Kriterler" hakkındaki 02.05.2019 tarihli ve 2019/125 sayılı kararına şu uzantıdan ulaşabilirsiniz: https://www.kvkk.gov.tr/Icerik/5470/Kisisel-Verileri-Koruma-Kurulu-nun-Yeni-Yayinlanan-Karari Erişim Tarihi: 25 Mart 2020.

9/4 hükmüne göre çok daha detaylı şekilde 7 ana başlık ve 28 alt başlıkla düzenlenmiştir. Kurulun belirlediği kriterlerdeki ana başlıklar şu şekildedir;

i. "*Karşılıklılık durumu*
ii. *İlgili ülkenin kişisel verilerin işlenmesine ilişkin mevzuatı ve uygulanması*
iii. *Bağımsız veri koruma otoritesinin bulunması*
iv. *Kişisel verilerin korunması ile ilgili uluslararası antlaşmalara taraf olma ile uluslararası kuruluşlara üye olma durumu*
v. *Ülkemizin üye olduğu küresel ve bölgesel örgütlere üye olma durumu*
vi. *İlgili ülke ile yürütülen ticaret hacmi*
vii. *Diğer*"

Kriterlerin içindeki ana başlıklar kısmen Kanundaki kriterlerle benzerlik göstermekle birlikte yer yer farklılıklar barındırmaktadır.

Kanunun yürürlüğe girmesinden bu yana geçen süre içinde Kurul tarafından yeterli korumanın bulunduğu ülkeler listesi henüz ilan edilmiş değildir.

3.4.3.2.3. Bağlayıcı Şirket Kuralları (*Binding Corporate Rules*)

Bağlayıcı şirket kuralları (*binding corporate rules*), Working Party'nin hazırladığı çalışma belgeleri[187] ve GDPR'ın "Tanımlar" başlıklı 4. maddesinin 20. fıkrasında tanımlanmıştır. Burada yapılan tanımlamalardan hareketle bağlayıcı şirket kuralları, birden fazla ülkede ortak bir ekonomik faaliyet yürüten grup şirketlerinin (çok uluslu şirketlerin) birbirleri arasında ülkeler arası kişisel veri aktarımına ilişkin kuralları içeren ve tüm şirket çalışanları üzerinde bağlayıcı bir etkisi olan kişisel veri politikalarıdır. GDPR'ın 47. maddesi uyarınca bağlayıcı şirket kurallarının yetkili veri koruma otoritesi tarafından onaylanması gerektiği düzenlenmiştir. Ayrıca aynı madde içerisinde bağlayıcı şirket kurallarında asgari olarak bulunması gereken unsurlar belirtilmiştir[188].

---

[187] **Article 29 Data Protection Working Party**, Working Document Setting Up a Table With the Elements and Principles to Be Found in Binding Corporate Rules, 6 Şubat 2018, 18/EN, WP256 rev.01, (Çevrimiçi) https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=614109 Erişim Tarihi: 27 Nisan 2020, s. 2.
[188] Detaylı bilgi için bkz. GDPR m. 47/2.

Bağlayıcı şirket kuralları ile ilgili olarak Kurul tarafından 10 Nisan 2020 tarihinde, yeterli korumanın bulunmadığı ülkelerde faaliyet gösteren çok uluslu yapıdaki grup şirketleri arasında kişisel veri aktarımına ilişkin bir duyuru yapılmıştır[189]. Duyurunun çalışmamız bağlamında öne çıkan kısmı aşağıdaki gibidir:

> "(…) *Bilindiği üzere Kurul, Türkiye'de yerleşik veri sorumlusu tarafından yeterli veri koruması bulunmayan ülkelerde yerleşik veri sorumlusuna/veri işleyene kişisel verilerin aktarımında, ilgili tarafların yeterli bir korumayı yazılı olarak taahhüt etmelerine imkân sağlayan yöntemlerden birini Taahhütnameler olarak belirlemiş ve taraflarca hazırlanarak Kurul onayına sunulacak Taahhütnamelerde bulunması gereken asgari unsurları da belirleyerek ilan etmişti. Bu kapsamda söz konusu taahhütnamelerin Kurul tarafından onaylanması akabinde yurt dışına veri aktarımı mümkün olabilmektedir.*
>
> *Bununla birlikte söz konusu taahhütnameler, genellikle şirketler arasında gerçekleştirilecek iki taraflı veri aktarımlarını kolaylaştırmakla birlikte çok uluslu şirket toplulukları arasında yapılacak veri aktarımları bakımından uygulama pratiğini sağlamakta yetersiz kalabilmektedir. Bu nedenle Kurul tarafından, söz konusu şirketler arasında gerçekleştirilecek uluslararası veri aktarımlarında kullanılmak üzere diğer bir yöntem olarak da Bağlayıcı Şirket Kuralları belirlenmiştir.*" dedikten sonra bu kuralların işlevine değinmiştir.
>
> *"Bağlayıcı Şirket Kuralları, yeterli korumanın bulunmadığı ülkelerde faaliyet gösteren çok uluslu grup şirketleri için kişisel verilerin yurt dışına aktarımında kullanılan ve yeterli bir korumanın yazılı olarak taahhüt edilmesini sağlayan veri koruma kurallarıdır. Bu kapsama giren şirketlerin, ilgili formu doldurup gerekli talimatları*

[189] Kurulun 10 Nisan 2020 yayınlanma tarihli "Bağlayıcı Şirket Kuralları Hakkında Duyuru" başlıklı açıklamasına şu uzantıdan ulaşabilirsiniz: https://www.kvkk.gov.tr/Icerik/6728/YURT-DISINA-KISISEL-VERI-AKTARIMINDA-BAGLAYICI-SIRKET-KURALLARI-HAKKINDA-DUYURU Erişim Tarihi: 27 Nisan 2020.

izleyerek Kuruma, Bağlayıcı Şirket Kuralları başvurusu yapması gerekmektedir.

6698 sayılı Kanunun 9 uncu maddesinin (2) numaralı fıkrasının (b) bendi gereğince, söz konusu başvurular Kurul'un iznine tabidir."

Kurul kararının yayınlandığı Kurumun internet sitesinde kararda bahsedildiği gibi "Veri Sorumluları İçin Bağlayıcı Şirket Kuralları Başvuru Formu" ve "Veri Sorumluları İçin Bağlayıcı Şirket Kurallarında Bulunması Gereken Temel Hususlara İlişkin Yardımcı Doküman" başlıklı iki adet belge[190] ilgililerin kullanımına sunulmuştur.

Her iki belgenin de tanımlar kısmında bağlayıcı şirket kuralları Working Party çalışma belgeleri ve GDPR'daki tanımlamalara paralel olacak şekilde tanımlanmıştır:

"*Bir şirketler topluluğuna bağlı olarak Türkiye'de yerleşik bir veri sorumlusu tarafından, bu şirketler topluluğuna bağlı olarak yurt dışında bir veya daha fazla ülkede faaliyet gösteren şirketler, teşebbüsler ile ortak bir ekonomik faaliyette bulunan veya veri işleme faaliyetine ilişkin ortak bir karar mekanizması bulunan veri sorumlularına yapılacak olan kişisel veri aktarımları veya aktarım setlerinde uyulması gereken kişisel veri koruma kurallarını ifade eder.*"

Veri sorumluları tarafından Kuruma yapılan bağlayıcı şirket kuralları başvurusu ile ilgili olarak resmî başvuru tarihinden itibaren bir yıl içerisinde karar verileceği, gerekmesi durumunda bu sürenin altı aylık dönemlerle uzatılabileceği belirtilmiştir[191].

Bu belgelerin içeriği incelendiğinde özellikle "Veri Sorumluları İçin Bağlayıcı Şirket Kurallarında Bulunması Gereken Temel Hususlara İlişkin

---

[190] İsmi geçen iki belgeye de şu uzantıdan ulaşabilirsiniz: https://www.kvkk.gov.tr/Icerik/6728/YURT-DISINA-KISISEL-VERI-AKTARIMINDA-BAGLAYICI-SIRKET-KURALLARI-HAKKINDA-DUYURU Erişim Tarihi: 27 Nisan 2020.

[191] Bkz. Veri Sorumluları İçin Bağlayıcı Şirket Kuralları Başvuru Formu, s.3.

Yardımcı Doküman" başlıklı belge Working Party'nin bağlayıcı şirket kuralları üzerine yayınladığı çalışma belgeleri ile aynı doğrultuda olduğu görülmektedir.[192].

Kurulun bağlayıcı şirket kuralları hakkında hazırladığı belgelerin içeriğinde bahsedilen başvuruların karara bağlanma sürelerinin çok uzun olması ve bu sürenin gerekmesi halinde herhangi bir sınırlama koymaksızın altı aylık dönemlerle uzatılabileceğinin belirtilmesi uygulamada özellikle çok uluslu şirketler nezdinde çeşitli sıkıntılar yaratabileceğini düşünmekteyiz. Bu sıkıntıların, Kurul tarafından yeterli korumanın bulunduğu ülkelere ilişkin listenin açıklanması, bağlayıcı şirket kurallarına ilişkin yapılan başvuru süreçlerinin hızlandırılması ve Türkiye'deki uygulamaya, mevcut sorunlara ve ihtiyaçlara yönelik özgün içerikli kuralların belirlenmesi ile aşılabileceği kanaatindeyiz.

[192] Aynı görüşte bkz. **Murat Volkan Dülger, Cansu Ceren Kahraman**, "KVKK'dan Kişisel Verilerin Yurt Dışına Aktarımında Önemli Bir Adım: Bağlayıcı Şirket Kuralları", (Çevrimiçi) https://www.hukukihaber.net/kvkkdan-kisisel-verilerin-yurt-disina-aktariminda-onemli-bir-adim-baglayici-sirket-kurallari-makale,7685.html Erişim Tarihi: 27 Nisan 2020.

ÜÇÜNCÜ BÖLÜM
VERİ SORUMLULARININ KİŞİSEL VERİLERİN KORUNMASI KANUNU KAPSAMINDAKİ ÖZEL YÜKÜMLÜLÜKLERİ

1. AYDINLATMA YÜKÜMLÜLÜĞÜ

1.1. Genel Olarak

Bireylerin kişisel verilerin korunması alanında sahip oldukları temel enstrümanlar; bireylere sağlanan haklar ve veri sorumlularına getirilen yükümlülüklerdir[193]. Bireyler kendilerine sağlanmış haklarını kullanarak kendi kişisel verileri üzerinde yapılan veri işleme faaliyetlerinin hukuka uygun olarak yapılıp yapılmadığını kontrol etme, denetleme imkânı elde edeceklerdir[194]. Bu sebeplerle ilgili kişinin aydınlatılması kişisel verilerin korunması hukukunda çok büyük bir öneme sahiptir[195].

Kanunun "Veri sorumlusunun aydınlatma yükümlülüğü" başlıklı 10. maddesi uyarınca; "kişisel verilerin elde edilmesi sırasında veri sorumlusu veya yetkilendirdiği kişi" tarafından ilgili kişileri aydınlatma (bilgi verme) yükümlülüğü getirilmiştir. İlgili madde hükmü aşağıdaki gibidir:

> "*(1) Kişisel verilerin elde edilmesi sırasında veri sorumlusu veya yetkilendirdiği kişi, ilgili kişilere;*
>
> *a) Veri sorumlusunun ve varsa temsilcisinin kimliği,*
>
> *b) Kişisel verilerin hangi amaçla işleneceği,*
>
> *c) İşlenen kişisel verilerin kimlere ve hangi amaçla aktarılabileceği,*" düzenlenmiştir. Ayrıca;

---

[193] **Şehriban İpek Aşıkoğlu**, "Veri Sorumlularının Aydınlatma Yükümlülüğü -Avrupa Birliği ve Türk Hukukunda-", Kişisel Verilerin Korunması Dergisi, Cilt 1, Sayı 2, s. 41-65, 2019, s. 42.

[194] **Mesut Serdar Çekin**, Avrupa Birliği Hukukuyla Mukayeseli Olarak 6698 Sayılı Kanun Çerçevesinde Kişisel Verilerin Korunması Hukuku, On İki Levha Yayınları, İstanbul 2019, s. 119; **Aşıkoğlu**, "Veri Sorumlularının Aydınlatma Yükümlülüğü -Avrupa Birliği ve Türk Hukukunda-", s. 42.

[195] **Deryck Beyleveld**, "The Duty to Provide Information to Data Subject: Articles 10 and 11 of Directive 95/46/EC", The Data Protection Directive and Medical Research Across Europe, İngiltere 2004, s. 70; **Küzeci**, s. 224.

"ç) Kişisel veri toplamanın yöntemi ve hukuki sebebi,

d) 11 inci maddede sayılan diğer hakları,

konusunda bilgi vermekle yükümlüdür."

Aydınlatma yükümlülüğünün temelinde veri işleme faaliyetinin dürüstlük kuralına uygun şekilde gerçekleştirilmesi ve Kanunun veri işlenmesine ilişkin genel ilkelerinde düzenlenmemiş olsa da şeffaflık (*transparency*) ilkesinin bir sonucudur[196].

Veri sorumlusu veya onun yetkilendirdiği kişi tarafından ilgili kişiye karşı aydınlatma yükümlülüğünün gerçekleştirilmesi sonucunda ilgili kişi, kendi kişisel verilerinin kimler tarafından işlendiğini, veri sorumlusunun temsilcisinin kim olduğunu, kişisel verilerinin hangi amaçlarla işlendiğini, kimlere ve hangi amaçlarla aktarılabileceğini, bu verilerin toplanma yöntemini ve hukuki sebebini ve Kanun tarafından kendisine tanınan hakların neler olduğunu öğrenecektir. Kaldı ki ilgili kişi, Kanunun "İlgili kişinin hakları" başlıklı 11. maddesi uyarınca dilediği zaman veri sorumlusuna başvurarak kendisiyle ilgili bu bilgileri elde etmesi mümkündür. Bu noktada değinilmesi gereken bir husus; Kanunun 11. maddesi uyarınca ilgili kişinin bilgi edinme hakkını kullanması bir sınırlama getirilmediği için her zaman mümkün iken, Kanunun 10. maddesi uyarınca aydınlatma yükümlülüğü yalnızca kişisel verinin elde edilmesi sırasında yerine getirilmesi gereken bir yükümlülük olmasıdır.

Konuya ilişkin olarak Kurul tarafından 2019 yılının Nisan ayında "Aydınlatma Yükümlülüğünün Yerine Getirilmesi Rehberi" yayınlanmıştır[197]. Bu başlık altında mevzuata ek olarak ilgili olduğu ölçüde Aydınlatma Rehberi üzerinden de açıklamalar yapılacaktır.

---

[196] **Mesut Serdar Çekin**, Avrupa Birliği Hukukuyla Mukayeseli Olarak 6698 Sayılı Kişisel Verilerin Korunması Kanunu, On İki Levha Yayınları, İstanbul 2018, s. 103; **Şimşek**, s. 88.

[197] Kişisel Verileri Koruma Kurumu, Aydınlatma Yükümlülüğünün Yerine Getirilmesi Rehberi, Ankara 2019, (Çevrimiçi) https://www.kvkk.gov.tr/SharedFolderServer/CMSFiles/a569a068-c079-4189-b134-f57bc727af7d.pdf Erişim Tarihi: 27 Mart 2020. Bundan sonra "Aydınlatma Rehberi" olarak anılacaktır.

1.2. Aydınlatma Yükümlülüğüne İlişkin Usul ve Esaslar

Kanunun 10. maddesindeki düzenlemelere ek olarak Kişisel Verileri Koruma Kurumu tarafından uygulamadaki belirsizliklerin giderilmesi ve konuyla ilgili daha detaylı bir düzenleme yapmak adına "Aydınlatma Yükümlülüğünün Yerine Getirilmesinde Uyulacak Usul ve Esaslar Hakkında Tebliğ[198]" hazırlanmıştır. Tebliğ 10.03.2018 tarihli ve 30356 sayılı Resmî Gazete'de yayımlanarak yürürlüğe girmiştir. Aydınlatma yükümlülüğünün yerine getirilmesi noktasında detaylı usul ve esasları içerdiği için bundan sonraki açıklamalarımızı Tebliğe odaklanarak yapacağız.

1.2.1. Aydınlatma Yükümlülüğünün Kapsamı

Tebliğin "Aydınlatma yükümlülüğünün kapsamı" başlıklı 4. maddesinde öncelikle; "kişisel verilerin elde edilmesi sırasında veri sorumluları veya yetkilendirdiği kişilerce, ilgili kişilerin bilgilendirilmesi" gerektiği Kanuna paralel şekilde belirtildikten sonra maddenin devamında, veri sorumluları veya yetkilendirdiği kişilerce yapılması gereken aydınlatmanın "asgari" olarak aşağıdaki konuları içermesi gerektiği belirtilmiştir. Bu konular aşağıdaki gibidir:

i. "Veri sorumlusunun ve varsa temsilcisinin kimliği
ii. Kişisel verilerin hangi amaçla işleneceği
iii. Kişisel verilerin kimlere ve hangi amaçla aktarılabileceği
iv. Kişisel veri toplamanın yöntemi ve hukuki sebebi
v. İlgili kişinin Kanunun 11. maddesinde sayılan diğer hakları"

Görüldüğü üzere Tebliğin 4. maddesi sayılan bilgilendirme konuları çoğunlukla Kanunun 10. maddesinin tekrarı niteliğinde olduğu söylenebilir. Ancak Tebliğde, Kanundan farklı şekilde aydınlatma yükümlülüğü kapsamında yapılacak bilgilendirme faaliyetinin "asgari olarak" yukarıda sayılan konuları içermesi gerektiğini düzenlemiştir. Bunun anlamı yukarıda sayılan bilgilendirme

[198] Aydınlatma Yükümlülüğünün Yerine Getirilmesinde Uyulacak Usul ve Esaslar Hakkında Tebliğ'in metnine şu uzantıdan ulaşabilirsiniz:
https://www.resmigazete.gov.tr/eskiler/2018/03/20180310-5.htm Erişim Tarihi: 27 Mart 2020. Bundan sonra "Tebliğ" olarak anılacaktır.

konularından bir tanesinin bile aydınlatma bildiriminde bulunmaması durumunda veri sorumlusunun aydınlatma yükümlülüğünü doğru bir şekilde yerine getirmemiş olmasına sebep olacağıdır. Böyle bir durumda idari para cezasının gündeme gelmesi de söz konusu olabilecektir.

Kurul kendisine gelen bir şikâyet üzerine e-ticaret ve teknoloji şirketi Amazon'un Türkiye'deki bazı faaliyetlerinde Kanunun 10. maddesinde düzenlenen aydınlatma yükümlülüğüne ve Kanunun 12. maddesinde düzenlenen veri güvenliğine ilişkin yükümlülüklere aykırılıklar tespit etmiştir. Kurulun 27 Şubat 2020 tarihli ve 2020/173 sayılı kararı uyarınca[199];

> "(…) *www.amazon.com.tr'ye ilişkin yürütülen resen inceleme neticesinde yukarıda yer verilen değerlendirmeler sonucunda*
>
> *Veri sorumlusunun ilgili kişilerin iletişim bilgilerini işlemek suretiyle ticari elektronik ileti göndermek hususunda ilgili kişilerin açık rızasını usulüne uygun olarak almadığı, açık rıza dışında da bir işleme nedenine dayanmadığı, diğer yandan üyenin temas kişilerine ait e-posta adreslerinin de bu kişilerin açık rızalarına dayanmaksızın işlendiği, ayrıca veri sorumlusu tarafından Kanunun 4'üncü maddesinde yer alan genel ilkelere aykırı hareket edildiği,*
>
> *Veri sorumlusunun Gizlilik Bildiriminde 'Amazon Kişisel Bilgilerinizi Paylaşıyor mu?' başlığı altında 'Yukarıda belirtilenler haricinde, hakkınızdaki kişisel bilgiler üçüncü taraflarla paylaşıldığında, bir bildirim alacaksınız ve bu bilgileri paylaşmamayı seçme şansınız olacaktır.' ifadesine yer verildiği, metinde yer aldığı şekilde ilgili kişinin kişisel verilerini paylaşmamayı tercih etme şansının mümkün olmasının, ancak ilgili kişinin açık rızasına istinaden verilerinin işlenmesi halinde geçerli olabileceği, ancak usulüne uygun bir açık rıza alınmadığı dikkate alındığında, kişisel verilerin aktarılmasına ilişkin Kanun hükümlerine aykırı hareket edildiği,*

[199] Kurulun 27.02.2020 tarihli ve 2020/173 sayılı kararına şu uzantıdan ulaşabilirsiniz: https://www.kvkk.gov.tr/Icerik/6739/2020-173 Erişim Tarihi: 17 Mayıs 2020.

Kişisel verilerin yurt dışına aktarılması konusunda Kanunun 9'uncu maddesinde yer alan yeterli korumanın bulunduğu ülkelerin Kurulca henüz belirlenmediği, veri sorumlusunun yazılı taahhüdünün Kurum tarafından onaylanmadığı da dikkate alındığında, veri sorumlusunun kişisel verilerin yurtdışına aktarılması konusunda Kanunun 9'uncu maddesinin (1) numaralı fıkrasında yer aldığı üzere ilgili kişilerin açık rızasını alması gerektiği, ancak veri sorumlusunun yurt dışına aktarıma ilişkin usulüne uygun bir açık rıza alma yoluna gitmediği, yalnızca amazon hizmetlerinin kullanılması suretiyle gizlilik bildiriminde yer alan hususların kabul edilmiş olduğu varsayımının Kanuna uygun bir açık rıza olarak nitelendirilemeyeceği

dikkate alındığında veri sorumlusu tarafından Kanunun 12'nci maddesinin (1) numaralı fıkrasındaki yükümlülüklerin yerine getirilmemesinden dolayı Kanunun 18'inci maddesinin (1) numaralı maddesinin (b) bendi kapsamında 1.100.000 TL idari para cezası uygulanmasına"

karar verilmiştir[200]. Bu karar gizlilik bildirimlerinin yalnızca açıklanmasının ilgili kişiden açık rızanın usulüne uygun olarak temin edildiği anlamına gelmeyeceği, hususlarının altını çizmesi bakımından önem taşımaktadır.

1.2.2. Aydınlatma Yükümlülüğüne İlişkin Usul ve Esaslar

Aydınlatma yükümlülüğü konusunda getirdiği yeni ve çeşitli kurallarla düzenlemenin omurgasını oluşturduğunu söyleyebileceğimiz Tebliğin "Usul ve esaslar" başlıklı 5. maddesi uyarınca; "veri sorumlusu ya da yetkilendirdiği kişi tarafından sözlü, yazılı, ses kaydı, çağrı merkezi gibi fiziksel veya elektronik ortam kullanılmak suretiyle aydınlatma yükümlülüğünün yerine getirilmesinin" mümkün

[200] Bu kararla birlikte Kurul tarafından Amazon'a ek olarak aydınlatma yükümlülüğüne aykırılıktan 100.000 TL idari para cezası verilmiştir.

olduğu düzenlenmiştir. Böylece veri sorumluları tarafından aydınlatma yükümlülüğünün hangi vasıtalar kullanılarak yapılması gerektiği düzenlenmiştir.

Tebliğin 5. Maddesinin devamında ise veri sorumluları ya da yetkilendirdiği kişi tarafından aydınlatma yükümlülüğü yerine getirilirken uyulması gereken usul ve esaslar detaylı şekilde düzenlenmiştir. Bu usul ve esaslar aşağıdaki gibidir:

i. "İlgili kişinin açık rızasına veya Kanundaki diğer işleme şartlarına bağlı olarak kişisel veri işlendiği **her durumda** aydınlatma yükümlülüğü" veri sorumluları ya da yetkilendirdiği kişi tarafından yerine getirilmelidir. Tebliğ, getirdiği bu düzenleme açısından GDPR'daki aydınlatma yükümlülüğünden çok daha sert bir rejim getirmiştir[201]. Zira GDPR'ın 13. maddesinin son fıkrası uyarınca ilgili kişinin konuya ilişkin halihazırda bilgi sahibi olması durumunda, yine de ek bir aydınlatma yapılmasına gerek olmadığı düzenlenmiştir.

ii. "Kişisel verilerin işleme amacı değiştiğinde, veri işleme faaliyetinden önce bu amaç için aydınlatma yükümlülüğü ayrıca yerine getirilmelidir."

- Bu düzenleme Kanunun m. 10/1-b hükmündeki "Kişisel verilerin hangi amaçla işlendiği" ve m. 10/1-c hükmündeki "İşlenen kişisel verilerin kimlere ve hangi amaçla aktarılabileceği" düzenlemeleri ile paralellik göstermektedir. Bu düzenleme uyarınca daha önce ilgili kişi nezdinde aydınlatma yükümlülüğünü yerine getiren veri sorumlusu, yaptığı bu aydınlatma içindeki tek bir veri işleme amacının değişmesi durumunda dahi henüz bu değişen amaç doğrultusunda veri işleme faaliyetine başlamadan önce ilgili kişiye bu değişiklikle ilgili yeni bir aydınlatma yapmakla yükümlü olduğu düzenlenmiştir.

[201] **Dülger**, s. 398.

iii. Veri sorumlusunun, Kanun ve Veri Sorumluları Sicili Hakkında Yönetmelik uyarınca "Sicile (Veri Sorumluları Sicil Bilgi Sistemi veya VERBİS) kayıt yükümlülüğünün bulunması durumunda, aydınlatma yükümlülüğü çerçevesinde ilgili kişiye verilecek bilgiler, Sicile açıklanan bilgilerle uyumlu olmalıdır."

iv. "Aydınlatma yükümlülüğünün yerine getirilmesi, ilgili kişinin talebine bağlı değildir."

- Bu düzenleme ile birlikte veri sorumlularının ilgili kişinin talep etmemesi gerekçesiyle aydınlatma yükümlülüğünden kurtulmasının önüne geçilmiştir. Yani veri sorumluları veya yetkilendirdikleri kişi tarafından ilgili kişinin talebinin varlığı aranmaksızın aydınlatma yükümlülüğünün yerine getirilmesi zorunludur.

v. "Aydınlatma yükümlülüğünün yerine getirildiğinin ispatı veri sorumlusuna aittir."

- Aydınlatma yükümlülüğünün yerine getirildiğine dair olası bir uyuşmazlıkta ispat yükümlülüğü altında olan veri sorumlusunun uygun ispat araçları ile bunu ortaya koyabilmesi gereklidir. Örneğin ilgili kişiye veri sorumlusu tarafından sözlü olarak yapılan aydınlatmanın ilgili kişi tarafından böyle bir aydınlatmanın yapılmadığının iddia edilmesi halinde, veri sorumlusu tarafından gerekli ispatın sağlanması pek mümkün olamayacaktır. Bu sebeple veri sorumlusunun aydınlatma yükümlülüğünü yerine getirdiğinin ispatı noktasında aydınlatmanın yapıldığına ilişkin delillerin yazılı veya elektronik ortamlarda tutulması bu hususta önemli bir rol oynayacaktır.

vi. "Kişisel veri işleme faaliyetinin açık rıza şartına dayalı olarak gerçekleştirilmesi halinde, aydınlatma yükümlülüğü ve açık rızanın alınması işlemlerinin ayrı ayrı yerine getirilmesi gerekmektedir."

- Bu düzenleme ile birlikte ilgili kişinin açık rızasının olması halinde dahi veri sorumlusunun aydınlatma yükümlülüğünün devam etmesidir. Diğer bir ifadeyle aydınlatma yükümlülüğü, veri işleme şartlarından ilgili kişinin açık rızasının varlığı halinde veya ilgili kişinin açık rızası olmadan veri işleme faaliyetinin yapılabileceği hallerde herhangi bir farklılık göstermeden devam edecektir.
- Kurul kendisine gelen bir şikâyet üzerine e-ticaret ve teknoloji şirketi Amazon'un Türkiye'deki bazı faaliyetlerinde Kanunun m. 10. maddesinde düzenlenen aydınlatma yükümlülüğüne ve Kanunun 12. maddesinde düzenlenen veri güvenliğine ilişkin yükümlülüklere aykırılıklar tespit etmiştir. Kurulun 27 Şubat 2020 tarihli ve 2020/173 sayılı kararı uyarınca[202]; "(…) *www.amazon.com.tr'ye ilişkin yürütülen resen inceleme neticesinde yukarıda yer verilen değerlendirmeler sonucunda,*

  Veri sorumlusunca web sitesinde yayımlanan Gizlilik Bildiriminin, birçok bilgi içermesi, veri işlemeye ilişkin genel bir bilgilendirme olması nedeniyle kişisel verilerin işlenmesine ilişkin ilgili kişilere aydınlatma yapıldığı anlamına gelmediği göz önünde bulundurulduğunda ihbar edilen web sitesine girişle birlikte çerezler vasıtasıyla kişisel verilerin işlenmeye başlamasına karşın, çerezler, üyelik girişi gibi veri işlemenin başladığı hiçbir aşamada aydınlatma yükümlülüğünün, Kanunun 10'uncu maddesinde ve Aydınlatma Yükümlülüğünün Yerine Getirilmesinde Uyulacak Usul ve Esaslar Hakkında Tebliğde düzenlenen usul ve esaslara uygun olarak yerine getirilmediği kanaati

[202] Kurulun 27 Şubat 2020 tarihli ve 2020/173 sayılı kararına şu uzantıdan ulaşabilirsiniz: https://www.kvkk.gov.tr/Icerik/6739/2020-173 Erişim Tarihi: 17 Mayıs 2020.

oluştuğundan Kanunun 10'uncu maddesinde düzenlenen Aydınlatma Yükümlülüğünü yerine getirmeyen veri sorumlusu hakkında Kanunun 18'inci maddesinin (1) numaralı fıkrasının (a) bendi uyarınca 100.000 TL idari para cezası uygulanmasına" karar verilmiştir[203]. Bu karar çerezlere ilişkin aydınlatma metinlerinin ve politikaların şirketler tarafından usulüne uygun hazırlanması gerektiğini belirtmektedir. Bu kapsamda internet sitelerindeki çerez türlerinin ilgili kişi tarafından opt-in yöntemiyle kendisi tarafından seçilmesi gerektiği, gizlilik bildirimlerinin yalnızca açıklanmasının ilgili kişiden açık rızanın usulüne uygun olarak temin edildiği anlamına gelmeyeceği kanaatindeyiz.

vii. "Aydınlatma yükümlülüğü kapsamında açıklanacak kişisel veri işleme amacının belirli, açık ve meşru olması gerekir. Aydınlatma yükümlülüğü yerine getirilirken, aydınlatma metninde genel nitelikte ve muğlak ifadelere yer verilmemelidir. Gündeme gelmesi muhtemel başka amaçlar için kişisel verilerin işlenebileceği kanaatini uyandıran ifadeler kullanılmamalıdır."

- Bu konuda Kurulun 26.07.2018 tarihli ve 2018/90 sayılı "Veri sorumlusu tarafından aydınlatma yükümlülüğü ve açık rıza onayı alınması süreçlerinin ayrı ayrı yerine getirilmesi gerektiği ile ilgili" kararı[204] uyarınca; "*Online platformda iş başvurusu alan veri sorumlusu şirketler topluluğunun kişisel veri işleme süreçlerinin Kurul tarafından re'sen incelenmesini teminen yapılan başvuru neticesinde,*

[203] Bu kararla birlikte Kurul tarafından Amazon'a ek olarak veri güvenliğine ilişkin yükümlülüklere aykırılıktan 1.000.000 TL idari para cezası verilmiştir.

[204] Kurulun 26.07.2018 tarihli ve 2018/90 sayılı kararına şu uzantıdan ulaşabilirsiniz: https://www.kvkk.gov.tr/Icerik/5420/-Veri-sorumlusu-tarafindan-aydinlatma-yukumlulugu-ve-acik-riza-onayi-alinmasi-sureclerinin-ayri-ayri-yerine-getirilmesi-gerektigi-ile-ilgili-Kisisel-Verileri-Koruma-Kurulunun-26-07-2018-tarihli-ve-2018-90-sayili-Karar-Ozeti Erişim Tarihi: 25 Mart 2020.

Online platformda iş başvurusunda bulunurken üyelik kaydı yapılmasının zorunlu olduğu, üyelik kaydı yapılması sırasında ise, aynı kutucuğun işaretlenmesi yoluyla hem aydınlatma metninin okunduğuna, hem de kişisel verilerin işlenmesi hususunda açık rıza verildiğine ilişkin onay alınması yoluna gidildiği tespit edilmiştir.

Bu kapsamda; (...) Tüm bu hususlar bir arada değerlendirildiğinde; söz konusu uygulamanın 6698 sayılı Kişisel Verilerin Korunması Kanununun (Kanun) amacına ve Aydınlatma Yükümlülüğünün Yerine Getirilmesinde Uyulacak Usul ve Esaslar Hakkında Tebliğin 5 inci maddesinin (1) numaralı fıkrasının (f) bendinde yer alan hükme uygun olmadığı, bu itibarla ***aydınlatma metninin okunduğuna ilişkin geri bildirim alınması ile ilgili kişilerin kişisel verilerinin işlenmesi hususunda gerekli seçimlik haklarının da tanındığı açık rıza metninin onaylandığının ispatını sağlayacak mekanizmaların ayrıştırılması*** *hususunda veri sorumlusunun talimatlandırılmasına karar verilmiştir.*" Kurul, bu kararında ilgili kişiden açık rıza alınması işlemi ile veri sorumlusu veya yetkilendirdiği kişi tarafından aydınlatma yükümlülüğünün yerine getirilmesi işlemlerinin birbirinden ayrı şekilde yapılması ve yapılan bu işlemlere ait ispat mekanizmalarının da birbirinden ayrıştırılması gerektiği belirtilmiştir.

- Bu konuda Kurulun 02.05.2019 tarihli ve 2019/122 sayılı "İlgili kişinin T.C. Ziraat Bankası A.Ş.'ye yaptığı başvurunun cevaplandırılmaması ve veri sorumlusu tarafından internet üzerinden yayımlanan aydınlatma metninin mevzuatta

düzenlenen şartları taşımaması hakkında" kararı[205] uyarınca; "*6698 sayılı Kişisel Verilerin Korunması Kanununun (Kanun) 11 inci maddesinde belirtilen hakları kapsamındaki taleplerini içeren kayıtlı elektronik posta (KEP) aracılığıyla veri sorumlusu T.C. Ziraat Bankası A.Ş.'ye (Banka) başvuran ancak, Kanunda düzenlenen otuz günlük süre içerisinde başvurusu cevaplandırılmayan ilgili kişinin gerek bu konuda gerekse veri sorumlusunun, internet sitesi üzerinden yayımladığı aydınlatma metninin mevzuatta düzenlenen şartları taşımadığı hususunda Kuruma yapılan şikâyet başvurusu hakkında; (…)*

Bankanın internet sitesinde yer alan aydınlatma metninde, Bankanın kişisel veri işleme amaçlarının, ilgili kişilerin kişisel verilerinin Kanunun 5 inci ve 6 ncı maddelerinde belirtilen işleme şartlarından hangisine dayanılarak işlendiğine yönelik hukuki sebep açıkça belirtilmeksizin sıralandığı; kişisel veri işleme amaçları sıralandıktan sonra metin içerisinde yer verilen - gibi amaçlar kapsamında işlenmektedir - ifadesinin ise, gündeme gelmesi muhtemel başka amaçlar için kişisel verilerin işlenebileceği kanaatini uyandırır nitelikte olduğu; bu çerçevede söz konusu aydınlatma metninin Aydınlatma Yükümlülüğünün Yerine Getirilmesinde Uyulacak Usul ve Esaslar Hakkında Tebliğ'in (Tebliğ) 5 inci maddesinin birinci fıkrasının (g) ve (h) bentlerinde yer verilen hükümlere uygun hazırlanmaması nedeniyle, Bankanın internet sitesinde yer alan aydınlatma metninin yeniden gözden geçirilerek Tebliğ hükümlerine uygun hale getirilmesi yönünde

[205] Kurulun 02.05.2019 tarihli ve 2019/122 sayılı kararına şu uzantıdan ulaşabilirsiniz: https://www.kvkk.gov.tr/Icerik/5461/2019/122 Erişim Tarihi: 29 Mart 2020.

talimatlandırılmasına karar verilmiştir." Bu karar ile birlikte Kurul, veri işleme amacının birden fazla olması ve aydınlatma metninde veri işleme amacının net şekilde hangi amaçlarla yapıldığının belirtilmemesi, bunun yerine muğlak ifadeler kullanılması halinde hazırlanan aydınlatma metinlerinin hukuka aykırı olduğu ve böylece veri sorumlusunun aydınlatma yükümlülüğünü yerine getirmemiş olduğunu vurgulamıştır.

- Kurul, diğer bir kararında ise aydınlatma metinlerinde yer alacak veri işleme amaçlarının sınırlılık ve ölçülülük ilkelerine uygun olması gerektiğini belirtmiştir. Bu doğrultuda Kurulun 25.03.2019 tarihli ve 2019/82 sayılı "Bir market zincirinin sadakat kart uygulamasına ilişkin ihbar ve şikayetler hakkında" kararı[206] uyarınca; "*Aydınlatma metninin incelenmesinden ucu açık ifadelere yer verildiği, öte yandan Sadakat Kart Programına üye olunması aşamasında elde edilen kişisel veriler ve bunların aktarıldığı taraflar hususları başta olmak üzere, Üyelik ve Rıza Metni ile Aydınlatma Metni arasındaki tutarsızlıklar bulunduğu, nitekim, elde edilen kişisel verilerin sosyal paylaşım siteleri ile paylaşılacağı hususunda kişilerin aydınlatılmasına rağmen yapılan güncelleme neticesinde Üyelik ve Rıza Beyanı'nda bu ifadenin metinden çıkarılması ile birlikte söz konusu paylaşım için kişilerin açık rızalarının alınmadığı bir durumun oluşmasına sebebiyet verildiği,*

  Ayrıca, aydınlatma metninde Şirketleri tarafından özel nitelikli kişisel verilerin de (sendika/dernek/vakıf üyeliklerine

[206] Kurulun 25.03.2019 tarihli ve 2019/82 sayılı kararına şu uzantıdan ulaşabilirsiniz: https://www.kvkk.gov.tr/Icerik/5463/-Bir-market-zincirinin-sadakat-kart-uygulamasina-iliskin-ihbar-ve-sikayetler-hakkinda-Kisisel-Verileri-Koruma-Kurulunun-25-03-2019-tarihli-ve-2019-82-sayili-Karari Erişim Tarihi: 29 Mart 2020.

ilişkin bilgiler, ceza mahkûmiyeti, güvenlik tedbirleriyle ilgili veriler, cinsel hayat, biyometrik veri ve sağlık durumunuza ilişkin bilgiler gibi) işlenebileceği ifadelerine yer verildiği görülmüş olup, Şirketin temel faaliyet alanının gıda ve ihtiyaç maddelerinin perakende olarak tüketicilere ulaştırılması olduğu, Şirkete ait tüm işyerlerinde sunulan Sadakat Kart uygulamasının ise bir pazarlama programı olarak tasarlandığı dikkate alındığında, ceza mahkûmiyeti, güvenlik tedbirleriyle ilgili veriler gibi özel nitelikli kişisel verilerin işlenmesinin veri sorumlusunun faaliyetleri kapsamında amaçla bağlantılı, sınırlı ve ölçülü olmadığı değerlendirildiğinden, Üyelik ve Rıza Beyanı ile Aydınlatma Metni arasındaki tutarsızlıkların giderilmesi ve Şirketin Aydınlatma Metninin Kanunun temel ilkeleri ve Tebliğ hükümleri de dikkate alınmak suretiyle güncellenmesi gerektiği hususunda Şirketin talimatlandırılmasına (...) karar verilmiştir." Bu kararda Kurul, genel olarak veri sorumlularının aydınlatma yükümlülüklerini yerine getirirken dikkat etmeleri gereken bazı noktalardan bahsetmiş ve veri işleme amaçlarının sınırlı ve ölçülü olması gerektiğinin altını çizmiştir.

- Yukarıdaki kararlara ek olarak Fransız veri koruma otoritesi CNIL (Commission Nationale de l'Informatique et des Libertés) tarafından Google aleyhine verilen 29.01.2019 tarihli kararda[207] özet olarak Google tarafından yapılan aydınlatmanın yeterince açık bir şekilde yapılmadığını, metnin erişilebilir olmadığını, metinde net bir dil kullanılarak

[207] CNIL ("Commission nationale de l'informatique et des libertés", İngilizcesi "National Commission on Informatics and Liberty") Fransız Veri Koruma Kurulu'nun Google'a kestiği idari para cezasına ilişkin olarak bkz. https://www.cnil.fr/sites/default/files/atoms/files/san-2019-001.pdf Erişim Tarihi: 30 Mart 2020.

veri işleme amaçlarının sınırlarının çizilmediğini, muğlak ifadelerle "şemsiye" aydınlatma yapıldığını, rızanın uygun şekilde alınmadığını, bu sebeple ilgili kişilerin Google tarafından yürütülen veri işleme faaliyetlerini tam olarak anlayamadıklarını belirtmiştir. Bu saptamaların ardından CNIL tarafından Google'a 50 milyon Euro tutarında idari para cezası kesmiştir. CNIL bu karar ile birlikte GDPR ile birlikte yürürlüğe giren üst düzey idari para cezasını ilk kez uygulamıştır[208].

viii. "Aydınlatma yükümlülüğü kapsamında ilgili kişiye yapılacak bildirimin anlaşılır, açık ve sade bir dil kullanılarak gerçekleştirilmesi gerekmektedir."

- Kurulun bir önceki paragrafta alıntıladığımız 02.05.2019 tarihli ve 2019/122 sayılı kararı bu madde için de geçerlidir.

ix. "Kanunun 10. maddesinin birinci fıkrasının (ç) bendinde yer alan hukuki sebep kavramından kasıt, aydınlatma yükümlülüğü kapsamında kişisel verilerin Kanunun 5 ve 6. maddelerinde belirtilen işleme şartlarından hangisine dayanılarak işlendiğidir. Aydınlatma yükümlülüğünün yerine getirilmesi esnasında hukuki sebebin açıkça belirtilmesi gerekmektedir."

- Kanunun "Veri sorumlusunun aydınlatma yükümlülüğü" başlıklı 10. maddesinin birinci fıkrasının (ç) bendinde; "Kişisel veri toplamanın yöntemi ve hukuki sebebi"nin ilgili kişiye yapılacak aydınlatma bildirimi sırasında açıklanması gerektiği düzenlenmiştir. Tebliğin bu düzenlemesiyle, Kanunun m. 10/1-ç hükmündeki "hukuki sebep" kavramından anlaşılması gerekenin kişisel verilerin Kanunun 5. ve 6. maddelerinde belirtilen veri işleme şartlarından hangisine dayanılarak işlendiğinin belirlenmiş olması

[208] **Dülger**, s. 403.

gerektiği ve bu doğrultuda ilgili kişinin bilgilendirilmesi gerekliliği düzenlenmiştir. Örneğin, veri sorumlusu tarafından aydınlatma yükümlülüğü kapsamında ilgili kişiye yapılacak olan bildirimde, ilgili kişinin kişisel verisi veri işleme şartlarından kanunda açıkça öngörülme sebebine dayanıyorsa bu kanunun hangi kanun olduğunun veya veri işleme şartlarından açık rıza alınmadan işleme yetkisi veren diğer sebeplere dayanıyorsa ise bunların açıkça ne olduğuna dair bilgi verilmesi gerekmektedir.

x. "Aydınlatma yükümlülüğü kapsamında, kişisel verilerin aktarılma amacı ve aktarılacak alıcı grupları belirtilmelidir."

- Bu düzenleme ile veri sorumlusunun kişisel verileri üçüncü kişilere aktarma amaçları ile kimlere aktaracağına ilişkin bilgilerin ilgili kişiye açıklanması gerektiği düzenlenmiştir. Bu doğrultuda örneğin veri sorumlusu bir aydınlatma metni hazırlıyorsa ve toplanan kişisel verilerin aktarılması söz konusu ise kişisel verilerin aktarılma amacı, aktarılacak alıcı grupları gibi kişisel veri aktarıma ilişkin bilgilerin düzenlenen bu aydınlatma metninde yer alması doğru bir uygulama olacaktır.

xi. "Aydınlatma yükümlülüğü kapsamında kişisel verilerin, tamamen veya kısmen otomatik yollarla ya da veri kayıt sisteminin parçası olmak kaydıyla otomatik olmayan yöntemlerden hangisiyle elde edildiği açık bir şekilde belirtilmelidir."

- Bu düzenleme ile birlikte veri sorumlusu tarafından ilgili kişiye yapılacak bilgilendirmeye, kişisel verilerin hangi yöntemlerle elde edildiğine ilişkin bilgilendirmenin de eklenmesi gerektiği düzenlenmiştir.

xii. "Aydınlatma yükümlülüğü yerine getirilirken eksik, ilgili kişileri yanıltıcı ve yanlış bilgilere yer verilmemelidir."

- Bu düzenleme uyarınca veri sorumlusu tarafından yapılacak bilgilendirme içeriğinde eksik bilgilerin olması, ilgili kişileri yanıltıcı ve yanlış bilgilere yer verilmesi durumunda yapılan aydınlatmanın hukuka aykırı olacağı anlaşılmaktadır.

1.2.3. Kişisel Verilerin İlgili Kişiden Elde Edilmemesi Halinde Aydınlatma Yükümlülüğü

Kişisel verilerin ilgili doğrudan kişinin kendisinden değil de bir üçüncü kişiden elde edilmesi durumunda aydınlatma yükümlülüğünün nasıl yerine getirilmesi gerektiği hususu Tebliğ içerisinde ayrıca düzenlenmiştir.

Tebliğin "Kişisel verilerin ilgili kişiden elde edilmemesi halinde aydınlatma yükümlülüğü" başlıklı 6. maddesi uyarınca kişisel verilerin ilgili kişiden elde edilmemesi halinde veri sorumlusu;

i. "Kişisel verilerin elde edilmesinden itibaren makul bir süre içerisinde,

ii. Kişisel verilerin ilgili kişi ile iletişim amacıyla kullanılacak olması durumunda, ilk iletişim kurulması esnasında,

iii. Kişisel verilerin üçüncü kişilere aktarılacak olması durumunda, en geç kişisel verilerin ilk kez aktarımının yapılacağı esnada"

ilgili kişiyi aydınlatma yükümlülüğünü yerine getirmesi gerekir.

Tebliğin yukarıda anlatılan 6. maddesindeki düzenleme ışığında, veri sorumlusunun ilgili kişiye ulaşamaması durumunda kişisel verilerin üçüncü kişilere aktarılmasının mümkün olmadığı sonucuna varılmaktadır[209].

Kişisel verilerin ilgili kişinin kendisinden değil de bir üçüncü kişiden elde edilmesi durumunda aydınlatma yükümlülüğünün nasıl yerine getirilmesi gerektiği hususu 95/46/EC sayılı Direktif'in 11. maddesinde ve GDPR'ın 14. maddesinde birbirlerine genel olarak benzer şekilde düzenlenmiştir.

Tebliğ'deki düzenlemelere ek olarak 95/46/EC sayılı Direktif ve GDPR'da kişisel verilerin ilgili kişiden elde edilmediği bazı durumlarda veri sorumlusunun

[209] **Dülger**, s. 405.

aydınlatma yükümlülüğü ortadan kalkabileceği düzenlenmiştir. Veri sorumlusunun aydınlatma yükümlülüğünün ortadan kalktığı bu durumlara; ilgili kişinin aydınlatma yükümlülüğü kapsamında erişeceği bilgilere halihazırda sahip olması, aydınlatma yükümlülüğü kapsamında ilgili kişiye bilgi sağlanmasının imkânsız olması veya veri sorumlusundan hakkaniyet gereği beklenmesi mümkün olmayacak şekilde ölçüsüz oranda aşırı bir çaba gerektirmesi gibi durumlar örnek olarak gösterilebilir.

1.3. Katmanlı Bilgilendirme (Layered Privacy Statement / Notice)

Veri sorumluları tarafından aydınlatma yükümlülüğü yerine getirilirken ilgili kişiye yapılması gereken ve kapsamının Kanunda belirtildiği bilgilendirmenin tamamının yapılması her zaman mümkün veya mantıklı olmayabilir[210]. McDonald ve Cranor tarafından yapılan bir araştırmada eğer internet kullanan bir Amerikalı'nın kendisine sunulan tüm gizlilik politikalarını okuması durumunda, bu kişinin her gün kırk dakikasını gizlilik politikalarını okumaya ayırması gerektiği ortaya çıkmıştır[211]. Bu sebeple uygulamada ilgili kişiler genellikle gizlilik politikalarını okumadan veya anlamadan kabul etme eğilimi göstermeye başlamışlardır[212].

Veri sorumlularının uzun ve detaylı aydınlatma metinlerini ilk seferde ilgili kişilere doğrudan sunmak yerine aydınlatma yükümlülüklerini katmanlı bilgilendirme yöntemiyle parça parça yerine getirmeleri mümkündür. Katmanlı bilgilendirmenin çevrimiçi ortamlarda, simgeler vasıtası ile mobil ve akıllı cihazlarda gerçekleştirilebilmesi mümkündür[213]. Kurum tarafından yapılan bir tanımlamada katmanlı bilgilendirme; "*kişisel verilerin elde edilmesi sırasında ilgili kişisel verilerinin elde edildiği konusunda ön bilgilendirme yapılarak, ilgili kişinin*

---

[210] **Kişisel Verileri Koruma Kurumu**, Kişisel Verilerin Korunması Hakkında Sıkça Sorulan Sorular, s. 90.
[211] **Armin Gerl, Bianca Meier**, "The Layered Privacy Language Art. 12 – 14 GDPR Extension – Privacy Enhancing User Interfaces", Datenschutz und Datensich - DuD, Cilt 43, s. 747-752, 2019, s. 1.
[212] **a.g.e.**
[213] **Aşıkoğlu**, "Veri Sorumlularının Aydınlatma Yükümlülüğü -Avrupa Birliği ve Türk Hukukunda-", s. 46.

Kanunun 10. maddesine uygun aydınlatmaya yönlendirilmesini[214]" ifade etmektedir. Information Commissioner's Office tarafından yapılan tanıma göre katmanlı bilgilendirme ("*A layered approach*" olarak anılmıştır.), daha detaylı ilave bilgi katmanlarına sahip temel gizlilik bilgilerinden oluşan kısa bilgilendirmeler olarak tanımlanmıştır[215]. Katmanlı bilgilendirmede bir anda yoğun ve uzun bir bilgilendirme yapmak yerine, bilgilendirmenin kısa ve sade bir ifadeyle zamana yayılarak parça parça yapılması gündeme gelmektedir.

Aydınlatma yükümlülüğünün fiziki veya elektronik ortamlarda yerine getirilmesi mümkündür (Tebliğ m. 5/1). Örneğin bir işyerinde güvenlik amacıyla kamera kaydı yapılması, buna ilişkin olarak ortak alanlara işyerinde kamera kaydı yapıldığına ilişkin bir kamera resminin bulunduğu uyarı levhasının asılması ve uyarı levhasının altına çalışanın detaylı aydınlatma metnine ulaşabilmesi için bir internet sitesi adresinin veya iletişime geçilecek kişinin bilgilerinin yazılması katmanlı bilgilendirmenin ilk aşamasına örnek olarak verilebilir. Katmanlı aydınlatma metninde asgari olarak veri sorumlusunun kimliği, aydınlatma ön bilgisi ve detaylı aydınlatma metnine erişim için bir yönlendirme ibaresi bulunmalıdır[216]. Bir önceki örnekte aydınlatma ön bilgisi kamera simgesi iken "bu işyerinde güvenlik amaçlı kamera kaydı yapılmaktadır" ibaresi de aydınlatma ön bilgisi olacaktır.

Katmanlı bilgilendirmenin elektronik ortamda yapılması durumunda veri sorumlusu tarafından ilgili kişiye en azından veri işleme amaçları, veri sorumlusunun kimliği ve ilgili kişinin haklarına ilişkin bir içeriğin şeffaflık (*transparency*) ilkesi uyarınca sunulması gerekmektedir[217]. Örneğin bir internet sitesinde açılan pop-up pencere üzerinde çerezlere ilişkin ilgili kişiden alınacak açık

---

[214] **Kişisel Verileri Koruma Kurumu**, Aydınlatma Rehberi, s. 8.
[215] **Information Commissioner's Office**, Guide to the General Data Protection Regulation (GDPR), 22 Mayıs 2019 - 1.0.699, (Çevrimiçi) https://ico.org.uk/media/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr-1-0.pdf Erişim Tarihi: 27 Mart 2020, s. 98.
[216] **Kişisel Verileri Koruma Kurumu**, Aydınlatma Rehberi, s. 19.
[217] **Article 29 Data Protection Working Party**, Guidelines on Transparency Under Regulation 2016/679, 11 Nisan 2018, 17/EN, WP260 rev.01, (Çevrimiçi) https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=622227 Erişim Tarihi: 27 Mart 2020, s. 19.

rıza için ilgili kişinin rızasını ortaya koyan olumlayıcı bir eylem (*affirmative action*) ortaya koyması gerekmektedir. Olumlayıcı eylem kavramı GDPR'ın m. 4/1-11 hükmündeki rıza (*consent*) tanımı içerisinde sayılan şartlardan bir tanesidir[218]. Bu kapsamda internet sayfasında sağlanacak opt-in ve opt-out seçeneklerini kullanarak ilgili kişi hangi veri işleme faaliyetlerine izin verdiğini hangilerine izin vermediğini, pop-up penceresinde yapılan kısa aydınlatmalar ve detaylı aydınlatma metinlerine yönlendiren linklerin varlığı sayesinde rahatça anlayabilecektir. Burada ilgili kişinin verilerinin işlenmesine ilişkin ortaya koyacağı rızanın geçerli olabilmesi için rızasını ortaya koyan olumlayıcı bir eylem yapması gerekmektedir. Bu sebeple internet sitesinde ilgili kişinin doldurması gereken kutucukların önceden varsayılan olarak doldurulmuş olmaması gerekmektedir[219]. Bu şekilde önceden işaretlenmiş şekilde ilgili kişinin olumlayıcı bir aksiyon yapmasına gerek kalmadan alınan rızalar geçersizdir. Kaldı ki bu şekilde alınan rızaların geçersiz olduğu hususu Kurulun 27 Şubat 2020 tarihli ve 2020/173 sayılı Amazon kararında belirtilmiştir[220].

1.4. İstisnalar

Aydınlatma yükümlülüğünün veri sorumlusu veya yetkilendirdiği kişi tarafından yapılması genel kural olsa da bu kuralın da istisnaları mevcuttur. Kanunun istisnaları düzenleyen 28. maddesinde; Kanunun tamamen kapsamı dışında kalan hallerin düzenlenmesinin yanı sıra aydınlatma yükümlülüğünün yerine getirilmesine ilişkin de bazı istisnalar düzenlenmiştir.

---

[218] **Damian Clifford, Inge Graef, Peggy Valcke**, "Pre-formulated Declarations of Data Subject Consent—Citizen-Consumer Empowerment and the Alignment of Data, Consumer and Competition Law Protections", German Law Journal, Cilt 20, Sayı 5, s. 679-721, 2019, s. 704.

[219] ABAD'ın 1 Ekim 2019 tarihli ve C-673/17 sayılı Planet49 kararı, yüksek mahkeme tarafından bir İnternet sitesinin GDPR öncesi dönemdeki çerez kullanımı hakkında GDPR'ın yürürlüğe girmesinden sonra verilmiş ilk karardır ve çerez kullanımının şartları ve özellikle rızanın alınması bakımından başka tespitlerin yanı sıra bu önemli tespiti barındırmaktadır. Karara şu uzantıdan ulaşabilirsiniz:
http://curia.europa.eu/juris/document/document.jsf;jsessionid=E1263B9218236FAB0174B7EB1208B0E7?text=&docid=218462&pageIndex=0&doclang=en&mode=lst&dir=&occ=first&part=1&cid=609404 Erişim Tarihi: 27 Mart 2020.

[220] Kurulun 27.02.2020 tarihli ve 2020/173 sayılı kararına şu uzantıdan ulaşabilirsiniz: https://www.kvkk.gov.tr/Icerik/6739/2020-173 Erişim Tarihi: 17 Mayıs 2020. Bahsi geçen karar bu bölümün 1.2.2. ve 3.4. numaralı başlıkları altında kısım kısım incelenmiştir.

Kanunun 28. maddenin birinci fıkrası uyarınca;

i. "Kişisel verilerin, üçüncü kişilere verilmemek ve veri güvenliğine ilişkin yükümlülüklere uyulmak kaydıyla gerçek kişiler tarafından tamamen kendisiyle veya aynı konutta yaşayan aile fertleriyle ilgili faaliyetler kapsamında işlenmesi,

ii. Kişisel verilerin resmi istatistik ile anonim hâle getirilmek suretiyle araştırma, planlama ve istatistik gibi amaçlarla işlenmesi,

iii. Kişisel verilerin millî savunmayı, millî güvenliği, kamu güvenliğini, kamu düzenini, ekonomik güvenliği, özel hayatın gizliliğini veya kişilik haklarını ihlal etmemek ya da suç teşkil etmemek kaydıyla, sanat, tarih, edebiyat veya bilimsel amaçlarla ya da ifade özgürlüğü kapsamında işlenmesi,

iv. Kişisel verilerin millî savunmayı, millî güvenliği, kamu güvenliğini, kamu düzenini veya ekonomik güvenliği sağlamaya yönelik olarak kanunla görev ve yetki verilmiş kamu kurum ve kuruluşları tarafından yürütülen önleyici, koruyucu ve istihbari faaliyetler kapsamında işlenmesi,

v. Kişisel verilerin soruşturma, kovuşturma, yargılama veya infaz işlemlerine ilişkin olarak yargı makamları veya infaz mercileri tarafından işlenmesi."

durumlarında Kanun hükümlerinin uygulanmayacağı düzenlendiğinden veri sorumlusunun aydınlatma yükümlülüğü bulunmayacaktır.

Yukarıda sayılan Kanunun getirdiği genel istisna durumlarına ek olarak, özel istisna hallerinin belirtildiği Kanunun 28. maddesinin ikinci fıkrası uyarınca:

i. "Veri işlemenin suç işlenmesinin önlenmesi veya suç soruşturması için gerekli olması;

ii. İlgili kişinin kendisi tarafından alenileştirilmiş kişisel verilerin işlenmesi;

iii. Kişisel veri işlemenin kanunun verdiği yetkiye dayanılarak görevli ve yetkili kamu kurum ve kuruluşları ile kamu kurumu niteliğindeki meslek kuruluşlarınca, denetleme veya düzenleme görevlerinin

yürütülmesi ile disiplin soruşturma veya kovuşturması için gerekli olması;

iv. Kişisel veri işlemenin bütçe, vergi ve mali konulara ilişkin olarak devletin ekonomik ve mali çıkarlarının korunması amacıyla gerekli olması"

durumunda veri sorumlusunun aydınlatma yükümlülüğü, Kanunun amacına ve temel ilkelerine uygun ve orantılı olmak kaydıyla, uygulanmayacaktır.

1.5. İdari Yaptırım

Kanunun 18. maddesi uyarınca Kanunun 10. maddesinde düzenlenen aydınlatma yükümlülüğünün yerine getirilmemesi durumunda ilgili veri sorumlularına 5.000 Türk Lirası'ndan 100.000 Türk Lirası'na kadar idari para cezası verilecektir.

Kanunun 18. Maddesindeki tüm idari para cezaları her sene o yılın yeniden değerleme oranlarına göre hesaplanarak güncel idari para cezasının miktarı belirlenecektir.

Aydınlatma yükümlülüğünün yerine getirilmemesi durumunda uygulanacak idari para cezası için 2020 yılında uygulanacak alt sınır 9.013 Türk Lirası iken üst sınırı ise 180.264 Türk Lirası'dır.

2. İLGİLİ KİŞİLER TARAFINDAN YAPILAN BAŞVURULARI CEVAPLANDIRMA VE KURUL KARARLARINI YERİNE GETİRME YÜKÜMLÜLÜĞÜ

2.1. Genel Olarak

İlgili kişilerin Kanundan kaynaklı ve Kanunun uygulanması ile ilgili taleplerini iletebilmeleri ve kendilerine ait kişisel verilerine ilişkin haklarını koruyabilmek adına çeşitli hak arama yöntemleri belirlenmiştir.

İlgili kişi tarafından yapılan başvuruların cevaplandırılması yükümlülüğü, ilgili kişinin kendi kişisel verileri hakkında bilgi edinme hakkı ile bağlantılı bir

kavram olup, bilgi edinme hakkını kullanan ilgili kişiye verilecek cevaplar açık, anlaşılır ve sade olmalıdır[221].

2.2. İlgili Kişinin Hakları

Kanunun "İlgili kişinin hakları" başlıklı 11. maddesi uyarınca ilgili kişi;

- "Kişisel verilerinin işlenip işlenmediğini öğrenme
- Kişisel verileri işlenmişse buna ilişkin bilgi talep etme
- Kişisel verilerinin işlenme amacını ve bunların amacına uygun kullanılıp kullanılmadığını öğrenme
- Yurt içinde veya yurt dışında kişisel verilerin aktarıldığı üçüncü kişileri bilme
- Kişisel verilerin eksik veya yanlış işlenmiş olması hâlinde bunların düzeltilmesini isteme
- Kişisel verilerin silinmesini veya yok edilmesini isteme
- Kişisel verilerin düzeltilmesi, silinmesi veya yok edilmesine ilişkin işlemlerin kişisel verilerin aktarıldığı üçüncü kişilere bildirilmesini isteme
- İşlenen verilerin münhasıran otomatik sistemler vasıtasıyla analiz edilmesi suretiyle kişinin kendisi aleyhine bir sonucun ortaya çıkmasına itiraz etme
- Kişisel verilerin kanuna aykırı olarak işlenmesi sebebiyle zarara uğraması hâlinde zararın giderilmesini talep etme"

haklarını veri sorumlusundan her zaman talep edebileceği düzenlenmiştir.

2.3. Veri Sorumlusuna Başvuru Usulü

İlgili kişinin Kanunun uygulanmasıyla ilgili taleplerini veri sorumlusuna ne şekilde ileteceği hususu Kanunun 13. maddesinde ve bu maddeye dayanılarak Kurum tarafından hazırlanıp 10.03.2018 tarihli ve 03356 sayılı Resmî Gazete'de

[221] **Başalp**, s. 49.

yayımlanarak aynı tarihte yürürlüğe giren "Veri Sorumlusuna Başvuru Usul ve Esasları Hakkında Tebliğ[222]" içerisinde düzenlemiştir.

Tebliğin 4. maddesi uyarınca; "kişisel verisi işlenen gerçek kişiler, veri sorumlusuna başvuru hakkına" sahip olduğu ve ilgili kişilerin, başvurularını Türkçe olarak yapmak kaydıyla bu haktan yararlanabilecekleri düzenlenmiştir. Bu düzenlemeden hareketle Türkçe dilinde yapılmayan başvuruların dikkate alınmama olasılığı gündeme gelebilecektir. Hiç şüphesiz böyle bir durum temel hak ve özgürlüklerden kabul edilen kişisel verilerin korunması kavramı ile bağdaşmayacaktır. Bu sebeple örneğin İngilizce hizmet veren bir şirkete ilgili kişi tarafından başvurunun İngilizce yapılması sebebiyle şirketin başvuruya cevap vermemesi Kanunun genel ilkelerinden yola çıkarak hem dürüstlük kuralına hem de hakkaniyete aykırı olacağından veri sorumlusunun İngilizce başvuruyu kabul etmesi gerektiği kanaatindeyiz. Örneğin, İngilizce hizmet veren bir şirket hakkında ilgili kişinin şirkete yaptığı İngilizce başvuruya şirketin cevap vermemesi durumunda Kurul, Tebliğ'deki açık düzenlemeye rağmen herhangi bir yaptırım uygulayacak mıdır? Mevcut yasal düzenlemeye göre bunun pek mümkün olmadığı söylenebilecek olsa da böyle bir durumun hem dürüstlük kuralına hem de hakkaniyete aykırılık yaratacak olması sebebiyle, Kurulun olası bir uyuşmazlıkta, şirketlerin kendisine yapılan başvurularda Türkçe'ye ek olarak hizmetlerini sunarken kullandıkları dillerdeki başvuruları da kabul etmeleri gerektiğine ilişkin bir ilke kararı alması muhtemeldir.

Veri sorumlusuna başvuru usulü hakkındaki Kanunun 13. maddesinin birinci fıkrası uyarınca; "ilgili kişinin, Kanunun uygulanmasıyla ilgili taleplerini yazılı olarak veya Kurulun belirleyeceği diğer yöntemlerle veri sorumlusuna iletmesi" gerektiği düzenlenmiştir. Burada bahsedilen yazılı başvuru dışındaki "Kurulun belirleyeceği diğer yöntemlerin" neler olduğu hususu Tebliğin 5. maddesinin birinci fıkrasında açıklanmıştır. Tebliğin "Başvuru usulü" başlıklı m. 5/1 hükmü

[222] Kurum tarafından hazırlanıp 10.03.2018 tarihli ve 03356 sayılı Resmî Gazete'de yayımlanan Veri Sorumlusuna Başvuru Usul ve Esasları Hakkında Tebliğ'e şu uzantıdan ulaşabilirsiniz: https://www.resmigazete.gov.tr/eskiler/2018/03/20180310-6.htm Erişim Tarihi: 2 Nisan 2020. Bu başlık altında "Tebliğ" olarak anılacaktır.

uyarınca; "ilgili kişi, Kanunun 11. maddesinde belirtilen hakları kapsamındaki taleplerini, yazılı olarak başvurabilmenin dışında kayıtlı elektronik posta (KEP) adresi üzerinden veya güvenli elektronik imza, mobil imza ya da ilgili kişi tarafından veri sorumlusuna daha önce bildirilen ve veri sorumlusunun sisteminde kayıtlı bulunan elektronik posta adresini kullanmak suretiyle veya başvuru amacına yönelik geliştirilmiş bir yazılım ya da uygulama vasıtasıyla veri sorumlusuna iletebileceği" düzenlenmiştir.

Tebliğin m. 5/2 hükmü uyarınca ilgili kişi tarafından yapılacak başvuruda;

i. "başvuranın ad, soyad bilgilerinin ve başvuru yazılı ise imzasının,

ii. Türkiye Cumhuriyeti vatandaşları için T.C. kimlik numarasının, yabancılar için uyruğu, pasaport numarası veya varsa kimlik numarasının,

iii. tebligata esas yerleşim yeri veya iş yeri adresinin,

iv. varsa bildirime esas elektronik posta adresi, telefon ve faks numarasının,

v. talep konusunun"

bulunması zorunludur. Tebliğde ilgili kişinin başvurusunda bu unsurların bulunmasının zorunlu olduğunun belirtilmesinden hareketle bu unsurlardan birinde dahi eksiklik olması halinde başvurunun yapılmamış sayılma yaptırımı ile karşı karşıya kalabileceğini düşünmekteyiz. Eğer öyleyse ilgili kişinin buna mutlaka dikkatinin çekilmesi gerekir. Buna ilişkin bir ibare mutlaka aydınlatma metninde yer almalıdır.

Tebliğin 5. maddesinin devam fıkraları uyarınca başvuru konusuna ilişkin bilgi ve belgeler başvuruya eklenmelidir. İlgili kişi tarafından yazılı olarak yapılan başvurularda, veri sorumlusuna veya temsilcisine evrakın tebliğ edildiği tarih, başvuru tarihi olacaktır. Diğer yöntemlerle yapılan başvurularda ise başvurunun veri sorumlusuna ulaştığı tarih, başvuru tarihi kabul edilecektir.

Kanunun m. 13/2 ve benzer şekilde düzenleme yapılan Tebliğin m. 6/5 hükmü uyarınca; "veri sorumlusunun; başvuruda yer alan talepleri, talebin niteliğine göre en kısa sürede ve en geç otuz gün içinde ücretsiz olarak sonuçlandırmakla yükümlü" olduğu düzenlenmiştir. Ancak, başvuruya cevap

verebilmek için yapılacak işlem veya işlemlerin veri sorumlusu üzerinde ayrıca bir maliyet yaratması durumunda veri sorumlusu, başvuru sahibinden Kurul tarafından belirlenen tarifedeki ücreti almayı talep edebilir.

Kanunun m. 13/3 hükmü ve Tebliğin m. 6/2 ve 6/3 hükümleri uyarınca veri sorumlusunun başvuranın talebine iki farklı cevap verebileceği sınırlı sayıda düzenlenmiştir. Buna göre veri sorumlusu başvuranın talebini kabul edecek veya gerekçesini açıklayarak reddedebilecektir. Ancak her halükârda verilecek cevap ilgili kişiye yazılı olarak veya elektronik ortamda bildirilmesi gerekecektir. Başvuruda yer alan talebin kabul edilmesi hâlinde talebin gereği veri sorumlusunca yerine getirilmeli ve ilgili kişiye bu hususta bilgi verilmesi gereklidir. Kanunun m. 13/3 hükmünün son cümlesi ve Tebliğin m. 6/5 hükmünün son cümlesi uyarınca başvurunun, veri sorumlusunun hatasından kaynaklanması durumunda başvurandan alınan ücretin ilgiliye iade edilmesi gerektiği düzenlenmiştir.

Tebliğin "Ücret" başlıklı 7. maddesi uyarınca ilgili kişinin başvurusuna yazılı olarak cevap verilecekse, on sayfaya kadar olan cevaplarda başvurandan herhangi bir ücret alınmayacağı düzenlenmiştir. On sayfanın üzerindeki her sayfa için 1 Türk Lirası işlem ücreti alınabilir[223]. Veri sorumlusu tarafından başvuruya flash bellek, CD gibi bir kayıt ortamında cevap verilmesi halinde, veri sorumlusu tarafından başvurandan talep edilebilecek ücret kayıt ortamının maliyetini geçemeyecektir.

2.4. Şikâyet Hakkı

İlgili kişi tarafından veri sorumlusuna yapılan başvurunun kabul edilmemesi veya veri sorumlusu tarafından verilmiş olan cevabın yeterli olmaması ya da başvuruya veri sorumlusu tarafından hiç cevap verilmemesi hallerinde ilgili kişinin Kurula şikâyette bulunabileceği düzenlenmiştir.

İlgili kişinin Kurula şikâyet hakkı ve bu şikâyet hakkına ilişkin usul ve esaslar Kanunun 14. ve 15. Maddelerinde düzenlenmiştir.

[223] Burada belirtilen 1 Türk Lirası, Tebliğin 2018 yılında yayımlanan orijinal halindeki tutardır. Bu tutarın her yıl yeniden değerleme oranına göre hesaplanarak güncel tutarın belirlenmesi gerekebilir.

Kanunun "Kurula şikâyet" başlıklı 14. maddesi uyarınca; "*ilgili kişinin yaptığı başvurunun reddedilmesi, verilen cevabın yetersiz bulunması veya başvuruya veri sorumlusu tarafından süresinde cevap verilmemesi hâllerinde; ilgili kişi, veri sorumlusunun cevabını öğrendiği tarihten itibaren otuz ve halükârda başvuru tarihinden itibaren altmış gün içinde Kurula şikâyette bulunabileceği*" düzenlenmiştir. Burada dikkat edilmesi gereken bir husus ilgili kişinin her halükârda başvuru tarihinden itibaren Kurula şikâyet için altmış günlük süresi bulunmamaktadır. Eğer ilgili kişi veri sorumlusuna başvuru yaptıktan sonra, veri sorumlusu ilgili kişinin başvuru tarihinden sonraki beşinci günde ilgili kişiye yazılı olarak cevap verdiyse, bu durumda ilgili kişi veri sorumlusunun bu cevabını öğrendiği tarihten itibaren Kurula şikâyet başvurusu yapabilmek için otuz günlük süresi olacaktır. Veri sorumlusunun kendisine yapılan başvuruya cevap vermek için otuz günlük süresi olduğundan, eğer veri sorumlusu bu başvuruya hiçbir şekilde otuz gün içerisinde cevap vermezse otuzuncu günün sonunda cevap verme süresi biteceği için bu süreden sonra ilgili kişinin Kurula şikâyet başvurusunda bulunmak için otuz günlük başvuru süresi başlayacaktır. Diğer bir ifadeyle veri sorumlusunun otuz günlük süre içerisinde ilgili kişiye hiç cevap vermemesi veya otuzuncu günde cevap vermesi durumunda, ilgili kişinin veri sorumlusuna başvuru tarihinden itibaren Kurula şikâyette bulunabilmek için en fazla altmış günlük bir süresi (ilk otuz gün veri sorumlusunun cevap süresi ve ikinci otuz gün veri sorumlusunun cevap süresi sona erdikten sonraki Kurula başvuru süresi) olacaktır. Bu konuda uygulamada sürelerin yorumlanmasında farklılıklar olduğu için Kurul 24.01.2019 tarihli ve 2019/9 sayılı kararı[224] ile konuya açıklık getirmiştir:

> "*Kurumumuza intikal eden şikâyet başvurularının incelenmesi neticesinde veri sorumlusuna başvuru yolunu tüketen ilgili kişiler tarafından Kurula şikâyette bulunulması sürecinde Kanunda yer alan sürelerin yorumlanmasında farklılıklar olduğu görülmüştür. Bu itibarla Kanunun 14 üncü maddesinin (1) numaralı fıkrası uyarınca;*

[224] Kurulun 24.01.2019 tarihli ve 2019/9 sayılı kararına şu uzantıdan ulaşabilirsiniz: https://www.kvkk.gov.tr/Icerik/5358/Kamuoyu-Duyurusu Erişim Tarihi: 2 Nisan 2020.

İlgili kişi tarafından yapılan başvuruya veri sorumlusunca 30 gün içinde bir cevap verilmesi halinde ilgili kişinin veri sorumlusunun cevabını müteakip 30 gün içerisinde şikâyette bulunabileceği, bu itibarla söz konusu hallerde ilgili kişinin veri sorumlusuna başvurduğu tarihten itibaren 60 günlük süresinin bulunmadığı,

İlgili kişi tarafından yapılan başvuruya veri sorumlusunca bir cevap verilmediği durumda ise ilgili kişinin veri sorumlusuna başvurduğu tarihten itibaren 60 gün içinde Kurula şikâyette bulunabileceği,

İlgili kişi tarafından yapılan başvuruya veri sorumlusunca Kanunda tanınan 30 günlük süre sonrasında bir cevap verilmesi halinde ilgili kişinin, Kanunda veri sorumlusuna tanınan 30 günlük süre sonrasında verilecek cevabı beklemekle yükümlü olmadığı ve veri sorumlusuna tanınan sürenin dolması ile birlikte Kurula şikâyette bulunabileceği göz önüne alınarak, ilgili kişinin veri sorumlusunun kendisine cevap verdiği tarihten itibaren 30 gün değil, veri sorumlusuna başvurduğu tarihten itibaren 60 gün içinde Kurula şikâyette bulunabileceği"

Kanunun 13. maddesi uyarınca düzenlenen veri sorumlusuna başvuru yolu tüketilmeden Kurula şikâyet yoluna başvurulamaz (Kanun, m. 13/2). Kurula şikâyet hakkına ek olarak kişilik hakları ihlal edilen kişilerin, genel hükümlere göre tazminat talep etme haklarının olduğu düzenlenmiştir (Kanun, m. 13/3). Bu durumda ilgili kişi kişilik hakkının ihlali sebebiyle yargı yoluna başvurarak genel hükümler uyarınca mahkemeden kişilik hakkını ihlal eden kişiyi kendisine uygun bir tazminat ödemeye hükmetmesini talep edebilecektir[225].

Kanunun m. 15/1 hükmü uyarınca; "Kurul, şikâyet üzerine veya ihlal iddiasını öğrenmesi durumunda re'sen (*ex officio, kendiliğinden*), görev alanına giren konularda gerekli incelemeyi yapacağı" düzenlenmiştir. Ek olarak Kanunun

[225] **Kişisel Verileri Koruma Kurumu**, İlgili Kişinin Hak Arama Rehberi, s. 6. İsmi geçen rehbere şu uzantıdan ulaşabilirsiniz: https://www.kvkk.gov.tr/SharedFolderServer/CMSFiles/7226b55d-b1e7-4e78-a3c4-0b1ba82ce542.pdf Erişim Tarihi: 2 Nisan 2020.

m. 15/2 hükmü uyarınca Kurul'un; "01.11.1984 tarihli ve 3071 sayılı Dilekçe Hakkının Kullanılmasına Dair Kanunun 6. maddesinde belirtilen şartları taşımayan ihbar veya şikâyetleri incelemeye almayacağı" düzenlenmiştir. Bu doğrultuda ismi geçen kanunun 6. Maddesi uyarınca;

i. "Belli bir konuyu ihtiva etmeyen,

ii. Yargı mercilerinin görevine giren konularla ilgili olan,

iii. 4. maddede gösterilen şartlardan herhangi birini taşımayan"

dilekçeler incelemeye alınmayacaktır. Dilekçe Hakkının Kullanılmasına Dair Kanunun "Dilekçede bulunması zorunlu şartlar" başlıklı 4. maddesi uyarınca dilekçede;

i. "dilekçe sahibinin adı-soyadı,

ii. imzası,

iii. iş veya ikametgâh adresinin"

bulunması zorunludur. Dolayısıyla buradaki şartları taşımayan başvurular Kurul tarafından değerlendirilmeyecektir.

İlgili kişilerin e-Devlet bilgileriyle giriş yaparak Kurula şikayet edebilmeleri için Kurumun internet sitesinde bir şikayet modülü[226] oluşturulmuş ve bu modülün kullanımına ilişkin Kurul tarafından "KVKK Şikayet Modülü Kılavuzu[227]" yayınlanmıştır. Böylece ilgili kişiler Kurula şikayetlerini dilerlerse Kurumun internet sitesindeki şikâyet modülü üzerinden de yapabileceklerdir.

İlgili kişinin Kurala yaptığı usulüne uygun şikâyet üzerine Kurul, ilgili kişinin talebini inceler ve ilgililere cevap verir ancak; şikâyetin yapıldığı tarihten itibaren altmış gün içerisinde cevap verilmezse talep Kurul tarafından reddedilmiş sayılır (Kanun, m. 15/4).

Kurulun şikâyet üzerine ya da kendiliğinden yaptığı inceleme neticesinde, bir ihlalin var olduğunu tespit etmesi durumunda Kurul, tespit ettiği hukuka aykırılıkların veri sorumlusunca giderilmesine karar vererek bu kararını ilgililere

---

[226] Kurumun oluşturduğu şikâyet modülüne şu uzantıdan ulaşabilirsiniz: https://sikayet.kvkk.gov.tr/ Erişim Tarihi: 3 Nisan 2020.

[227] KVKK Şikâyet Modülü Kılavuzuna şu uzantıdan ulaşabilirsiniz: https://kvkk.gov.tr/SharedFolderServer/CMSFiles/1624cbad-5ea1-4d73-8519-4a4835eebdb3.pdf Erişim Tarihi: 3 Nisan 2020.

tebliğ eder. Kurulun bu kararı, tebliğden itibaren gecikmeksizin ve en geç otuz gün içinde yerine getirilmek zorundadır (Kanun, m.15/5).

İlgili kişinin şikâyeti üzerine veya Kurul tarafından re'sen yapılan inceleme neticesinde ihlalin yaygın olduğunun tespit edilmesi durumunda Kurul, bu konuyla ilgili bir ilke kararı alabilir ve bu kararını yayımlayabilir (Kanun, m.15/6).

Kanunun 15. maddesinin yedinci fıkrası uyarınca Kurul, kendisine yapılan şikâyet başvurusunu inceledikten sonra ortada telafisi güç veya imkânsız zararların bulunduğunu ve açıkça hukuka aykırılık olduğunu tespit etmesi durumunda, şikâyete taraf veri sorumlusu bünyesinde veri işleme faaliyetinin ya da kişisel verilerin yurt dışına aktarılmasının durdurulmasına karar verebilir.

2.5. İstisnalar

İlgili kişinin kanundan kaynaklanan haklarını kullanması genel kural olsa da bu kuralın da istisnaları mevcuttur. Kanunun istisnaları düzenleyen 28. maddesinde; Kanunun tamamen kapsamı dışında kalan hallerin düzenlenmesinin yanı sıra ilgili kişinin haklarını kullanmasına ilişkin de bazı istisnalar düzenlenmiştir.

İlgili kişinin uğradığı zararın giderilmesini isteme hakkı dışındaki hakları Kanunun 28. Maddesinin ikinci fıkrasında öngörülen bazı durumlarda uygulanmayacaktır. Kanunun m. 28/2 hükmü uyarınca;

> "*Bu Kanunun amacına ve temel ilkelerine uygun ve orantılı olmak kaydıyla veri sorumlusunun aydınlatma yükümlülüğünü düzenleyen 10 uncu, zararın giderilmesini talep etme hakkı hariç, ilgili kişinin haklarını düzenleyen 11 inci ve Veri Sorumluları Siciline kayıt yükümlülüğünü düzenleyen 16 ncı maddeleri aşağıdaki hâllerde uygulanmaz:*
>
> *a) Kişisel veri işlemenin suç işlenmesinin önlenmesi veya suç soruşturması için gerekli olması.*
>
> *b) İlgili kişinin kendisi tarafından alenileştirilmiş kişisel verilerin işlenmesi.*
>
> *c) Kişisel veri işlemenin kanunun verdiği yetkiye dayanılarak görevli ve yetkili kamu kurum ve kuruluşları ile kamu kurumu*

niteliğindeki meslek kuruluşlarınca, denetleme veya düzenleme görevlerinin yürütülmesi ile disiplin soruşturma veya kovuşturması için gerekli olması.

ç) Kişisel veri işlemenin bütçe, vergi ve mali konulara ilişkin olarak Devletin ekonomik ve mali çıkarlarının korunması için gerekli olması."

GDPR'ın "Kısıtlamalar (*Restrictions*)" başlıklı 23. maddesi uyarınca ilgili kişinin hakları bakımından ciddi istisnalar getirilmiştir. Söz konusu madde uyarınca; veri sorumlusu (*data controller*) veya veri işleyenin (*processor*) tabi olduğu Birlik veya üye devlet hukukunda ilgili kişinin sahip olduğu haklarının temel hak ve özgürlüklerin özüne saygı göstermek ve demokratik bir toplumda gerekli ve ölçülü olmak şartıyla bir yasama tedbiriyle aşağıda sayılı haller çerçevesinde kısıtlanabileceği düzenlenmiştir:

i. "Milli güvenlik
ii. Savunma
iii. Kamu güvenliği
iv. Kamu güvenliğine yönelik tehditlere karşı güvence sağlanması ve bu tehditlerin engellenmesi de dahil olmak üzere suçların önlenmesi, soruşturulması, tespit edilmesi ya da kovuşturulması veya cezaların infaz edilmesi
v. Birlik veya üye devletin genel kamu menfaati için önemli olan diğer amaçlar; özellikle parasal, bütçesel, vergisel konular ve kamu sağlığı ile sosyal güvenlik konuları dahil olmak üzere Birlik veya üye devletin önemli ekonomik veya mali menfaati
vi. Yargı bağımsızlığının ve adli süreçlerin korunması
vii. Profesyonel mesleklere ilişkin etik kural ihlallerinin önlenmesi, soruşturulması, tespit edilmesi ya da kovuşturulması
viii. Resmi bir yetkinin kullanımı ile bağlantılı bir izleme, denetleme veya düzenleme işlevi
ix. İlgili kişinin veya diğer kişilerin hak ve özgürlüklerinin korunması
x. Medeni hukuktan kaynaklanan taleplerin icra edilmesi"

2.6. İdari Yaptırım

Kanunun 18. maddesi uyarınca; Kurul tarafından ilgili kişinin şikâyet hakkını kullanması veya re'sen inceleme yapılması sonucunda verilen kararların veri sorumlusu tarafından yerine getirilmemesi durumunda ilgili veri sorumlularına 25.000 Türk Lirası'ndan 1.000.000 Türk Lirası'na kadar idari para cezası verileceği düzenlenmiştir.

Kanunun 18. maddesinde belirtilen tüm idari para cezaları her sene o yılın yeniden değerleme oranlarına göre hesaplanarak güncel idari para cezasının miktarı belirlenecektir.

Kurul tarafından verilen kararların yerine getirilmemesi durumunda uygulanacak idari para cezası için 2020 yılında uygulanacak alt sınır 45.066 Türk Lirası iken üst sınırı ise 1.802.641 Türk Lirası'dır.

3. VERİ GÜVENLİĞİNE İLİŞKİN YÜKÜMLÜLÜKLER

3.1. Genel Olarak

Kişisel verilerin etkili bir şekilde korunabilmesi için veri işleme faaliyetinin her aşamasında hem veri sorumluları hem de veri işleyenler tarafından işlenen verilerin güvenliğinin sağlanması gerekmektedir. Bu konuda Kanunun "Veri güvenliğine ilişkin yükümlülükler" başlıklı 12. maddesi uyarınca veri sorumlularına;

i. "kişisel verilerin hukuka aykırı olarak işlenmesini önlemek,
ii. kişisel verilere hukuka aykırı olarak erişilmesini önlemek,
iii. kişisel verilerin muhafazasını sağlamak,"

amacıyla uygun güvenlik seviyesini temin etmek için gerekli her türlü teknik ve idari önlemleri almak yükümlülükleri atfedilmiştir.

Kişisel verilerin korunması ile hedeflenen amacın bireyin korunması iken veri güvenliği kurallarıyla hedeflenen amacın verinin kendisini korumak olduğuna

ilişkin doktrinde görüş mevcuttur[228]. Bu görüşe katılmakla birlikte, ek olarak verinin kendisinin korunmasıyla ilgili kişinin mahremiyetinin de korunduğu ve aslında bunun da amaçlandığı kanaatindeyiz.

Kişisel verilerin, veri sorumlusu adına başka bir gerçek veya tüzel kişi tarafından işlenmesi durumunda hem veri sorumlusu hem de veri sorumlusu adına veri işleyen gerçek veya tüzel kişiler, yukarıda belirtilen tedbirlerin alınması hususunda müştereken sorumlulukları bulunmaktadır (Kanun, m. 12/2).

Kanunda veri güvenliğinin sağlanabilmesi için başkaca teminatlar da getirilmiştir. Bu kapsamda Kanunun 12. maddesinin üçüncü fıkrası uyarınca; "*Veri sorumlusu, kendi kurum veya kuruluşunda, bu Kanun hükümlerinin uygulanmasını sağlamak amacıyla gerekli denetimleri yapmak veya yaptırmak zorundadır.*" hükmü düzenlenmiştir. Bu düzenlemeye ek olarak veri sorumluları ile veri işleyen kişilerin, öğrendikleri kişisel verileri Kanun hükümlerine aykırı olarak başkasına açıklamamaları ve veri işleme amaçları dışında kullanmamaları gerektiği, bu yükümlülüğün veri sorumlusu veya veri işleyen kişinin görevinden ayrılmasından sonra da devam edeceği düzenlenmiştir (Kanun m. 12/4).

Kişisel Verileri Koruma Kurumu tarafından yayımlanan "Kişisel Veri Güvenliği Rehberi (Teknik ve İdari Tedbirler)[229]" ile veri güvenliğine ilişkin alınması gereken teknik ve idari tedbirler detaylı şekilde açıklanmıştır.

Veri güvenliği yükümlülüğüne ilişkin benzer bir düzenleme GDPR'ın "veri işlemenin güvenliği (*security of processing*)" başlıklı 32. maddesinde ve GDPR'ın gerekçesinin 83. maddesinde yapılmıştır. Bu kapsamda GDPR'da da Kanun'daki düzenlemeye benzer şekilde veri sorumluları ve veri işleyenlerin mevcut risklere uygun olacak bir güvenlik düzeyini sağlamak adına gerekli teknik ve idari tedbirleri alması gerekmektedir. GDPR'ın m. 32/1 hükmü uyarınca bu güvenlik tedbirlerine aşağıda sayılanlar örnek olarak gösterilmiştir:

i. Kişisel veriler üzerinde takma adlar kullanımı veya şifreleme

---

[228] **Küzeci**, s. 357.

[229] **Kişisel Verileri Koruma Kurumu**, Kişisel Veri Güvenliği Rehberi (Teknik ve İdari Tedbirler), Ankara 2018, (Çevrimiçi) https://www.kvkk.gov.tr/yayinlar/veri_guvenligi_rehberi.pdf Erişim Tarihi: 3 Nisan 2020. Bundan sonra bu başlık altında "Veri Güvenliği Rehberi" olarak anılacaktır.

ii. Veri işleme sistem ve hizmetlerinin gizlilik, uyum, geçerlilik ve direncinin devamlı şekilde sağlanabilmesi

iii. Fiziksel veya teknik bir olayın gerçekleşmesi durumunda kişisel verilerin geçerliliğinin ve kişisel verilere erişimin eski haline geri getirilebilmesi

iv. Veri işleme faaliyetinin güvenliğinin temini için teknik ve idari tedbirlerin düzenli şekilde test edilmesi, incelenmesi ve değerlendirilmesine ilişkin bir süreç oluşturulması

Yukarıda sayılan güvenlik tedbirleri GDPR kapsamında örnekleme yoluyla sayılmıştır ve veri sorumluları uygun gördükleri diğer önlemleri de alabileceklerdir. Uygulanması planlanan bir tedbiri belirlerken GDPR m. 32/1 hükmü uyarınca şu hususların değerlendirilmesi gerekmektedir:

i. En gelişmiş teknolojilerin incelenmesi

ii. Tedbire ilişkin uygulama maliyeti

iii. Veri işleme faaliyetinin amaçları, kapsamı, doğası, bağlamı

iv. Gerçek kişilerin hak ve özgürlükleri açısından çeşitli olasılık ve önemdeki risklerin bulunup bulunmadığı

Veri sorumluları ile veri işleyenler tarafından etkili ve yeterli şekilde güvenlik tedbirlerinin alınması durumunda günümüzde ciddi bir sıkıntı haline gelen siber saldırılara ve veri sızıntılarına meydan verilmemiş olunacak veya en azından bu sıkıntılara ilişkin riskler azaltılmış olunacaktır. Böylece bireylerin temel hak ve özgürlükleri korunurken, ticari hayatta da veri güvenliği ihlalleri sonucu meydana gelebilecek ekonomik kayıpların önüne geçilebilir.

3.2. Veri Güvenliğine İlişkin İdari Tedbirler

Veri Güvenliği Rehberi uyarınca veri güvenliğine ilişkin olarak alınması gereken idari tedbirler genel olarak aşağıdaki gibidir:

- "Mevcut risk ve tehditlerin belirlenmesi
- Çalışanların eğitilmesi ve çeşitli farkındalık çalışmaları yapılması
- Kişisel veri güvenliği politikalarının ve prosedürlerinin belirlenmesi
- Kişisel verilerin mümkün olduğunca azaltılması

- Veri işleyenler ile ilişkilerin yönetimi”

Yukarıda sayılan idari tedbirlerin dışında veri sorumlularının mevcut riskleri minimize edecek diğer uygun tedbirleri de almaları mümkündür. Bu kapsamda veri sorumluları tarafından veri güvenliğinin sağlanması adına alınabilecek diğer bazı idari tedbirler aşağıdaki gibidir[230]:

- “Kurumsal politikalar hazırlanması (Kişisel veri işleme, erişim, bilgi güvenliği, kullanım, saklama ve imha politikaları vb.)
- Kişisel veri işleme envanteri hazırlanması
- Sözleşmeler (Kişisel veri aktarımında veri sorumlusu - veri sorumlusu, veri sorumlusu - veri işleyen arasında sözleşme yapılması)
- Gizlilik taahhütnamelerinin hazırlanması
- Kurum bünyesinde periyodik ve/veya rastgele denetimlerin yapılması
- Risk analizlerinin yapılması
- İş sözleşmesi, disiplin yönetmeliği (Kanuna uygun hükümler ilave edilmesi)
- Kurumsal iletişim faaliyetlerinin yürütülmesi (Kriz yönetimi, Kurul ve ilgili kişiyi bilgilendirme süreçleri, itibar yönetimi vb.)
- Eğitim ve farkındalık faaliyetleri (Bilgi güvenliği ve Kanun)
- Veri sorumluları sicil bilgi sistemine (VERBİS) bildirim”

Kurul tarafından alınan 31.01.2018 tarihli ve 2018/10 sayılı karar ile birlikte "Özel Nitelikli Kişisel Verilerin İşlenmesinde Veri Sorumlularınca Alınması Gereken Yeterli Önlemler[231]" belirlenmiştir. Bu karar uyarınca;

> “*1- Özel nitelikli kişisel verilerin güvenliğine yönelik sistemli, kuralları net bir şekilde belli, yönetilebilir ve sürdürülebilir ayrı bir politika ve prosedürün belirlenmesi,*” gerektiği belirtilmiştir. Ayrıca;

[230] **Veri Güvenliği Rehberi**, s. 29.
[231] Kurul’un "Özel Nitelikli Kişisel Verilerin İşlenmesinde Veri Sorumlularınca Alınması Gereken Yeterli Önlemler”i içeren 31.01.2018 tarihli ve 2018/10 sayılı kararına şu uzantıdan ulaşabilirsiniz: https://www.kvkk.gov.tr/Icerik/4110/2018-10 Erişim Tarihi: 4 Nisan 2020.

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

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

b) Gizlilik sözleşmelerinin yapılması,

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

ç) Periyodik olarak yetki kontrollerinin gerçekleştirilmesi,

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

Bahsi geçen kararda verilerin bulunduğu ortamlara göre nasıl önlemler alınması gerektiği ne ilişkin elektronik ve fiziksel ortam ayrımına gidilerek çeşitli önlemler üzerinde durulmuştur. Kararın devamında;

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

a) Verilerin kriptografik yöntemler kullanılarak muhafaza edilmesi,

b) Kriptografik anahtarların güvenli ve farklı ortamlarda tutulması,

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

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

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

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

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

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

b) Bu ortamların fiziksel güvenliğinin sağlanarak yetkisiz giriş çıkışların engellenmesi," gerektiğinin üzerinde durulmuştur.

Kararda son olarak özel nitelikli kişisel verilerin üçüncü kişilere aktarılması diğer bir ifadeyle transfer edilmesine ilişkin çeşitli önlemlerden bahsedilmiştir. Buna göre;

"*5- Özel nitelikli kişisel veriler aktarılacaksa*

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

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

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

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

Kurul ayrıca kararında, yukarıda alıntılanan tedbirlere ek olarak; "Veri Güvenliği Rehberinde belirtilen ve uygun güvenlik düzeyini temin etmeye yönelik idari ve teknik tedbirlerin de veri sorumluları ve veri işleyenler tarafından dikkate alınması gerektiğini" belirtmiştir.

3.3. Veri Güvenliğine İlişkin Teknik Tedbirler

Veri Güvenliği Rehberi uyarınca veri güvenliğine ilişkin olarak alınması gereken idari tedbirler genel olarak aşağıdaki gibidir:

- "Siber güvenliğin sağlanması
- Kişisel veri güvenliğinin takibi
- Kişisel veri içeren ortamların güvenliğinin sağlanması
- Kişisel verilerin bulutta depolanması
- Bilgi teknolojileri sistemlerinin tedarik edilmesi, geliştirilmesi ve bakımı
- Kişisel verilerin yedeklenmesi"

Yukarıda sayılan teknik tedbirlerin dışında veri sorumlularının mevcut riskleri minimize edecek diğer uygun tedbirleri de almaları mümkündür. Bu kapsamda veri sorumluları tarafından veri güvenliğinin sağlanması adına alınabilecek diğer bazı idari tedbirler aşağıdaki gibidir[232]:

- "Yetki Matrisi
- Yetki Kontrol
- Erişim Logları
- Kullanıcı Hesap Yönetimi
- Ağ Güvenliği
- Uygulama Güvenliği
- Şifreleme
- Sızma Testi
- Saldırı Tespit ve Önleme Sistemleri
- Log Kayıtları
- Veri Maskeleme
- Veri Kaybı Önleme Yazılımları
- Yedekleme
- Güvenlik Duvarları

[232] **Veri Güvenliği Rehberi**, s. 29.

- Güncel Anti-Virüs Sistemleri
- Silme, Yok Etme veya Anonim Hale Getirme
- Anahtar Yönetimi"

Kurul tarafından sosyal medya şirketi Facebook hakkında verilen ihlal kararında şirketin veri güvenliğine ilişkin yeterli tedbirlerin alınmaması sebebiyle idari para cezası uygulamıştır[233]. Kurulun 11.04.2019 tarihli ve 2019/104 sayılı kararında özetle;

"*(...) Yapılan inceleme neticesinde,*

Facebook kullanıcı fotoğraflarına erişmek için üçüncü taraf uygulamalara izin veren bir fotoğraf API hatası keşfedildiği, Facebook tarafından yapılan inceleme sonrası bu durumu potansiyel bir yazılım bozukluğu olarak rapor ettiği,

API hatasının 13 Eylül - 25 Eylül 2018 tarihleri arasında 12 gün boyunca gerçekleştiği, bahse konu API hatasına Facebook tarafından zamanında müdahale edilmemesi bu konuda teknik ve idari tedbirlerin alınmasında eksikliklerin göstergesi olduğu, (...)

Facebook'un bahsi geçen üçüncü taraf uygulamaların normalde erişime izin verilmiş olan sayıdan daha fazla spesifik fotoğrafa gerçekten erişip erişemediklerini belirleyemediği dikkate alındığında, bu durumun Facebook'un kendi platformundaki veri akışını kontrol etme noktasında sıkıntılar yaşadığı ve bu kapsamdaki hususun Kanunun 12 nci maddesinin (1) numaralı fıkrasında öngörülen veri güvenliğine ilişkin yükümlülüklere aykırılık teşkil ettiği,

Açıklanan ihlalin 6,8 milyon kullanıcıyı ve 876 geliştirici tarafından oluşturulan 1.500 uygulamayı etkilemiş olabileceği,

Türkiye'de bulunan yaklaşık 300 bin kullanıcının veri ihlalinden etkilenmiş olabileceği, (...) hususları dikkate alınarak (...)

[233] Kurulun Facebook hakkında verdiği bir diğer ihlal kararı için Kurulun 18.09.2019 tarihli ve 2019/269 sayılı kararına bakabilirsiniz. Karara şu uzantıdan ulaşabilirsiniz: https://kvkk.gov.tr/Icerik/5534/2019-269 , Erişim Tarihi: 4 Nisan 2020.

Kanunun 12 nci maddesinin (1) numaralı fıkrası çerçevesinde gerekli teknik ve idari tedbirleri almadığı anlaşılan Facebook hakkında Kanunun 18 nci maddesinin (1) numaralı fıkrasının (b) bendi uyarınca 1.100.000 TL (...) idari para cezası uygulanmasına karar verilmiştir."

3.4. İhlal Bildirimi ve Kurul Kararları

Kanunun 12. maddesinin beşinci fıkrası uyarınca; "işlenen kişisel verilerin başkaları tarafından kanuni olmayan yollarla elde edilmesi hâlinde, veri sorumlusunun bu durumu en kısa sürede ilgilisine ve Kurula bildirmesi gerektiği, ayrıca gerekmesi halinde Kurulun, bu durumu Kurumun internet sitesinde veya uygun göreceği başka bir yöntemle ilan edebileceği" düzenlenmiştir.

Kişisel Verileri Koruma Kurulu 24.01.2019 tarihli ve 2019/10 sayılı kararı ile GDPR hükümlerini dikkate alarak veri ihlal bildirimlerine ilişkin çeşitli hususları düzenlemiştir. Bu kararla birlikte veri sorumluları tarafından gerekmesi halinde doldurulacak bir "Veri İhlali Bildirim Formu" ve yararlanılması için bir "Veri İhlali Bildirim Formu Kılavuzu" da hazırlanmıştır. Kurul bu kararını, formu ve kılavuzu Kurumun internet sitesinde yayınlamıştır[234].

Kurulun 24.01.2019 tarihli ve 2019/10 sayılı kararının, veri sorumluları tarafından yapılacak veri ihlal bildirimleri hakkında çeşitli hususlara değindiği kısmı aşağıdaki gibidir:

"Kanunun 12 nci maddesinin (5) numaralı fıkrasının 'İşlenen kişisel verilerin kanuni olmayan yollarla başkaları tarafından elde edilmesi hâlinde, veri sorumlusu bu durumu en kısa sürede ilgilisine ve Kurula bildirir….' hükmünde yer alan 'en kısa sürede' ifadesinin 72 saat olarak yorumlanmasına ve bu kapsamda veri sorumlusunun bu durumu öğrendiği tarihten itibaren gecikmeksizin ve en geç 72 saat içinde Kurula bildirmesine, veri sorumlusunca söz konusu veri ihlalinden etkilenen kişilerin belirlenmesini müteakip ilgili kişilere de

[234] Kurulun 24.01.2019 tarihli ve 2019/10 sayılı kararına, Veri İhlali Bildirim Formuna ve Veri İhlali Bildirim Formu Kılavuzuna şu uzantıdan ulaşabilirsiniz:
https://www.kvkk.gov.tr/Icerik/5362/Veri-Ihlali-Bildirimi Erişim Tarihi: 4 Nisan 2020.

makul olan en kısa süre içerisinde, ilgili kişinin iletişim adresine ulaşılabiliyorsa doğrudan, ulaşılamıyorsa veri sorumlusunun kendi web sitesi üzerinden yayımlanması gibi uygun yöntemlerle bildirim yapılmasına,

Veri sorumlusu tarafından Kurula haklı bir gerekçe ile 72 saat içinde bildirim yapılamaması halinde, yapılacak bildirimle birlikte gecikmenin nedenlerinin de Kurula açıklanmasına,

Kurula yapılacak bildirimde aşağıda yer verilen Kişisel Veri İhlal Bildirim Formu'nun kullanılmasına,

Formda yer alan bilgilerin aynı anda sağlanmasının mümkün olmadığı hallerde, bu bilgilerin gecikmeye mahal verilmeksizin aşamalı olarak sağlanmasına,

Veri sorumlusu tarafından veri ihlallerine ilişkin bilgilerin, etkilerinin ve alınan önlemlerin kayıt altına alınması ve Kurulun incelemesine hazır halde bulundurulmasına,

Veri işleyen nezdinde bulunan kişisel verilerin kanuni olmayan yollarla başkaları tarafından elde edilmesi halinde, veri işleyenin bu konuda herhangi bir gecikmeye yer vermeksizin veri sorumlusuna bildirimde bulunmasına,

Veri ihlalinin yurtdışında yerleşik veri sorumlusu nezdinde yaşanması halinde, bu ihlalin sonuçlarının Türkiye'de yerleşik ilgili kişileri etkilemesi ve ilgili kişilerin sunulan ürün ve hizmetlerden Türkiye'de faydalanmaları durumunda, bu veri sorumlusu tarafından da aynı esaslar çerçevesinde Kurula bildirimde bulunulmasına,

Veri ihlali gerçekleşmesi halinde veri sorumlusu tarafından kendi nezdinde kimlere raporlama yapılacağı, Kanun kapsamında yapılacak bildirimler ile veri ihlalinin olası sonuçlarının değerlendirilmesi hususunda, kendi nezdindeki sorumluluğun kimde olduğunun belirlenmesi gibi konuları içeren bir veri ihlali müdahale planı hazırlanarak belirli aralıklarla bu planın gözden geçirilmesine karar verilmiştir."

Kurulun 18.09.2019 tarihli ve 2019/271 sayılı kararında[235] ise yukarıda alıntıladığımız kararında değinmediği diğer bir önemli husus olan veri sorumluları tarafından ilgili kişilere yapılacak bildirime bulunması gereken aşağıdaki asgari unsurları belirtmiştir:

- "İhlalin ne zaman gerçekleştiği,
- Kişisel veri kategorileri bazında (kişisel veri ile özel nitelikli kişisel veri ayrımı yapılarak) hangi kişisel verilerin ihlalden etkilendiği,
- Kişisel veri ihlalinin olası sonuçları,
- Veri ihlalinin olumsuz etkilerinin azaltılması için alınan veya alınması önerilen tedbirler,
- İlgili kişilerin veri ihlali ile ilgili bilgi almalarını sağlayacak irtibat kişilerinin isim ve iletişim detayları ya da veri sorumlusunun web sayfasının tam adresi, çağrı merkezi vb. iletişim yolları"

Kurul 2019/271 sayılı kararında ayrıca veri sorumlusu tarafından ilgili kişiye yapılacak bildirimin dilinin açık ve sade bir dille yapılması gerektiğinin altını çizmiştir.

3.5. İdari Yaptırım

Kanunun 18. maddesi uyarınca Kanunun 12. maddesinde düzenlenen veri güvenliğine ilişkin yükümlülüklerin yerine getirilmemesi durumunda ilgili veri sorumlularına 15.000 Türk Lirası'ndan 1.000.000 Türk Lirası'na kadar idari para cezası verilecektir.

Kanunun 18. maddesinde belirtilen tüm idari para cezaları her sene o yılın yeniden değerleme oranlarına göre hesaplanarak güncel idari para cezasının miktarı belirlenecektir.

Veri güvenliğine ilişkin yükümlülüklerin yerine getirilmemesi durumunda uygulanacak idari para cezası için 2020 yılında uygulanacak alt sınır 27.040 Türk Lirası iken üst sınırı ise 1.802.641 Türk Lirası'dır.

---

[235] Kurulun 18.09.2019 tarihli ve 2019/271 sayılı kararına şu uzantıdan ulaşabilirsiniz: https://www.kvkk.gov.tr/Icerik/5547/2019-271 Erişim Tarihi: 4 Nisan 2020.

4. KİŞİSEL VERİLERİN SİLİNMESİ, YOK EDİLMESİ VEYA ANONİM HALE GETİRİLMESİ YÜKÜMLÜLÜĞÜ

4.1. Genel Olarak

Kanunun "Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi" başlıklı 7. maddesinde; "*Kanun ve ilgili diğer kanun hükümlerine uygun olarak işlenmiş olmasına rağmen, işlenmesini gerektiren sebeplerin ortadan kalkması hâlinde kişisel veriler resen veya ilgili kişinin talebi üzerine veri sorumlusu tarafından silinir, yok edilir veya anonim hâle getirilir.*" hükmü düzenlenmiştir. Ayrıca maddenin son fıkrasına göre; "kişisel verilerin silinmesine, yok edilmesine veya anonim hâle getirilmesine ilişkin usul ve esasların yönetmelikle düzenleneceği" belirtilmiştir. Bu konudaki "Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi Hakkında Yönetmelik[236]" 28.10.2017 tarihli ve 30224 sayılı Resmî Gazete'de yayımlanmış ve Yönetmelik yürürlük maddesindeki düzenleme uyarınca 01.01.2018 tarihinde yürürlüğe girmiştir. Ayrıca Kişisel Verileri Koruma Kurumu tarafından "Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi Rehberi[237]" Kurumun sitesinde yayınlanmıştır.

Çalışmamızın bu başlığında, konuya ilişkin teknik ve detaylı düzenlemeler içermesi sebebiyle daha çok Yönetmelik ve Rehberdeki düzenlemelere atıflar yaparak açıklamalarda bulunacağız.

---

[236] Bundan sonra "Yönetmelik" olarak anılacaktır. Yönetmeliğin tam metnine şu uzantıdan ulaşabilirsiniz: https://www.mevzuat.gov.tr/Metin.Aspx?MevzuatKod=7.5.24038&MevzuatIliski=0&sourceXmlSearch=Ki%C5%9Fisel%20verilerin%20silin Erişim Tarihi: 5 Nisan 2020.

[237] **Kişisel Verileri Koruma Kurumu**, Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi Rehberi, Ankara 2018, (Çevrimiçi) https://www.kvkk.gov.tr/SharedFolderServer/CMSFiles/bc1cb353-ef85-4e58-bb99-3bba31258508.pdf Erişim Tarihi: 5 Nisan 2020. Bundan sonra "Rehber" olarak anılacaktır.

4.2. Kişisel Veri Saklama ve İmha Politikası

Veri Sorumluları Sicili'ne kayıt yükümlülüğü bulunan veri sorumlularının Yönetmeliğin 5. maddesi uyarınca, kişisel veri işleme envanterine uygun şekilde bir kişisel veri saklama ve imha politikası hazırlamaları gerekmektedir.

Kişisel veri işleme envanteri, Yönetmeliğin "Tanımlar" başlıklı m. 4/1-e hükmü uyarınca; "*Veri sorumlularının iş süreçlerine bağlı olarak gerçekleştirmekte oldukları kişisel verileri işleme faaliyetlerini; kişisel verileri işleme amaçları, veri kategorisi, aktarılan alıcı grubu ve veri konusu kişi grubuyla ilişkilendirerek oluşturdukları ve kişisel verilerin işlendikleri amaçlar için gerekli olan azami süreyi, yabancı ülkelere aktarımı öngörülen kişisel verileri ve veri güvenliğine ilişkin alınan tedbirleri açıklayarak detaylandırdıkları envanter*" olarak tanımlanmıştır.

Yönetmeliğin 6. maddesi uyarınca kişisel veri saklama ve imha politikalarında asgari olarak;

- "*Kişisel veri saklama ve imha politikasının hazırlanma amacına,*
- *Kişisel veri saklama ve imha politikası ile düzenlenen kayıt ortamlarına,*
- *Kişisel veri saklama ve imha politikasında yer verilen hukuki ve teknik terimlerin tanımlarına,*
- *Kişisel verilerin saklanmasını ve imhasını gerektiren hukuki, teknik ya da diğer sebeplere ilişkin açıklamaya,*
- *Kişisel verilerin güvenli bir şekilde saklanması ile hukuka aykırı olarak işlenmesi ve erişilmesinin önlenmesi için alınmış teknik ve idari tedbirlere,*
- *Kişisel verilerin hukuka uygun olarak imha edilmesi için alınmış teknik ve idari tedbirlere,*
- *Kişisel verileri saklama ve imha süreçlerinde yer alanların unvanlarına, birimlerine ve görev tanımlarına,*
- *Saklama ve imha sürelerini gösteren tabloya,*
- *Periyodik imha sürelerine,*

- *Mevcut kişisel veri saklama ve imha politikasında güncelleme yapılmış ise söz konusu değişikliğe"*

ilişkin bilgilerin bulunması gerektiği düzenlenmiştir.

Veri sorumlusunun yalnızca kişisel veri işleme envanteri yapıp, kişisel veri saklama ve imha politikaları oluşturması yeterli olmayıp, bu politikaları uygulamaya geçirmekle yükümlüdür (Yönetmelik m. 5/2).

4.3. Kişisel Verilerin Silinmesi

Kişisel verilerin silinmesi kavramı Yönetmeliğin 8. maddesinde; "*Kişisel verilerin silinmesi, kişisel verilerin ilgili kullanıcılar için hiçbir şekilde erişilemez ve tekrar kullanılamaz hale getirilmesi işlemidir. Veri sorumlusu, silinen kişisel verilerin ilgili kullanıcılar için erişilemez ve tekrar kullanılamaz olması için gerekli her türlü teknik ve idari tedbirleri almakla yükümlüdür.*" şeklinde düzenlenmiştir.

Kişisel verilerin silinmesine ilişkin teknik detaylar ve silme yöntemleri Kurumun yayınladığı Rehberde bulunmaktadır. Rehber uyarınca kişisel verilerin silinmesine ilişkin başvurulabilecek bazı yöntemler aşağıdaki gibidir[238]:

Hizmet Olarak Uygulama Türü Bulut Çözümleri	*"Bulut sisteminde veriler silme komutu verilerek silinmelidir. Anılan işlem gerçekleştirilirken ilgili kullanıcının bulut sistemi üzerinde silinmiş verileri geri getirme yetkisinin olmadığına dikkat edilmelidir."*
Kâğıt Ortamında Yer Alan Kişisel Veriler	*"Kâğıt ortamında bulunan kişisel veriler karartma yöntemi kullanılarak silinmelidir. Karartma işlemi, ilgili evrak üzerindeki kişisel verilerin, mümkün olan durumlarda kesilmesi, mümkün olmayan durumlarda ise geri döndürülemeyecek ve teknolojik çözümlerle okunamayacak şekilde sabit*

[238] Burada sayılan kişisel verileri silinmesine ilişkin yöntemlerin detayları için Rehberin s. 6 ve devamını inceleyebilirsiniz.

	mürekkep kullanılarak ilgili kullanıcılara görünemez hale getirilmesi şeklinde yapılır."
Merkezi Sunucuda Bulunan Ofis Dosyaları	*"Dosyanın işletim sistemindeki silme komutu ile silinmesi veya dosya ya da dosyanın bulunduğu dizin üzerinde ilgili kullanıcının erişim haklarının kaldırılması gerekir. Anılan işlem gerçekleştirilirken ilgili kullanıcının aynı zamanda sistem yöneticisi olmadığına dikkat edilmelidir."*
Taşınabilir Medyada Yer Alan Kişisel Veriler	*"Flash tabanlı saklama ortamlarındaki kişisel veriler, şifreli olarak saklanmalı ve bu ortamlara uygun yazılımlar kullanılarak silinmelidir."*
Veri Tabanları	*"Kişisel verilerin bulunduğu ilgili satırların veri tabanı komutları ile (DELETE vb.) silinmesi gerekir. Anılan işlem gerçekleştirilirken ilgili kullanıcının aynı zamanda veri tabanı yöneticisi olmadığına dikkat edilmelidir."*

Kişisel verilerin silinmesine ilişkin olarak Information Commissioner's Office tarafından "Kişisel Verilerin Silinmesi (*Deleting Personal Data*)" başlıklı bir belge hazırlanmıştır[239]. Bu belge içerisinde ICO, kişisel verilerin silinmesine ilişkin uygulamalarda pratiğe dönük gerçekçi bir yaklaşım besleyeceğini belirtmiş ve teknik bazı sebepler dolayısıyla imha edilemeyen kişisel verilerin kullanımdan çıkarılmasının yeterli olabileceğini belirtmiştir. Kişisel verinin kullanımdan çıkarılma kavramı, verinin bir daha kullanılmamak üzere ve mevcut olanaklarla bulunduğu kullanım alanından çıkarılmasını ifade etmektedir[240]. Zira bazı durumlarda silinmesi gereken kişisel verilerin, bulunduğu ortam veya veri işleme tekniği itibariyle silinmesi ve/veya diğer verilerden ayrıştırılması çok zor veya

[239] **Information Commissioner's Office**, Deleting Personal Data, 20140226, Version: 1.1, (Çevrimiçi) https://ico.org.uk/media/for-organisations/documents/1475/deleting_personal_data.pdf Erişim Tarihi: 5 Nisan 2020.
[240] **Dülger**, s. 473.

imkânsız olabilmekte ya da bu işlemler için veri sorumlusunun makul olmayan ölçüde masraflar yapması gerekebilmektedir. ICO'nun bu yaklaşımından farklı olarak Kurul tarafından kişisel verilerin imhasına ilişkin herhangi bir istisna getirilmemiştir[241].

4.4. Kişisel Verilerin Yok Edilmesi

Kişisel verilerin yok edilmesi kavramı Yönetmeliğin 10. maddesinde; "*Kişisel verilerin yok edilmesi, kişisel verilerin hiç kimse tarafından hiçbir şekilde erişilemez, geri getirilemez ve tekrar kullanılamaz hale getirilmesi işlemidir. Veri sorumlusu, kişisel verilerin yok edilmesiyle ilgili gerekli her türlü teknik ve idari tedbirleri almakla yükümlüdür.*" şeklinde düzenlenmiştir.

Kişisel verilerin yok edilmesine ilişkin teknik detaylar ve yöntemler Kurumun yayınladığı Rehberde bulunmaktadır. Rehber uyarınca yerel sistemlerde bulunan kişisel verilerin yok edilmesine ilişkin başvurulabilecek bazı yöntemler aşağıdaki gibidir[242]:

i. "*De-manyetize Etme: Manyetik medyanın özel bir cihazdan geçirilerek gayet yüksek değerde bir manyetik alana maruz bırakılması ile üzerindeki verilerin okunamaz biçimde bozulması işlemidir.*

ii. *Fiziksel Yok Etme: Optik medya ve manyetik medyanın eritilmesi, yakılması veya toz haline getirilmesi gibi fiziksel olarak yok edilmesi işlemidir. Optik veya manyetik medyayı eritmek, yakmak, toz haline getirmek ya da bir metal öğütücüden geçirmek gibi işlemlerle verilerin erişilmez kılınması sağlanır. Katı hal diskler bakımından üzerine yazma veya de-manyetize etme işlemi başarılı olmazsa, bu medyanın da fiziksel olarak yok edilmesi gerekir.*

iii. *Üzerine Yazma: Manyetik medya ve yeniden yazılabilir optik medya üzerine en az yedi kez 0 ve 1'lerden oluşan rastgele veriler yazarak eski*

---

[241] **a.g.e.**

[242] Burada sayılan kişisel verileri yok edilmesine ilişkin daha farklı yöntemler ve yöntemlerin detayları için Rehberin s. 9 ve devamını inceleyebilirsiniz.

verinin kurtarılmasının önüne geçilmesi işlemidir. Bu işlem özel yazılımlar kullanılarak yapılmaktadır."

Rehberde ayrıca çevresel sistemler, kâğıt ve mikrofiş ortamları, bulut ortamı gibi verilerin bulunduğu sistemlerin türüne göre kişisel verilerin yok edilmesine ilişkin çeşitli yöntemlerden bahsedilmiştir. Örneğin kâğıt ve mikrofiş ortamlarındaki kişisel verilerin, kalıcı ve fiziksel olarak ortam üzerine yazılı olduğundan ana ortamın yok edilmesi gerektiğinden bahsedilmiştir. Buna göre kişisel verilerin kâğıt üzerinde bulunması halinde verinin bulunduğu ortamı, yani kâğıdı, kâğıt imha veya kırpma makinaları ile anlaşılmaz boyutta, mümkünse yatay ve dikey olarak, geri birleştirilemeyecek şekilde küçük parçalara bölmek gerekecektir. Ancak kişisel verilerin bulunduğu kâğıt, tarama yoluyla elektronik ortama aktarılmış ise bulundukları elektronik ortama göre de-manyetize etme, fiziksel yok etme, üzerine yazma gibi yöntemlerin uygun olan biri veya birkaçının kullanılarak yok edilmesi gerekmektedir.

Rehberde düzenlenen çevresel sistemlerde ortam türüne bağlı olarak kullanılabilecek yok etme yöntemleri aşağıda yer almaktadır:

i. "*Ağ cihazları (switch, router vb.): Söz konusu cihazların içindeki saklama ortamları sabittir. Ürünler, çoğu zaman silme komutuna sahiptir ama yok etme özelliği bulunmamaktadır. (a)'da belirtilen uygun yöntemlerin bir ya da birkaçı kullanılmak suretiyle yok edilmesi gerekir.*

ii. *Flash tabanlı ortamlar: Flash tabanlı sabit disklerin ATA (SATA, PATA vb.), SCSI (SCSI Express vb.) arayüzüne sahip olanları, destekleniyorsa <block erase> komutunu kullanmak, desteklenmiyorsa üreticinin önerdiği yok etme yöntemini kullanmak ya da (a)'da belirtilen uygun yöntemlerin bir ya da birkaçı kullanılmak suretiyle yok edilmesi gerekir.*

iii. *Manyetik bant: Verileri esnek bant üzerindeki mikro mıknatıs parçaları yardımı ile saklayan ortamlardır. Çok güçlü manyetik ortamlara maruz bırakıp de-manyetize ederek ya da yakma, eritme gibi fiziksel yok etme yöntemleriyle yok edilmesi gerekir.*

iv. *Manyetik disk gibi üniteler: Verileri esnek (plaka) ya da sabit ortamlar üzerindeki mikro mıknatıs parçaları yardımı ile saklayan ortamlardır. Çok güçlü manyetik ortamlara maruz bırakıp de-manyetize ederek ya da yakma, eritme gibi fiziksel yok etme yöntemleriyle yok edilmesi gerekir.*

v. *Mobil telefonlar (Sim kart ve sabit hafıza alanları): Taşınabilir akıllı telefonlardaki sabit hafıza alanlarında silme komutu bulunmakta, ancak çoğunda yok etme komutu bulunmamaktadır. (a)'da belirtilen uygun yöntemlerin bir ya da birkaçı kullanılmak suretiyle yok edilmesi gerekir.*

vi. *Optik diskler: CD, DVD gibi veri saklama ortamlarıdır. Yakma, küçük parçalara ayırma, eritme gibi fiziksel yok etme yöntemleriyle yok edilmesi gerekir.*

vii. *Veri kayıt ortamı çıkartılabilir olan yazıcı, parmak izli kapı geçiş sistemi gibi çevre birimleri: Tüm veri kayıt ortamlarının söküldüğü doğrulanarak özelliğine göre (a)'da belirtilen uygun yöntemlerin bir ya da birkaçı kullanılmak suretiyle yok edilmesi gerekir.*

viii. *Veri kayıt ortamı sabit olan yazıcı, parmak izli kapı geçiş sistemi gibi çevre birimleri: Söz konusu sistemlerin çoğunda silme komutu bulunmakta, ancak yok etme komutu bulunmamaktadır. (a)'da belirtilen uygun yöntemlerin bir ya da birkaçı kullanılmak suretiyle yok edilmesi gerekir.*"

Rehber uyarınca; "bulut depolama ortamlarında yer alan kişisel verilerin depolanması ve kullanımı esnasında, kriptografik yöntemlerle şifrelenmesi ve kişisel veriler için mümkün olan yerlerde, özellikle hizmet alınan her bir bulut çözümü için ayrı ayrı şifreleme anahtarları kullanılması gerektiği belirtilmiştir. Bulut bilişim hizmet ilişkisi sona erdiğinde ise; kişisel verileri kullanılır hale gelebilmesi için gerekli olan şifreleme anahtarlarının tüm kopyalarının yok edilmesi" gerektiği belirtilmiştir. Ancak söz konusu şifreleme anahtarlarının yok edilmesi, kişisel verilere erişimin önüne geçmekte olup kişisel verileri yok edilmesine sebep olup olmayacağı tartışılabilir. Bu husus çalışma konumuzun

dışında olup daha çok bilgi teknolojilerini ilgilendirdiği için burada yalnızca tereddüdümüzün belirtilmesiyle yetinilecektir.

Rehberde ayrıca ek olarak; arızalanan ya da bakıma gönderilen cihazlarda yer alan kişisel verilerin ne şekilde yok edilmesi gerektiğine ilişkin aşağıdaki yöntemleri belirtmiştir[243]. Buna göre;

i. "İlgili cihazların bakım, onarım işlemi için üretici, satıcı, servis gibi üçüncü kurumlara aktarılmadan önce içinde yer alan kişisel verilerin de-manyetize etme, fiziksel yok etme, üzerine yazma gibi uygun yöntemlerin bir ya da birkaçı kullanılmak suretiyle yok edilmesi,

ii. Yok etmenin mümkün ya da uygun olmadığı durumlarda, veri saklama ortamının sökülerek muhafaza edilmesi, arızalı diğer parçaların üretici, satıcı, servis gibi üçüncü kurumlara gönderilmesi,

iii. Dışarıdan bakım, onarım gibi amaçlarla gelen personelin, kişisel verileri kopyalayarak kurum dışına çıkartmasının engellenmesi için gerekli önlemlerin alınması gerekmektedir."

4.5. Kişisel Verilerin Anonim Hale Getirilmesi

Kişisel verilerin anonim hale getirilmesi kavramı Yönetmeliğin 10. maddesinde; "*Kişisel verilerin anonim hale getirilmesi, kişisel verilerin başka verilerle eşleştirilse dahi hiçbir surette kimliği belirli veya belirlenebilir bir gerçek kişiyle ilişkilendirilemeyecek hale getirilmesidir. Kişisel verilerin anonim hale getirilmiş olması için; kişisel verilerin, veri sorumlusu, alıcı veya alıcı grupları tarafından geri döndürme ve verilerin başka verilerle eşleştirilmesi gibi kayıt ortamı ve ilgili faaliyet alanı açısından uygun tekniklerin kullanılması yoluyla dahi kimliği belirli veya belirlenebilir bir gerçek kişiyle ilişkilendirilemez hale getirilmesi gerekir. Veri sorumlusu, kişisel verilerin anonim hale getirilmesiyle ilgili gerekli her türlü teknik ve idari tedbirleri almakla yükümlüdür.*" şeklinde düzenlenmiştir.

[243] Rehber, s. 13.

Rehber uyarınca kişisel verilerin anonim hale getirilmesine ilişkin başvurulabilecek bazı yöntemler aşağıdaki gibidir[244]:

Değer Düzensizliği Sağlamayan Anonim Hale Getirme Yöntemleri	*"Değişkenleri Çıkartma*
	Kayıtları Çıkartma
	Bölgesel Gizleme
	Genelleştirme
	Alt ve Üst Sınır Kodlama
	Global Kodlama
	Örnekleme
Değer Düzensizliği Sağlayan Anonim Hale Getirme Yöntemleri	*Mikro Birleştirme*
	Veri Değiş Tokuşu
	Gürültü Ekleme
Anonim Hale Getirmeyi Kuvvetlendirici İstatistiksel Yöntemler	*K-Anonimlik*
	L-Çeşitlilik
	T-Yakınlık"

Kişisel verilerin anonim hale getirilmesine ilişkin olarak Working Party'nin 10 Nisan 2014 tarihli ve 05/2014 sayılı "Anonim Hale Getirme Teknikleri (*Anonymisation Techniques*)" başlıklı bir çalışması bulunmaktadır[245]. Çalışmanın temel amacı anonim hale getirme tekniklerinin sınırlarını ve geçerliliklerini incelemektir[246]. Working Party bu çalışma içerisinde anonim hale getirme tekniklerinin uygulanması sonucu ortaya çıkacak olası riskleri aynı zamanda bu

[244] Burada sayılan kişisel verileri anonim hale getirme yöntemlerinin detayları için Rehberin s. 16 ve devamını inceleyebilirsiniz.

[245] **Article 29 Data Protection Working Party**, Opinion 05/2014 on Anonymisation Techniques, 10 Nisan 2014, 0829/14/EN, WP216, (Çevrimiçi) https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp216_en.pdf Erişim Tarihi: 7 Nisan 2020.

[246] Working Party'nin 05/2014 sayılı Anonim Hale Getirme Teknikleri hakkında detaylı bir değerlendirme ve eleştiriler için bkz. **Khaled El Emam, Cecilia Alvarez**, "A Critical Appraisal of the Article 29 Working Party Opinion 05/2014 on Data Anonymization Techniques", International Data Privacy Law, Cilt 5, Sayı 1, s. 73–87, 2015, (Çevrimiçi) https://academic.oup.com/idpl/article-abstract/5/1/73/2863828 Erişim Tarihi: 7 Nisan 2020.

tekniklerin sağlamlığının test edilmesi için kriter olarak almıştır[247]. Bu üç kriter aşağıdaki gibidir:

i. Seçilme (*singling out*) - Herhangi bir bireyin diğerlerinin arasından seçilmesi mümkün mü?

ii. Eşleşme (*linkability*) - Kayıtların herhangi bir bireyle eşleşmesi mümkün mü?

iii. Çıkarım (*inference*) - Herhangi bir bilginin herhangi bir bireyle ilgili olduğu çıkarımı yapılabilir mi?

Working Party'nin bu çalışmasındaki bir diğer önemli husus ise psödonimizasyon (*pseudonymisation*) kavramını tanıtması ve uygulamada en çok görülen psödonimizasyon tekniklerini açıklamasıdır[248]. Bu kavramdan daha sonra GDPR içerisinde de bahsedilmiştir. GDPR'ın m. 4/1-5 hükmü uyarınca psödonimizasyon; bir kişisel verinin, herhangi bir ilave veri kullanılmaksızın bir kişisel veri sahibi (ilgili kişi) ile ilişkilendirilemeyecek şekilde işlenmesini ifade etmektedir[249]. Diğer bir ifadeyle psödonimizasyon tekniği, ilgili kişinin kimliğini belirli ya da belirlenebilir kılan verilerin değiştirilmesi veya gizlenmesi olarak tanımlanabilir. Örneğin, kişinin adının, soyadının, kimlik numarasının ve doğum tarihinin diğer verilerinden ayrı bir ortamda şifre altında saklanması çok yaygın kullanılan bir psödonimizasyon tekniğidir. Ancak bu teknikte veriler geri dönüşü olmayacak şekilde yok edilmediği veya tek yönlü bir şifrelemeye tabi tutulmadığı ve gizlenen veya yerleri değiştirilen doğru veri setlerine ulaşılması olasılığı var olduğu için psödonim verilerin ilgili kişinin kimliğinin belirlenebilir kılınmasına

---

[247] **Article 29 Data Protection Working Party**, Opinion 05/2014 on Anonymisation Techniques, s. 11-12.

[248] **Elizabeth A. Brasher**, "Addressing the Failure of Anonymization: Guidance from the European Union's General Data Protection Regulation", Columbia University Business Law Review, Cilt 2018, s. 209-253, 2018, (Çevrimiçi) https://academiccommons.columbia.edu/doi/10.7916/d8-zgve-y962 Erişim Tarihi: 7 Nisan 2020, s. 246. Ayrıca bkz: Psödonimizasyon kavramına ilişkin olarak açıklamalar içeren diğer bir Working Party çalışması için bkz. **Article 29 Data Protection Working Party**, Opinion 4/2007 on the Concept of Personal Data, s. 18 vd.

[249] **Hüseyin Murat Develioğlu**, 6698 sayılı Kişisel Verilerin Korunması Kanunu ile Karşılaştırmalı Olarak Avrupa Birliği Genel Veri Koruma Tüzüğü Uyarınca Kişisel Verilerin Korunması Hukuku, On İki Levha Yayıncılık, İstanbul 2017, s. 36; **Han**, "Kişisel Verilerin İşlenmesi Bağlamında Hukuka Uygunluk Sebebi Olarak Veri Sahibinin Rızası", s. 426.

imkân veren veriler olarak kabul edilmektedir[250]. Bu tespit çok önem arz etmektedir. Zira, ortada bir gerçek kişiyi belirli veya belirlenebilir kılan bir veri yoksa kişisel verinin de olmadığı kabul edilecek ve bu sebeple ilgili kişi koruma mekanizmalarından yararlanamayacaktır. Ancak Working Party'nin burada bahsedilen açıklamaları uyarınca psödonim verilerin, kişiyi *dolaylı şekilde belirlenebilir kılan*[251] veriler olarak kabul edilmesi sebebiyle kişisel verilerin korunması hukuku kapsamında korunması gerekmektedir[252].

Working Party, psödonimizasyon tekniğinin bir anonim hale getirme tekniği olmadığını, yalnızca kişisel veri sahibinin kimliği ile veri setleri arasındaki bağlantıyı azaltması sebebiyle kullanışlı bir güvenlik tedbiri olduğunu vurgulamaktadır[253].

Information Commissioner's Office tarafından da kişisel verilerin anonim hale getirilmesine ilişkin kapsamlı bir belge yayınlanmıştır[254]. Bu belge, konuya ilişkin tanımlamalar, açıklamaları, uygulamaya yönelik çeşitli anonim hale getirme teknikler ve özellikle bol miktarda açıklamalı örnekler içermesi sebebiyle konunun teknik kısımlarını daha anlaşılır kılmıştır. Bu çalışmada kullanılan teknikler ve anlatımlar Kurumun hazırladığı Rehber ile benzerlikler göstermektedir.

---

[250] **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, Cilt 34, Sayı 2, s. 284-322, 2017, (Çevrimiçi) https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2927945 Erişim Tarihi: 7 Nisan 2020, s. 296-297; **Article 29 Data Protection Working Party**, Opinion 4/2007 on the Concept of Personal Data, s. 18.

[251] **Jules Polonetsky, Omer Tene, Kelsey Finch**, "Shades of Gray: Seeing The Full Spectrum of Practical Data De-Identification", Santa Clara Law Review, Cilt 56, Sayı 3, s. 593-629, 2016, (Çevrimiçi) https://digitalcommons.law.scu.edu/cgi/viewcontent.cgi?article=2827&context=lawreview , Erişim Tarihi: 8 Nisan 2020, s. 605-606-608.

[252] **Han**, "Kişisel Verilerin İşlenmesi Bağlamında Hukuka Uygunluk Sebebi Olarak Veri Sahibinin Rızası", s. 426.

[253] **Brasher**, s. 246-247; **Article 29 Data Protection Working Party**, Opinion 05/2014 on Anonymisation Techniques, s. 20.

[254] **Information Commissioner's Office**, Anonymisation: Managing Data Protection Risk Code of Practice, İngiltere 2012, (Çevrimiçi) https://ico.org.uk/media/for-organisations/documents/1061/anonymisation-code.pdf Erişim Tarihi: 7 Nisan 2020.

4.6. Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesinde Süreler

4.6.1. Kişisel Verileri Resen Silme, Yok Etme veya Anonim Hale Getirme Süreleri

Yönetmeliğin "Kişisel verileri resen silme, yok etme veya anonim hale getirme süreleri" başlıklı 11. maddesinde; "*Kişisel veri saklama ve imha politikası hazırlamış olan veri sorumlusu, kişisel verileri silme, yok etme veya anonim hale getirme yükümlülüğünün ortaya çıktığı tarihi takip eden ilk periyodik imha işleminde, kişisel verileri siler, yok eder veya anonim hale getirir."* denilmiştir.

Hükmün devamında, "*Periyodik imhanın gerçekleştirileceği zaman aralığı, veri sorumlusu tarafından kişisel veri saklama ve imha politikasında belirlenir. Bu süre her halde altı ayı geçemez. Kişisel veri saklama ve imha politikası hazırlama yükümlülüğü olmayan veri sorumlusu, kişisel verileri silme, yok etme veya anonim hale getirme yükümlülüğünün ortaya çıktığı tarihi takip eden üç ay içinde, kişisel verileri siler, yok eder veya anonim hale getirir. Kurul, telafisi güç veya imkânsız zararların doğması ve açıkça hukuka aykırılık olması halinde, bu maddede belirlenen süreleri kısaltabilir.*" hususları düzenlenmiştir.

Madde kapsamında kişisel verileri re'sen silme, yok etme veya anonim hale getirme sürelerine ilişkin detaylı bir düzenleme yapılmıştır. Bu madde kapsamında veri sorumlularının uymaları gereken çeşitli yükümlülükler düzenlenmiştir.

4.6.2. Kişisel Verileri İlgili Kişinin Talep Etmesi Durumunda Silme ve Yok Etme Süreleri

Yönetmeliğin "Kişisel verileri ilgili kişinin talep etmesi durumunda silme ve yok etme süreleri" başlıklı 11. maddesinde; "*İlgili kişi, Kanunun (Değişik ibare: RG-28/4/2019-30758) 11. ve 13. maddelerine istinaden veri sorumlusuna başvurarak kendisine ait kişisel verilerin silinmesini veya yok edilmesini talep ettiğinde;*

a) Kişisel verileri işleme şartlarının tamamı ortadan kalkmışsa; veri sorumlusu talebe konu kişisel verileri siler, yok eder veya anonim hale getirir. Veri

sorumlusu, ilgili kişinin talebini en geç otuz gün içinde sonuçlandırır ve ilgili kişiye bilgi verir.

b) Kişisel verileri işleme şartlarının tamamı ortadan kalkmış ve talebe konu olan kişisel veriler üçüncü kişilere aktarılmışsa veri sorumlusu bu durumu üçüncü kişiye bildirir; üçüncü kişi nezdinde bu Yönetmelik kapsamında gerekli işlemlerin yapılmasını temin eder.

c) Kişisel verileri işleme şartlarının tamamı ortadan kalkmamışsa, bu talep veri sorumlusunca Kanunun 13. maddesinin üçüncü fıkrası uyarınca gerekçesi açıklanarak reddedilebilir ve ret cevabı ilgili kişiye en geç otuz gün içinde yazılı olarak ya da elektronik ortamda bildirilir." hükmü düzenlenmiştir.

Madde kapsamında bu kez veri sorumlusu tarafından kendiliğinden silme, yok etme veya anonim hale getirme konusu yerine veri sahibi ilgili kişi tarafından veri sorumlusundan kişisel verilerin silinmesinin veya yok edilmesinin talep edilmesi durumunda uygulanacak süreç düzenlenmiştir.

4.7. Yaptırım

Kanunun "Suçlar" başlıklı 17. maddesi uyarınca; "kişisel verilere ilişkin suçlar bakımından 26.09.2004 tarihli ve 5237 sayılı Türk Ceza Kanunu'nun (TCK) 135 ila 140. maddelerinin uygulanacağı" ve 6098 sayılı Kanunun 7. maddesi hükmüne aykırı olarak; kişisel verileri silmeyen veya anonim hâle getirmeyenlerin 5237 sayılı Kanunun "Verileri yok etmeme" başlıklı 138. maddesine göre cezalandırılacağı düzenlenmiştir. Bahsi geçen madde aşağıdaki gibidir:

> "*(1) Kanunların belirlediği sürelerin geçmiş olmasına karşın verileri sistem içinde yok etmekle yükümlü olanlara görevlerini yerine getirmediklerinde bir yıldan iki yıla kadar hapis cezası verilir.*
>
> *(2) (Ek: 21/2/2014-6526/5 md.) Suçun konusunun Ceza Muhakemesi Kanunu hükümlerine göre ortadan kaldırılması veya yok edilmesi gereken veri olması hâlinde verilecek ceza bir kat artırılır.*"

TCK'nın 139. maddesi uyarınca verileri yok etmeme suçunun soruşturulması ve kovuşturulması şikâyete bağlı değildir. Dolayısıyla savcılık şikâyet üzerine veya

kendiliğinden soruşturma başlatabilecektir ve şikâyetin geri çekilmesi durumu soruşturma veya kovuşturmanın devamını etkilemeyecektir.

Son olarak TCK'nın 140. maddesi uyarınca verileri yok etmeme suçunun işlenmesi dolayısıyla tüzel kişiler hakkında bunlara özgü güvenlik tedbirlerinin uygulanacağı düzenlenmiştir.

5. VERİ SORUMLULARI SİCİLİNE KAYIT OLMA YÜKÜMLÜLÜĞÜ

5.1. Genel Olarak

Kanunun "Veri Sorumluları Sicili" başlıklı 16. maddesi uyarınca veri sorumlularının belirli şartlar altında Kişisel Verileri Koruma Kurumu Başkanlığı tarafından kamuya açık olarak tutulan Veri Sorumluları Sicili'ne[255] kayıt olma yükümlülüğü bulunmaktadır.

Sicile kayıt yükümlülüğüyle ilgili çeşitli kurallar, istisnalar ve diğer ayrıntılar Kurulun kararlarıyla ve Kurum tarafından 30.12.2017 tarihli ve 30286 sayılı Resmî Gazete'de yayımlanarak 01.01.2018 tarihinde yürürlüğe giren Veri Sorumluları Sicili Hakkında Yönetmelik[256] ile düzenlenmiştir. Bu sebeple veri sorumlusunun Sicile kayıt olma yükümlülüğü kapsamında bu bölümde yapılacak açıklamalar Kanuna ek olarak Kurul kararları ve Yönetmelik hükümleri çerçevesinde yapılacaktır.

5.2. Sicilin Oluşturulması, İdaresi, Gözetimi ve Sicile Erişim

Yönetmeliğin 5. maddesi uyarınca Sicilin oluşturulması, idaresi ve gözetimi ile ilgili olarak aşağıdaki ilke, usul ve esaslara uyulması gerektiği düzenlenmiş olup bu kapsamda;

---

[255] Bundan sonra "Sicil" olarak anılacaktır.

[256] Kurum tarafından 30.12.2017 tarihli ve 30286 sayılı Resmî Gazete'de yayımlanan Veri Sorumluları Sicili Hakkında Yönetmelik'e şu uzantıdan ulaşabilirsiniz: https://www.resmigazete.gov.tr/eskiler/2017/12/20171230-7.htm Erişim Tarihi: 6 Nisan 2020. Bundan sonra bu başlık altında "Yönetmelik" olarak anılacaktır.

i. "Veri sorumlularının, kişisel veri işleme faaliyetine başlamadan önce Sicile kaydolmak zorunda olduğu,

ii. Türkiye'de yerleşik olmayan veri sorumlularının, veri işleme faaliyetine başlamadan önce veri sorumlusu temsilcisi marifetiyle Sicile kaydolmak zorunda olduğu,

iii. Sicilin kamuya açık biçimde tutulduğu ve Kurulun kamuya açıklık ilkesinin sağlanması şartıyla, bu ilkenin kapsamını ve istisnalarını belirlemeye yetkili olduğu,

iv. Sicil başvurularında Sicile beyan edilecek açıklamaların kişisel veri işleme envanterine dayalı olarak hazırlanması gerektiği,

v. Veri sorumluları için belirtilen aydınlatma yükümlülüğünde, ilgili kişinin başvurularının yanıtlanmasında ve ilgili kişi tarafından verilecek açık rızanın kapsamının belirlenmesinde kişisel veri işleme envanterine göre Sicile sunulan ve Sicilde yayınlanan bilgilerin esas alınması gerektiği" hususlarına değinilmiştir.

vi. Yönetmelikte ayrıca; "Veri sorumlularının, Sicile sunulan ve Sicilde yayınlanan bilgilerin eksiksiz, doğru, güncel ve hukuka uygun olmasından sorumlu olduğu ve veri sorumlularının Sicile kaydolmasının Kanun kapsamındaki diğer yükümlülüklerini ortadan kaldırmayacağı,

vii. Yönetmeliğin 16. maddesinde belirtilen objektif kriterlere dayalı olarak belirli şartları taşıyan veri sorumlularının Kurul tarafından Sicile kayıt yükümlülüğünden muaf tutulmasının, bu veri sorumlularının Kanun kapsamındaki yükümlülüklerini ortadan kaldırmayacağı,

viii. Sicile ilişkin işlemlerin, veri sorumluları tarafından VERBİS üzerinden gerçekleştirileceği" belirtildikten sonra son olarak,

ix. "Veri sorumluları tarafından Sicile sunulan ve Sicilde yayınlanan kişisel verilerin işlendikleri amaç için gerekli olan azami sürenin; Kanunun 7. maddesinde öngörülen veri sorumlularının kişisel verileri

silme, yok etme veya anonim hale getirme yükümlülüklerinin yerine getirilmesinde esas alınacağı"

düzenlenmiştir.

5.3. Sicile Kayıt Yükümlülüğü

5.3.1. Kayıt Yükümlülüğünün Başlangıcı

Yönetmeliğin "Kayıt yükümlülüğünün başlangıcı" başlıklı 8. maddesi uyarınca; "veri sorumlularının, kişisel veri işleme faaliyetine başlamadan önce Sicile kayıt yükümlülüklerini yerine getirmek zorunda oldukları" düzenlenmiştir. Ancak başta kayıt yükümlülüğü altında olmayan ve sonradan Sicile kayıt yükümlüsü haline gelen veri sorumlularının, yükümlülük altına girmelerini takip eden otuz gün içerisinde Sicile kaydolmaları gerekmektedir (Yönetmelik, m. 8/2).

Yönetmeliğin 8. maddesinin üçüncü fıkrasında kayıt yükümlülüğü altında bulunan veri sorumlularına Kurum tarafından bir ek süre verilebileceği düzenlenmiştir. Buna göre veri sorumluları; "herhangi bir fiili, teknik ya da hukuki imkânsızlık nedeniyle Sicile kayıt yükümlülüğünün yerine getirilememesi halinde, bu imkânsızlığın ortaya çıkmasından itibaren en geç yedi iş günü içerisinde Kuruma yazılı olarak başvurup gerekçesini belirterek kayıt yükümlülüklerini yerine getirmek için Kurumdan ek süre talep edebilirler. Bu durumda Kurum tarafından başvuru incelenerek, bir defaya mahsus olmak ve her halde otuz günü geçmemek üzere veri sorumlusuna ek süre verebilir."

5.3.2. Kayıt Yükümlülüğü Kapsamında İletilecek Bilgiler

Yönetmeliğin "Kayıt yükümlülüğü kapsamında iletilecek bilgiler" başlıklı 9. maddesinde veri sorumlusu tarafından yapılacak Sicile kayıt başvurusunda hangi bilgilerin bulunması gerektiği düzenlenmiştir. Buna göre Sicile yapılacak başvuruda aşağıdaki bilgilerin bulunması gereklidir:

i. "Veri sorumlusu, varsa veri sorumlusu temsilcisi ve irtibat kişisine ait kimlik ve adres bilgilerine ilişkin Kurul tarafından belirlenecek başvuru formunda yer alan bilgiler,

ii. Kişisel verilerin hangi amaçla işleneceği,

iii. Veri konusu kişi grubu ve grupları ile bu kişilere ait veri kategorileri hakkındaki açıklamalar,

iv. Kişisel verilerin aktarılabileceği alıcı veya alıcı grupları,

v. Yabancı ülkelere aktarımı öngörülen kişisel veriler,

vi. Kanunun 12. maddesinde öngörülen ve Kurul tarafından belirlenen kriterlere göre alınan tedbirler,

vii. Kişisel verilerin mevzuatta öngörülen veya işlendikleri amaç için gerekli olan azami muhafaza edilme süresi."

Bu düzenleme, Sicile kayıt başvurusunda bulunması gereken bilgilerin sayıldığı Kanunun 16. maddesinin üçüncü fıkrasındaki düzenlemeyle birkaç küçük farklılık dışında oldukça benzerdir.

Kayıt yükümlülüğü kapsamında iletilecek bilgilerin düzenlendiği Yönetmeliğin 9. maddesinin dördüncü fıkrasında "Sicile açıklanacak kişisel verilerin mevzuatta belirtilen ya da işlendikleri amaç için gerekli olan azami muhafaza edilme süresine ilişkin bilgilerin de kişisel veri kategorileri ile eşleştirilerek Sicile bildirilmesi gerektiği" düzenlenmiştir. Buna göre kişisel verilerin işlendikleri amaç için gerekli olan azami muhafaza edilme süresi belirlenirken aşağıdaki hususlara dikkat edilmesi gerekmektedir;

i. "İlgili veri kategorisinin işlenme amacı kapsamında veri sorumlusunun faaliyet gösterdiği sektörde genel teamül gereği kabul edilen süre

ii. İlgili veri kategorisinde yer alan kişisel verinin işlenmesini gerekli kılan ve ilgili kişiyle tesis edilen hukuki ilişkinin devam edeceği süre

iii. İlgili veri kategorisinin işlenme amacına bağlı olarak veri sorumlusunun elde edeceği meşru menfaatin hukuka ve dürüstlük kurallarına uygun olarak geçerli olacağı süre

iv. İlgili veri kategorisinin işlenme amacına bağlı olarak saklanmasının yaratacağı risk, maliyet ve sorumlulukların hukuken devam edeceği süre

v. Belirlenecek azami sürenin ilgili veri kategorisinin doğru ve gerektiğinde güncel tutulmasına elverişli olup olmadığı

vi. Veri sorumlusunun hukuki yükümlülüğü gereği ilgili veri kategorisinde yer alan kişisel verileri saklamak zorunda olduğu süre

vii. Veri sorumlusu tarafından, ilgili veri kategorisinde yer alan kişisel veriye bağlı bir hakkın ileri sürülmesi için belirlenen zamanaşımı süresi"

Veri sorumlularına yol gösterici olacak bu düzenlemeyle çeşitli verilerin muhafaza sürelerine ilişkin kanunlarda genellikle bilgi bulunmamasının neden olduğu belirsizliği ortadan kaldırmaya yardımcı olacak kriterler belirlenmiştir. Ek olarak Yönetmeliğin m. 9/5 hükmü uyarınca veri sorumlularının, kişisel verilerin azami muhafaza edilme sürelerinin kişisel veri işleme envanterinde yazılı bilgilerle uyumlu olup olmadığını ve azami sürenin aşılıp aşılmadığını takip edebilmeleri için kişisel verileri saklama ile imha politikası hazırlamaları ve bu politikaların uygulanmasını temin etmeleri gerekmektedir. Bu hüküm uyarınca Sicile kayıt yükümlülüğü bulunan veri sorumlularının kişisel veri saklama ile imha politikaları hazırlamak yükümlülüğü olduğu anlaşılmaktadır.

5.3.3. Kayıt Başvurusu

Yönetmeliğin 10. maddesi uyarınca; Yönetmeliğin 9. maddesinde sayılan ve bir önceki başlık altında listelediğimiz Sicile yapılacak başvuruda bulunması gereken bilgilerin Veri Sorumluları Sicil Bilgi Sistemi'ne diğer adıyla VERBİS'e yüklenmesi ile birlikte veri sorumlularının Sicile kayıt yükümlülüğünü yerine getirmiş sayılacağı düzenlenmiştir.

5.3.4. Veri Sorumlusu, Veri Sorumlusu Temsilcisi ve İrtibat Kişisinin Yükümlülükleri

Sicile kayıt yükümlülüğünün kim tarafından, nasıl yerine getirileceği ve bu yükümlülük kapsamındaki hukuki sorumluluğun kimin üzerinde olduğuna ilişkin olarak Yönetmeliğin 11. maddesinde birtakım önemli düzenlemeler yapılmıştır. Yönetmeliğin m. 11/1 hükmü uyarınca; "*Tüzel kişilerde veri sorumlusu tüzel kişiliğin kendisidir. Türkiye'de yerleşik olan tüzel kişilerin Kanun kapsamındaki veri sorumlusu yükümlülükleri, ilgili mevzuat hükümlerine göre tüzel kişiliği temsil*

ve ilzama yetkili organ veya ilgili mevzuatta belirtilen kişi veya kişiler marifetiyle yerine getirilir." denilerek bu soruların önemli bir kısmına cevap getirilmiştir. Bu düzenlemeler ışığında örneğin bir anonim şirket için şirketi temsil ve ilzama yetkili organ olan Yönetim Kurulu yükümlülük altında olacakken, limited şirketler için ise müdür veya müdürler kurulu yükümlülük altında olacaktır.

Aynı fıkranın devamında tüzel kişiliği temsile yetkili organın, Kanunun kapsamındaki yükümlülüklerini yerine getirirken bir veya birden fazla kişiyi görevlendirebileceği, ancak bu durumda dahi Kanundan kaynaklanan sorumluluklarının ortadan kalkmadığı düzenlenmiştir. Yani örneğin bir anonim şirketin Yönetim Kurulu aldığı bir Yönetim Kurulu kararı ile Kanundan kaynaklı yükümlülüklerin yerine getirilmesi için belirli çalışanları yetkilendirebilecektir, ancak bu yetkilendirmeye rağmen Kanundan kaynaklı sorumluluk, yetkilendirilen kişilerde değil bu örnek kapsamında anonim şirketin Yönetim Kurulunda kendini gösterecektir.

5.3.4.1. Türkiye'de Yerleşik Olmayan Veri Sorumluları Açısından Veri Sorumlusu Temsilcisi Belirleme Yükümlülüğü

Veri sorumlusunun Türkiye'de yerleşik olmaması (merkezinin Türkiye dışında olması) durumunda, veri sorumlusu tarafından bir veri sorumlusu temsilcisi atanması gerekmektedir. Veri sorumlusu temsilcisi, veri sorumlusunun yetkili organı tarafından alınacak bir atama kararıyla belirlenecektir. Bu atama kararının tasdikli bir örneği, Sicile yapılacak kayıt başvurusu esnasında veri sorumlusu temsilcisi tarafından Kuruma ibraz edilecektir. Yönetmeliğin 11. maddesinin üçüncü fıkrası uyarınca veri sorumlusunun yetkili organı tarafından alınan atama kararında, veri sorumlusu temsilcisine asgari olarak aşağıda sayılı olan yetkilerin verilmesi gerekmektedir:

i. "Kurum tarafından yapılan tebligat veya yazışmaları veri sorumlusu adına tebellüğ veya kabul etme,

ii. Kurum tarafından veri sorumlusuna yöneltilen talepleri veri sorumlusuna iletme, veri sorumlusundan gelecek cevabı Kuruma iletme,

iii. Kurul tarafından başkaca bir esasın belirlenmemiş olması halinde; ilgili kişilerin Kanunun 13. maddesinin birinci fıkrası uyarınca veri sorumlusuna yönelteceği başvuruları veri sorumlusu adına alma ve veri sorumlusuna iletme,

iv. Kurul tarafından başkaca bir esasın belirlenmemiş olması halinde; ilgili kişilere Kanunun 13. maddesinin üçüncü fıkrası uyarınca veri sorumlusunun cevabını iletme,

v. Veri sorumlusu adına Sicile ilişkin iş ve işlemleri yapma."

Bu yetkilerin veri sorumlusu temsilcisine verilme amacının Kurum ile veri sorumlusu arasındaki iletişimin sağlıklı şekilde, kesintisiz bir biçimde sürdürülmesi ve Kanunun uygulanmasının temin edilmesi olduğu söylenebilir.

5.3.4.2. Türkiye'de Yerleşik Tüzel Kişi Veri Sorumlularının İrtibat Kişisi Atama Yükümlülüğü

Türkiye'de yerleşik tüzel kişi sıfatını haiz veri sorumluları, Sicile kayıt esnasında Sicile işlemek üzere bir irtibat kişisi belirlemek zorundadır. Veri sorumlusu tarafından belirlenen bu irtibat kişisinin bilgileri Sicile işlenir. Burada önem arz eden husus, irtibat kişisinin Kanun ve Yönetmelik hükümlerine göre veri sorumlusunu temsile yetkili olmadığıdır (Yönetmelik, m. 11/4). İrtibat kişisinin temel görevi, ilgili kişilerin veri sorumlusuna ileteceği taleplerin cevaplandırılması konusunda iletişim sağlamasıdır. Bu düzenlemeyle irtibat kişisinin aynı zamanda veri sorumlusu olmadığı, Kanundan kaynaklı yükümlülüklerin veri sorumlusu üzerinde olduğu, irtibat kişisinin Kanun ve Yönetmelik hükümlerine göre veri sorumlusunu temsile etmediğinin altı çizilmiştir.

Yönetmeliğin 11. maddesinin beşinci uyarınca; "*Kamu kurum ve kuruluşlarında irtibat kişisi, üst düzey yönetici tarafından Kurum ile iletişimi sağlamak amacıyla belirlenerek Sicile kaydı yapılan daire başkanı veya üstü yöneticidir.*" şeklinde bir düzenleme yapılarak irtibat kişisi olarak atanabilecek kişilerin pozisyonları daha sınırlı şekilde belirlenmiştir.

5.3.5. Kurum ile İletişimin Sağlanması, Kayıt Bilgilerinde Değişiklikler ve Sicil Kaydının Silinmesi

Yönetmeliğin "İletişimin sağlanması" başlıklı 12. maddesi uyarınca; "Kanunun uygulanmasıyla ilgili olarak Kurum tarafından veri sorumlusuyla kurulacak iletişimin hangi kanallar aracılığıyla yapılacağı düzenlenmiştir. Buna göre Kurum; Türkiye'de yerleşik gerçek veya tüzel kişiler için, Sicile bildirilen kimlik, adres veya KEP adresi bilgileri üzerinden ilgili gerçek veya tüzel kişi vasıtasıyla" iletişime geçileceği düzenlenmiştir. Türkiye'de yerleşik olmayan veri sorumluları ile Kurumun kuracağı iletişim, veri sorumlusunun Sicile bildirdiği temsilcisi üzerinden sağlanacaktır.

Yönetmeliğin "Kayıt bilgilerinde değişiklikler" başlıklı 13. maddesi uyarınca; Sicile kaydedilen bilgilerde herhangi bir değişiklik olması durumunda oluşan bu değişikliklerin, VERBİS portalı üzerinden yedi gün içinde Kuruma bildirilmesi gerekmektedir.

Yönetmeliğin "Sicil kaydının silinmesi" başlıklı 14. maddesi uyarınca; Sicil kaydının silinmesinin gerekmesi durumunda veri sorumlusunun bu konuyla ilgili olarak VERBİS üzerinden Kuruma başvurması gerekmektedir. Bu kapsamda veri sorumlusu bünyesinde Sicile kayıt yükümlüğünü gerektiren faaliyetlerin sona ermesi ya da ortadan kalkması durumunda, veri sorumlusunun Sicildeki kaydı silinecektir (Yönetmelik, m. 14/2). Sicildeki bulunan bu kayıtlara, istenildiğinde erişilebilir olmakla birlikte kayıtların üzerinde herhangi bir değişiklik yapılamayacak şekilde tutulacaktır. Son olarak Yönetmeliğin m. 14. maddesinin üçüncü fıkrası uyarınca Sicil kaydının silinmesi halinin, veri sorumlusunun Sicile kayıtlı olduğu dönemdeki yükümlülüklerini ortadan kaldırmayacaktır.

5.4. Sicile Kayıt Yükümlülüğünün Kapsamı ve İstisnaları

5.4.1. Yönetmelikle Belirlenen İstisnalar

Yönetmeliğin "İstisna uygulanacak haller" başlıklı 15. maddesi uyarınca; "aşağıda sayılan kişisel veri işleme faaliyetleri bakımından veri sorumlusunun bu faaliyetleri Sicile kayıt etmesi ve bildirmesi yükümlülüğü yoktur:

i. Kişisel veri işlemenin suç işlenmesinin önlenmesi veya suç soruşturması için gerekli olması,

ii. İlgili kişinin kendisi tarafından alenileştirilmiş kişisel verilerin işlenmesi,

iii. Kişisel veri işlemenin kanunun verdiği yetkiye dayanılarak görevli ve yetkili kamu kurum ve kuruluşları ile kamu kurumu niteliğindeki meslek kuruluşlarınca, denetleme veya düzenleme görevlerinin yürütülmesi ile disiplin soruşturma veya kovuşturması için gerekli olması,

iv. Kişisel veri işlemenin bütçe, vergi ve mali konulara ilişkin olarak Devletin ekonomik ve mali çıkarlarının korunması için gerekli olması."

5.4.2. Kurul Kararlarıyla Belirlenen İstisnalar

Kurul, Sicile kaydolma yükümlülüğü noktasında hangi veri sorumlularının bu yükümlülükten muaf tutulacağı noktasında karar alma yetkisini haizdir. Bu kapsamda Yönetmeliğin "İstisna kriterleri" başlıklı 16. maddesi uyarınca; "Kurul, aşağıdaki kriterleri göz önünde bulundurarak kayıt yükümlülüğüne istisna getirebilir:

i. Kişisel verinin niteliği

ii. Kişisel verinin sayısı

iii. Kişisel verinin işlenme amacı

iv. Kişisel verinin işlendiği faaliyet alanı

v. Kişisel verinin üçüncü kişilere aktarılma durumu

vi. Kişisel veri işleme faaliyetinin kanunlardan kaynaklanması

vii. Kişisel verilerin muhafaza edilmesi süresi

viii. Veri konusu kişi grubu veya veri kategorileri"

Kurulun bu konuda "Veri Sorumluları Siciline Kayıt Yükümlülüğünden İstisna Tutulacak Veri Sorumluları" ile ilgili 02.04.2018 tarihli ve 2018/32 sayılı

bir karar[257] alarak 15.05.2018 tarihli ve 30422 sayılı Resmî Gazete'de yayımlanmıştır. Bu karar uyarınca Sicile kayıt yükümlülüğünden istisna tutulacak veri sorumluları kararın ekindeki listede belirtilmiştir. Kurulun 2018/32 sayılı kararının ekindeki liste uyarınca aşağıdaki veri sorumluları Sicile kaydolma yükümlülüğünden muaf tutulmuştur:

i. "Herhangi bir veri kayıt sisteminin parçası olmak kaydıyla yalnızca otomatik olmayan yollarla kişisel veri işleyenler

ii. 18.01.1972 tarihli ve 1512 sayılı Noterlik Kanunu uyarınca faaliyet gösteren noterler

iii. 04.11.2004 tarihli ve 5253 sayılı Dernekler Kanunu'na göre kurulmuş derneklerden, 20.02.2008 tarihli ve 5737 sayılı Vakıflar Kanunu'na göre kurulmuş vakıflardan ve 18.10.2012 tarihli 6356 sayılı Sendikalar ve Toplu İş Sözleşmesi Kanununa göre kurulmuş sendikalardan yalnızca ilgili mevzuat ve amaçlarına uygun, faaliyet alanlarıyla sınırlı ve sadece kendi çalışanlarına, üyelerine, mensuplarına ve bağışçılarına yönelik kişisel veri işleyenler

iv. 22.04.1983 tarihli ve 2820 sayılı Siyasi Partiler Kanununa göre kurulmuş siyasi partiler

v. 19.03.1969 tarihli ve 1136 sayılı Avukatlık Kanunu uyarınca faaliyet gösteren avukatlar

vi. 01.06.1989 tarihli ve 3568 sayılı Serbest Muhasebeci Mali Müşavirlik ve Yeminli Mali Müşavirlik Kanunu uyarınca faaliyet gösteren serbest muhasebeci mali müşavirler ve yeminli mali müşavirler"

Yukarıda değindiğimiz kararın dışında Kurul, 18.08.2018 tarihli ve 30513 sayılı Resmî Gazete'de yayımlanan üç farklı kararıyla;

i. Gümrük müşavirlerini[258]

---

[257] Kurulun 02.04.2018 tarihli ve 2018/32 sayılı kararına şu uzantıdan ulaşabilirsiniz: https://www.kvkk.gov.tr/Icerik/4233/2018-32 Erişim Tarihi: 5 Nisan 2020.

[258] Kurulun 28.06.2018 tarihli ve 2018/68 sayılı kararı. Bu karara şu uzantıdan ulaşabilirsiniz: https://www.resmigazete.gov.tr/eskiler/2018/08/20180818-4.pdf Erişim Tarihi: 6 Nisan 2020.

ii. Arabulucuları[259]

iii. Yıllık çalışan sayısı 50'den az ve yıllık mali bilanço toplamı 25 milyon TL'den az olan gerçek veya tüzel kişi veri sorumlularından ana faaliyet konusu özel nitelikli kişisel veri işleme olmayanları[260]

Sicile kayıt yükümlülüğünden muaf tutmuştur.

Özetleyecek olursak; avukatlar, noterler, serbest muhasebeci mali müşavir ve yeminli mali müşavirler, siyasi partiler, dernek, vakıf ve sendikalar, gümrük müşavirleri, arabulucular, herhangi bir veri kayıt sisteminin parçası olmak kaydıyla yalnızca otomatik olmayan yollarla kişisel veri işleyenler ile yıllık mali bilanço toplamı 25 milyon TL'den ve yıllık çalışan sayısı 50'den az olan gerçek veya tüzel kişi veri sorumlularından ana faaliyet konusu özel nitelikli kişisel veri işleme olmayanlar Sicile kaydolma yükümlülüğünden muaf tutulmuşlardır. Kurul alacağı yeni kararlarla yeni istisnalar getirebilecektir veya halihazırdaki istisnaları değiştirebilecektir.

Kurul kendisine gelen yurtdışında yerleşik olan tüzel kişilerin Türkiye'deki şubeleri ve irtibat bürolarının Sicile kaydolma yükümlülüğü hakkındaki görüş talebi üzerine 23.07.2019 tarihli ve 2019/225 sayılı kararı[261] almıştır. Bu karar uyarınca özetle "*kişisel veri işleme süreçleri bakımından merkezden bağımsız bir şekilde Türkiye'de veri sorumlusu kriterlerine uygun olarak hareket eden bu şubelerin veri sorumlusu sayılacağı*" tespitinden hareketle yurtdışında yerleşik tüzel kişilerin Türkiye'de yer alan şubelerinin Sicile kaydolmakla yükümlü olduğunu belirtmiştir.

Kurul aynı karar içinde yurtdışında yerleşik tüzel kişilerin Türkiye'de bulunan irtibat büroları ile ilgili şubelerden farklı karara varmıştır. Buna göre Kurulun 2019/225 sayılı kararında "*Türkiye'de irtibat bürosu açılabilmesi için şirket tüzel kişiliklerinin yabancı ülke kanunlarına göre kurulması ve kurulan irtibat bürolarının Türkiye'de ticari faaliyette bulunmaması gerektiği, irtibat*

---

[259] Kurulun 05.07.2018 tarihli ve 2018/75 sayılı kararı. Bu karara şu uzantıdan ulaşabilirsiniz: https://www.resmigazete.gov.tr/eskiler/2018/08/20180818-5.pdf Erişim Tarihi: 6 Nisan 2020.

[260] Kurulun 19.07.2018 tarihli ve 2018/87 sayılı kararı. Bu karara şu uzantıdan ulaşabilirsiniz: https://www.resmigazete.gov.tr/eskiler/2018/08/20180818-6.pdf Erişim Tarihi: 6 Nisan 2020.

[261] Kurulun 23.07.2019 tarihli ve 2019/225 sayılı kararına şu uzantıdan ulaşabilirsiniz: https://www.kvkk.gov.tr/Icerik/5545/2019-225 Erişim Tarihi: 6 Nisan 2020.

bürolarının ticari faaliyet dışında haberleşme, fizibilite araştırması yapma, sosyal ve kültürel alanlarda bazı çalışmaları yürütme, şirketler arasında birleşme ve devirler için ön hazırlık yapma, tanıtım ve reklam, ülkedeki iş olanaklarının yakından takip etme ve bu konular hakkında merkez firmaya bilgi verme amacı doğrultusunda açılan bürolar olması ve şube özelliği bulunmadığı hususu dikkate alındığında" karara konu irtibat bürolarının Sicile kaydolma yükümlülüklerinin bulunmadığına karar vermiştir.

5.5. Sicile Kayıt Yükümlülüğüyle İlgili Önemli Tarihler

Sicile kayıt yükümlülüğünün veri sorumluları tarafından ne zamana kadar yerine getirileceğiyle ilgili Kanun ve Yönetmelikte herhangi bir düzenleme yapılmamıştır. Bu konuda Kurulun "Sicile Kayıt Yükümlülüğünün Başlama Tarihleri" ile ilgili 19.07.2018 tarihli ve 2018/88 sayılı kararı[262] ile bu kararda belirlenen Sicile kayıt sürelerinin uzatılması hakkındaki 17.12.2019 tarihli ve 2019/387 sayılı[263] kararlar uyarınca veri sorumlularının hangi tarihten itibaren başlayarak Sicile kayıt başvurusunda bulunabileceği ve başvuruların hangi tarihe kadar yapılabileceği düzenlenmiştir. Kurulun 2018/88 ve 2019/387 sayılı kararları uyarınca veri sorumlularının Sicile kaydolma yükümlülüğü kapsamında bağlı oldukları süreler aşağıdaki gibidir:

i. "Yıllık çalışan sayısı 50'den çok veya yıllık mali bilanço toplamı 25 milyon TL'den çok olan gerçek ve tüzel kişi veri sorumluları için Veri Sorumluları Siciline kayıt yükümlülüğü başlangıç tarihi 01.10.2018 olup Sicile kayıt yaptırmaları için bu veri sorumlularına 30.06.2020 tarihine kadar süre verilmiştir."

ii. "Yurtdışında yerleşik gerçek ve tüzel kişi veri sorumluları için Veri Sorumluları Siciline kayıt yükümlülüğü başlangıç tarihi 01.10.2018

[262] Kurulun 19.07.2018 tarihli ve 2018/88 sayılı kararına şu uzantıdan ulaşabilirsiniz: https://www.kvkk.gov.tr/Icerik/5272/2018-88 Erişim Tarihi: 6 Nisan 2020.

[263] Kurulun 17.12.2019 tarihli ve 2019/387 sayılı kararına şu uzantıdan ulaşabilirsiniz: https://www.resmigazete.gov.tr/eskiler/2019/12/20191228-8.pdf Erişim Tarihi: 6 Nisan 2020.

olup Sicile kayıt yaptırmaları için bu veri sorumlularına 30.06.2020 tarihine kadar süre verilmiştir."

iii. "Yıllık çalışan sayısı 50'den az ve yıllık mali bilanço toplamı 25 milyon TL'den az olmakla birlikte ana faaliyet konusu özel nitelikli kişisel veri işleme olan gerçek ve tüzel kişi veri sorumluları için Veri Sorumluları Siciline kayıt yükümlülüğü başlangıç tarihi 01.01.2019 olup Sicile kayıt yaptırmaları için bu veri sorumlularına 30.09.2020 tarihine kadar süre verilmiştir."

iv. "Kamu kurum ve kuruluşu veri sorumluları için Veri Sorumluları Siciline kayıt yükümlülüğü başlangıç tarihi 01.04.2019 olup Sicile kayıt yaptırmaları için bu veri sorumlularına 31.12.2020 tarihine kadar süre verilmiştir."

5.6. İdari Yaptırım

Kanunun 18. maddesi uyarınca Kanunun 16. maddesinde öngörülen Veri Sorumluları Siciline kaydolma ve bildirim yükümlülüğüne aykırı hareket edilmesi durumunda ilgili veri sorumlularına 20.000 Türk Lirası'ndan 1.000.000 Türk Lirası'na kadar idari para cezası verilecektir.

Kanunun 18. maddesinde belirtilen tüm idari para cezaları her sene o yılın yeniden değerleme oranlarına göre hesaplanarak güncel idari para cezasının miktarı belirlenecektir.

Veri Sorumluları Siciline kayıt ve bildirim yükümlülüğüne aykırı hareket edilmesi durumunda uygulanacak idari para cezası için 2020 yılında uygulanacak alt sınır 36.053 Türk Lirası iken üst sınırı ise 1.802.641 Türk Lirası'dır.

SONUÇ

Teknolojinin her geçen gün hızla gelişmesi ile birlikte gerek devletler gerekse özel hukuk gerçek ve tüzel kişileri bünyesinde kişisel verilerin elde edilmesi, analiz edilmesi, aktarılması başta olmak üzere her türlü veri işleme faaliyetinin artması kaçınılmaz bir olgu haline gelmiştir. Özellikle bilgi teknolojileri ile internetin bir araya gelmesiyle birlikte veri işleme faaliyetleri daha önce hiç olmadığı kadar kolay bir hale gelmiştir. Bu durumun ticari hayata ve devlet işleyişine olumlu katkıları olmakla beraber, diğer yandan bireylerin temel hak ve özgürlüklerini tehdit eden bir noktaya da gelmiştir. Söz konusu tehditleri en aza indirgeyebilmek adına öncelikle uluslararası organizasyonlar ve devletler kişisel verilerin korunması alanında yasal düzenlemeler yapmaya başlayarak kontrol altına alınması zor olan bu alana hukuki sınırlar çizmeye başlamışlardır. Kişisel verilerin korunmasına yönelik düzenlemeler Avrupa'da 1980'li yıllarda yapılmaya başlamış ve 108 sayılı Sözleşme, 95/46/EC sayılı Direktif ve 2016/679 sayılı Genel Veri Koruma Tüzüğü (*General Data Protection Regulation - GDPR*) gibi önemli düzenlemeler hayata geçirilmiştir. Konuya ilişkin ülkemizdeki spesifik yansımalar ise kendini ilk defa 2010 Anayasa değişikliği ve 2016 yılında çıkarılan 6698 sayılı Kişisel Verilerin Korunması Kanunu ile birlikte göstermiştir. 6698 sayılı Kanun'un hazırlık çalışmalarının yapıldığı sırada GDPR'ın da hazırlık çalışmalarının yürütülüyor olmasına rağmen 6698 sayılı Kanun, daha güncel ve ayrıntılı düzenlemeler içeren GDPR'ı değil, 95/46/EC sayılı Direktif'i esas alarak hazırlanmıştır. Avrupa Birliği, GDPR'ı 2016 yılında kabul etmesiyle birlikte 95/46/EC sayılı Direktif'i yürürlükten kaldırmıştır.

Kişisel verilerin işlenmesinin günümüzde kaçınılmaz bir hale gelmesi olgusu kişisel verilerle ilgili yapılan faaliyetlerin bir hukuki disiplin altına alınması ve bireylerin temel hak ve özgürlüklerinden olan kişisel verilerinin korunması hakkını temin edebilmek adına devletlerin konuyla ilgili yasama faaliyetlerini zaman içerisinde yoğunlaştırmasına sebep olmuştur.

6698 sayılı Kanun'da kişisel verilerin işleme amaçlarını ve vasıtalarını belirleyen, veri kayıt sisteminin kurulmasından ve yönetilmesinden sorumlu olan

gerçek veya tüzel kişi olarak tanımlanan veri sorumluları ile veri sorumlusunun verdiği yetkiye dayanarak onun adına kişisel verileri işleyen gerçek veya tüzel kişi olarak tanımlan veri işleyenlere çeşitli yükümlülükler getirilmiş ve kişisel verilerin işlenmesine ilişkin uyulması gereken temel ilkeler belirlenmiştir. Buna göre veri sorumlularının; aydınlatma yükümlülüğü, kişisel veri sahibi ilgili kişiler tarafından yapılan başvuruları cevaplandırma ve Kişisel Verileri Koruma Kurulu'nun verdiği kararları yerine getirme yükümlülüğü, veri güvenliğini sağlama yükümlülüğü, kişisel verilerin silinmesi, yok edilmesi veya anonim hale getirilmesi yükümlülüğü, veri sorumluları siciline kayıt olma yükümlülükleri bulunmaktadır. Ayrıca kişisel verileri işleme faaliyeti esnasında sürecin başından sonuna kadar her aşamasında izlenmesi gereken birtakım ilkeler belirlenmiştir. Bu ilkeler; hukuka ve dürüstlük kurallarına uygun olarak işleme, doğru ve gerektiğinde güncel olma, belirli, açık ve meşru amaçlar için işleme, işlendikleri amaçla bağlantılı, sınırlı ve ölçülü olma, ilgili mevzuatta öngörülen veya işlendikleri amaç için gerekli olan süre kadar muhafaza edilme ilkeleridir. Veri sorumlusunun 6698 sayılı Kanun'da sayılı yükümlülüklerini salt yerine getirmesi veya veri işleme şartının bulunması yeterli olmayıp veri işlemenin her aşamasında kişisel verilerin işlenmesine ilişkin temel ilkelere uyması gerekmektedir. Aksi halde veri sorumlusunun veri işleme faaliyeti 6698 sayılı Kanun'a aykırı olmaya devam edecektir.

Veri sorumlusunun yükümlülüklerini yerine getirmemesi durumunda 6698 sayılı Kanun içerisinde düzenlenen idari para cezalarının ilgili veri sorumlusu hakkında uygulanması gündeme gelebilecektir. Ek olarak kişisel verilere ilişkin suçlar bakımından ise failin veri sorumlusu olup olmadığına bakılmaksızın 5237 sayılı Türk Ceza Kanunu'nun 135 ila 140. maddelerinin de uygulanması mümkündür.

Verinin çoğu madenden, sanayi ve endüstri dalından daha çok finansal değer ifade ettiği 21. yüzyılda kişisel verilerin korunması hukuku bir disiplin yaratmak amacıyla hızla gelişmeye devam edecektir. Önümüzdeki yıllarda GDPR'ın yaratacağı doktrinsel ve yargısal kazanımlar hiç şüphesiz Türkiye'deki kişisel verilerin korunması hukukunu ve uygulamaları etkileyecektir. Bu konuda Kişisel Verileri Koruma Kurulu'nun alacağı kararlar ve yapılacak ikincil düzenlemelerle,

6698 sayılı Kanun'da değinilmeyen birçok konunun kapsanması oldukça muhtemeldir.

KAYNAKÇA

Çalışma kapsamında yararlanılan tüm internet siteleri 28 Mayıs 2020 tarihinde ziyaret edilmiş olup bu tarih itibariyle internet sitesinin erişilebilir olduğu ve atıf yapılan içeriğin mevcut olduğu teyit edilmiştir.

1. KİTAP, MAKALE VE BİLGİ NOTLARI

Akdağ, Hale : Türk Ceza Kanunu Kapsamında Kişisel Verilerin Korunması, Adalet Yayınevi, Ankara, 2013

Akgül, Aydın : Danıştay ve Avrupa İnsan Hakları Mahkemesi Kararları Işığında Kişisel Verilerin Korunması, Beta, İstanbul 2014.

Aksoy, Hüseyin Can : Medeni Hukuk ve Özellikle Kişilik Hakkı Yönünden Kişisel Verilerin Korunması, Çakmak Yayınevi, Ankara 2010.

Aşıkoğlu, Şehriban İpek : "Veri Sorumlularının Aydınlatma Yükümlülüğü -Avrupa Birliği ve Türk Hukukunda-", Kişisel Verilerin Korunması Dergisi, Cilt 1, Sayı 2, s. 41-65, 2019.

Aşıkoğlu, Şehriban İpek : Avrupa Birliği ve Türk Hukukunda Kişisel Verilerin Korunması ve Büyük Veri, 1. Baskı, On İki Levha Yayıncılık, İstanbul 2018.

Atasoy, Kemal : Kişilik Hakkı Kapsamında Sosyal Medyada Kişisel Verilerin Korunması ve Veri Sahibinin Rızası, Marmara Üniversitesi Hukuk Araştırmaları Dergisi, Cilt 22, Sayı 3, s. 269-301, 2016.

Avcı Braun, Cihan : Kişisel Verilerin İşlenmesinde Rıza, Yeditepe Üniversitesi Hukuk Fakültesi Dergisi, Cilt 15, Sayı 1, s. 13-33, 2018.

Ayözger, A. Çiğdem : Kişisel Verilerin Korunması Elektronik Haberleşme Sektörüne İlişkin Özel Düzenlemeler Dahil, Beta Yayınevi, İstanbul 2016.

Başalp, Nilgün : "Avrupa Birliği Veri Koruması Genel Regülasyonu'nun Temel Yenilikleri", Marmara Üniversitesi Hukuk Araştırmaları Dergisi, Cilt 21, Sayı 1, s. 77-105, 2015.

Başalp, Nilgün : Kişisel Verilerin Korunması ve Saklanması, Yetkin Yayınları, Ankara 2004.

Beyleveld, Deryck : "The Duty to Provide Information to Data Subject: Articles 10 and 11 of Directive 95/46/EC", The Data Protection Directive and Medical Research Across Europe, İngiltere 2004.

Brasher, Elizabeth A. "Addressing the Failure of Anonymization: Guidance from the European Union's General Data Protection Regulation", Columbia University Business Law Review, Cilt 2018, s. 209-253, 2018, (Çevrimiçi) https://academiccommons.columbia.edu/doi/10.7916/d8-zgve-y962 .

Bygrave, Lee A. : Data Protection Law (Approaching Its Rationale, Logic and Limits), Kluwer Law International, Hollanda 2002.

Carey, Peter : Data Protection A Practical Guide to UK and EU Law, 2. Baskı, Oxford University Press, İngiltere 2004.

Clifford, Damian / **Graef**, Inge / **Valcke**, Peggy : "Pre-formulated Declarations of Data Subject Consent—Citizen-Consumer Empowerment and the Alignment of Data, Consumer and Competition Law Protections", German Law Journal, Cilt 20, Sayı 5, s. 679-721, 2019.

Çekin, Mesut Serdar : "6698 sayılı Kişisel Verilerin Korunması Hakkında Kanun'un Big Data (Büyük Veri) ve İrade Serbestisi Açısından Değerlendirilmesi", İstanbul Üniversitesi Hukuk Fakültesi Mecmuası, Cilt 74, Sayı 2, s. 629-644, 2016, (Çevrimiçi) http://static.dergipark.org.tr/article-download/ade8/9dcb/8112/58e4bb01ca41c.pdf? .

Çekin, Mesut Serdar : Avrupa Birliği Hukukuyla Mukayeseli Olarak 6698 Sayılı Kanun Çerçevesinde Kişisel Verilerin Korunması Hukuku, On İki Levha Yayınları, İstanbul 2019.

Çekin, Mesut Serdar : Avrupa Birliği Hukukuyla Mukayeseli Olarak 6698 Sayılı Kişisel Verilerin Korunması Kanunu, On İki Levha Yayınları, İstanbul 2018.

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

Diorio, Samantha : "Data Protection Laws: Quilts versus Brackets", Syracuse Journal of International Law and Commerce, Cilt 42, s. 485-513, 2014.

Dülger, Murat Volkan : "AB Genel Veri Koruma Tüzüğü ve KVKK'da Rıza Kavramı", (Çevrimiçi) http://dulger.av.tr/wp-content/uploads/2019/05/AB_Genel_Veri_Koruma_Tuzugu_GDPR_ve_KVKK.pdf .

Dülger, Murat Volkan : Kişisel Verilerin Korunması Hukuku, 2. Baskı, Hukuk Akademisi Yayınları, İstanbul 2019.

Dülger, Murat Volkan : "Kişisel Verilerin Korunması Kanunu ve Türk Ceza Kanunu Bağlamında Kişisel Verilerin Ceza

Normlarıyla Korunması", İstanbul Medipol Üniversitesi Hukuk Fakültesi Dergisi, Cilt 3, Sayı 2, 2016.

Dülger, Murat Volkan / **Kahraman**, Cansu Ceren : "KVKK'dan Kişisel Verilerin Yurt Dışına Aktarımında Önemli Bir Adım: Bağlayıcı Şirket Kuralları", 11 Nisan 2020, (Çevrimiçi) https://www.hukukihaber.net/kvkkdan-kisisel-verilerin-yurt-disina-aktariminda-onemli-bir-adim-baglayici-sirket-kurallari-makale,7685.html .

Emam, Khaled El / **Alvarez**, Cecilia : "A Critical Appraisal of the Article 29 Working Party Opinion 05/2014 on Data Anonymization Techniques", International Data Privacy Law, Cilt 5, Sayı 1, s. 73–87, 2015, (Çevrimiçi) https://academic.oup.com/idpl/article-abstract/5/1/73/2863828 .

Erem, Faruk : "Ceza Hukukunda Meslek Sırrı", Ankara Üniversitesi Hukuk Fakültesi Dergisi, Cilt 1, No:1, 1943, s. 44.

Ertaş, Şeref : Eşya Hukuku, 10. Baskı, Barış Yayınları, İzmir 2012.

Fialova, Eva : "Data Portability and Informational Self-Determination", Masaryk Univerity Journal of Law and Technology, Cilt 8, Sayı 1, s. 45-55, 2014.

Gerl, Armin / **Meier**, Bianca**.** : "The Layered Privacy Language Art. 12 – 14 GDPR Extension – Privacy Enhancing User Interfaces", Datenschutz und Datensich - DuD, Cilt 43, s. 747-752, 2019.

Han, Işık Aslı : "Kişisel Verilerin İşlenmesi Bağlamında Hukuka Uygunluk Sebebi Olarak Veri Sahibinin Rızası",

Galatasaray Üniversitesi Hukuk Fakültesi Dergisi, Cilt 1, Sayı 1, s. 417-459, 2019.

Hornung, Gerrit / **Schnabel**, Christoph : "Data Protection in Germany I: The Population Census Decision and The Right to Informational Self-Determination", Computer Law & Security Review, Cilt 25, Sayı 1, s. 84-88, Ocak 2009.

Kaya, Mehmet Bedii (Çeviren) "Avrupa Birliği Adalet Divanı'nın 13 Mayıs 2014 Tarihli Google Unutulma Hakkı Kararı (Karar Çevirisi)", 2015 (Çevrimiçi) https://www.mbkaya.com/hukuk/ab-unutulma-hakki-kararceviri.pdf .

Kaya, Mehmet Bedii / **Taştan**, Furkan Güven : Kişisel Veri Koruma Hukuku (Mevzuat - İçtihat - Bibliyografya), On İki Levha Yayınları, 2. Baskı İstanbul 2019, (Çevrimiçi) https://www.mbkaya.com/hukuk/veri-koruma-hukuku.pdf .

Kuner, Christopher : European Data Protection Law: Corporate Compliance and Regulation, Second Edition, Oxford University Press, Oxford 2007.

Küzeci, Elif : Kişisel Verilerin Korunması, 4. Bası, On İki Levha Yayıncılık, 2020.

Keser Berber, Leyla Çevrimiçi Davranışsal Reklamcılık (Online Behavioral Advertising) Uygulamaları Özelinde Kişisel Verilerin Korunması, İstanbul 2014.

Keser Berber, Leyla / **Atabey**, Ayça / **Mert**, Melis : E-Gizlilik Tüzük Taslağının Son Versiyonu Üzerine Düşünceler, Kişisel Verileri Koruma Dergisi, Cilt 1, Sayı 2, s. 66-74, 2019, (Çevrimiçi) https://www.verbis.com.tr/makaleler/mk9.pdf .

Keser Berber, Leyla / **Ülgü**, Mahir / **Er**, Cüneyd : Elektronik Sağlık Kayıtları ve Özel Hayatın Gizliliği, İstanbul Bilgi Üniversitesi Yayınları, İstanbul 2009.

Lloyd, Ian J. : Information Technology Law, Eighth Edition, Oxford University Press, Oxford 2017.

Manav, Eda : "İş İlişkisinde İşçinin Kişisel Verilerinin Korunması" Gazi Üniversitesi Hukuk Fakültesi Dergisi, C. XIX, S. 2, s. 95-136, 2015.

Oğuzman, M. Kemal / **Barlas**, Nami : Medeni Hukuk, 17. Bası, Vedat Kitapçılık, İstanbul 2011.

Ozan, Selek : "Genel Veri Koruma Tüzüğü Işığında Kişisel Verilerin İşlenmesinde Rıza Açıklaması", DergiPark/Dokuz Eylül Üniversitesi Hukuk Fakültesi Dergisi, C. 21, S. 2, s. 911-951, 2019.

Polonetsky, Jules / **Tene**, Omer / **Finch**, Kelsey : "Shades of Gray: Seeing The Full Spectrum of Practical Data De-Identification", Santa Clara Law Review, Cilt 56, Sayı 3, s. 593-629, 2016, (Çevrimiçi) https://digitalcommons.law.scu.edu/cgi/viewcontent.cgi?article=2827&context=lawreview .

Samuelson, Pamela : "Privacy as Intellectual Property?", Stanford Law Review, Cilt 52, s. 1125-1173, 2000.

Schwartz, Paul : "Computer in German and American Constitutional Law: Towards an American Right of Informational Self-Determination", American Journal of Comparative Law, Cilt 37, s. 675-702, 1989.

Sirmen, Lale : Eşya Hukuku, Yetkin Yayınları, Ankara 2013.

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, Cilt 34, Sayı 2, s. 284-322, 2017, (Çevrimiçi)

https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2927945 .

Şimşek, Oğuz : Anayasa Hukukunda Kişisel Verilerin Korunması, Beta, İstanbul 2008.

Taştan, Furkan Güven : Türk Sözleşme Hukukunda Kişisel Verilerin Korunması, 2. Baskı, On İki Levha Yayınları, İstanbul 2017.

Uyarer, Sinem Göçmen : Kişisel Verilerin Korunması Kanunu ve Türk Ceza Kanunu Kapsamında Kişisel Verilerin Korunması, Seçkin Yayınevi, 2019.

Ünal, Mücahit : "Ses ve Görüntü Verilerinin Paylaşılmasının Kişisel Verilerin Korunması Kanunu Açısından Değerlendirilmesi", Lexpera Blog, 02.06.2020, (Çevrimiçi) https://blog.lexpera.com.tr/ses-ve-goruntu-verilerinin-paylasilmasinin-kisisel-verilerin-korunmasi-kanunu-acisindan-degerlendirilmesi/ .

Üzeltürk Tahmazoğlu, Sultan : "Kişisel Verilerin Korunması Hakkında Anayasa Değişikliği", Legal Hukuk Dergisi, S. 93, s. 3151-3156, 2010.

Yücedağ, Nafiye : "Kişisel Verilerin Korunması Kanunu Kapsamında Genel İlkeler", Kişisel Verileri Koruma Dergisi, Cilt 1, Sayı 1, s. 47-63, 2019.

Yücedağ, Nafiye : "Medeni Hukuk Açısından Kişisel Verilerin Korunması Kanunu'nun Uygulama Alanı ve Genel Hukuka Uygunluk Sebepleri", İstanbul Üniversitesi Hukuk Fakültesi Mecmuası, Cilt 75, Sayı 2, s. 765-790, 2017.

2. BELGE, GÖRÜŞ, ARAŞTIRMA, KARAR VE RAPORLAR

Article 29 Data Protection Working Party

- Opinion 4/2007 on the Concept of Personal Data, 20 Haziran 2007, 01248/07/EN, WP 136, (Çevrimiçi) https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2007/wp136_en.pdf .
- Opinion 1/2010 on the Concepts of "Controller" and "Processor", 16 Şubat 2010, 00264/10/EN, WP 169, (Çevrimiçi) https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2010/wp169_en.pdf .
- Opinion 06/2014 on the Notion of Legitimate Interests of the Data Controller Under Article 7 of Directive 95/46/EC, 9 Nisan 2014, 844/14/EN, WP217, (Çevrimiçi) https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp217_en.pdf .
- Guidelines on Transparency Under Regulation 2016/679, 11 Nisan 2018, 17/EN, WP260 rev.01, (Çevrimiçi) https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=622227 .
- Opinion 05/2014 on Anonymisation Techniques, 10 Nisan 2014, 0829/14/EN, WP216, (Çevrimiçi) https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp216_en.pdf .
- Working Document Setting Up a Table With the Elements and Principles to Be Found in Binding Corporate Rules, 6 Şubat 2018, 18/EN, WP256 rev.01, (Çevrimiçi) https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=614109 .

Avrupa Birliği Adalet Divanı

- 1 Ekim 2019 tarihli ve C-673/17 sayılı Bundesverband der Verbraucherzentralen und Verbraucherverbände — Verbraucherzentrale Bundesverband eV v. Planet49 GmbH kararı (Planet49 Kararı), (Çevrimiçi)

http://curia.europa.eu/juris/document/document.jsf;jsessionid=E1263B9218236FAB0174B7EB1208B0E7?text=&docid=218462&pageIndex=0&doclang=en&mode=lst&dir=&occ=first&part=1&cid=609404 .

- 8 Nisan 2014 tarihli, C-293/12 ve C-594/12 sayılı karar, (Çevrimiçi) https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX:62012CJ0293 .

Commission Nationale de l'Informatique et des Libertés (Bilgi ve Özgürlük Ulusal Komitesi - Fransa)

- Deliberation of the Restricted Committee SAN-2019-001 of 21 January 2019 Pronouncing a Financial Sanction Against GOOGLE LLC**,** (Çevrimiçi) https://www.cnil.fr/sites/default/files/atoms/files/san-2019-001.pdf .

European Data Protection Board

- Guidelines 05/2020 on Consent Under Regulation 2016/676, 4 Mayıs 2020, Version 1.1, (Çevrimiçi), https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_202005_consent_en.pdf .

Information Commissioner's Office

- Guide to the General Data Protection Regulation (GDPR), 22 Mayıs 2019 - 1.0.699, (Çevrimiçi) https://ico.org.uk/media/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr-1-0.pdf .

- Deleting Personal Data, 20140226, Version: 1.1, (Çevrimiçi) https://ico.org.uk/media/for-organisations/documents/1475/deleting_personal_data.pdf .

- Anonymisation: Managing Data Protection Risk Code of Practice, İngiltere 2012, (Çevrimiçi) https://ico.org.uk/media/for-organisations/documents/1061/anonymisation-code.pdf .

Kişisel Verileri Koruma Kurumu

- Açık Rıza Rehberi, (Çevrimiçi) https://www.kvkk.gov.tr/SharedFolderServer/CMSFiles/66b2e9c4-223a-4230-b745-568f096fd7de.pdf .
- Kişisel Verilerin İşlenme Şartları Rehberi, (Çevrimiçi) https://www.kvkk.gov.tr/SharedFolderServer/CMSFiles/8c90423f-97ea-4d81-a7c1-ace74295c2b8.pdf .
- Örneklerle Kişisel Verilerin Korunması, (Çevrimiçi) https://www.kvkk.gov.tr/Icerik/5521/Orneklerle-Kisisel-Verilerin-Korunmasi-Dokumani-Kurum-Internet-Sayfasinda-Yayinlanmistir- .
- İlgili Kişinin Hak Arama Rehberi, (Çevrimiçi) https://www.kvkk.gov.tr/SharedFolderServer/CMSFiles/7226b55d-b1e7-4e78-a3c4-0b1ba82ce542.pdf .
- Kişisel Veri Güvenliği Rehberi (Teknik ve İdari Tedbirler), Ankara 2018, (Çevrimiçi) https://www.kvkk.gov.tr/yayinlar/veri_guvenligi_rehberi.pdf .
- 100 Soruda Kişisel Verilerin Korunması Kanunu, Ankara 2018, (Çevrimiçi) https://www.kvkk.gov.tr/SharedFolderServer/CMSFiles/7d5b0a2f-e0ea-41e0-bf0b-bc9e43dfb57a.pdf .
- Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi Rehberi, Ankara 2018, (Çevrimiçi) https://www.kvkk.gov.tr/SharedFolderServer/CMSFiles/bc1cb353-ef85-4e58-bb99-3bba31258508.pdf .
- Aydınlatma Yükümlülüğünün Yerine Getirilmesi Rehberi, Ankara 2019, (Çevrimiçi)

https://www.kvkk.gov.tr/SharedFolderServer/CMSFiles/a569a068-c079-4189-b134-f57bc727af7d.pdf .

- Kişisel Verilerin Korunması Hakkında Sıkça Sorulan Sorular, KVKK Yayınları, Ankara 2018, (Çevrimiçi) https://www.kvkk.gov.tr/Icerik/4196/Kisisel-Verilerin-Korunmasi-Kanunu-Hakkinda-Sikca-Sorulan-Sorular .
- Kurulun 10 Nisan 2020 yayınlanma tarihli "Bağlayıcı Şirket Kuralları Hakkında Duyuru" başlıklı açıklaması, https://www.kvkk.gov.tr/Icerik/6728/YURT-DISINA-KISISEL-VERI-AKTARIMINDA-BAGLAYICI-SIRKET-KURALLARI-HAKKINDA-DUYURU .
- Kurulun yurt dışına kişisel veri aktarılması kapsamında hazırladığı taahhütname örnekleri, https://www.kvkk.gov.tr/Icerik/2053/Yurtdisina-Aktarim .
- Veri Sorumlusu ve Veri İşleyen, (Çevrimiçi) https://www.kvkk.gov.tr/SharedFolderServer/CMSFiles/f63e88cd-e060-4424-b4b5-f6413c602060.pdf .
- Kurulun 02.04.2018 tarihli ve 2018/32 sayılı kararı, https://www.kvkk.gov.tr/Icerik/4233/2018-32 .
- Kurulun 19.07.2018 tarihli ve 2018/88 sayılı kararı, https://www.kvkk.gov.tr/Icerik/5272/2018-88 .
- Kurulun 17.12.2019 tarihli ve 2019/387 sayılı kararı, https://www.resmigazete.gov.tr/eskiler/2019/12/20191228-8.pdf .
- Kurulun 05.07.2018 tarihli ve 2018/75 sayılı kararı, https://www.resmigazete.gov.tr/eskiler/2018/08/20180818-5.pdf .
- Kurulun 19.07.2018 tarihli ve 2018/87 sayılı kararı, https://www.resmigazete.gov.tr/eskiler/2018/08/20180818-6.pdf .

- Kurulun 23.07.2019 tarihli ve 2019/225 sayılı kararı, https://www.kvkk.gov.tr/Icerik/5545/2019-225 .
- Kurulun 02.04.2018 tarihli ve 2018/32 sayılı kararı, https://www.kvkk.gov.tr/Icerik/4233/2018-32 .
- Kurulun 28.06.2018 tarihli ve 2018/68 sayılı kararı, https://www.resmigazete.gov.tr/eskiler/2018/08/20180818-4.pdf .
- Kurulun 18.09.2019 tarihli ve 2019/271 sayılı kararı, https://www.kvkk.gov.tr/Icerik/5547/2019-271 .
- Kurulun 27.02.2020 tarihli ve 2020/173 sayılı kararı, https://www.kvkk.gov.tr/Icerik/6739/2020-173 .
- Kurulun 24.01.2019 tarihli ve 2019/9 sayılı kararı, https://www.kvkk.gov.tr/Icerik/5358/Kamuoyu-Duyurusu .
- Kurulun 24.01.2019 tarihli ve 2019/10 sayılı kararı, Veri İhlali Bildirim Formu ve Veri İhlali Bildirim Formu Kılavuzu, https://www.kvkk.gov.tr/Icerik/5362/Veri-Ihlali-Bildirimi .
- Kurulun 31.01.2018 tarihli ve 2018/10 sayılı kararı, https://www.kvkk.gov.tr/Icerik/4110/2018-10 .
- Kurulun 25.03.2019 tarihli ve 2019/82 sayılı kararı, https://www.kvkk.gov.tr/Icerik/5463/-Bir-market-zincirinin-sadakat-kart-uygulamasina-iliskin-ihbar-ve-sikayetler-hakkinda-Kisisel-Verileri-Koruma-Kurulunun-25-03-2019-tarihli-ve-2019-82-sayili-Karari .
- Kurulun 02.05.2019 tarihli ve 2019/122 sayılı kararı, https://www.kvkk.gov.tr/Icerik/5461/2019/122 .
- Kurulun 26.07.2018 tarihli ve 2018/90 sayılı kararı, https://www.kvkk.gov.tr/Icerik/5420/-Veri-sorumlusu-tarafindan-aydinlatma-yukumlulugu-ve-acik-riza-onayi-alinmasi-sureclerinin-ayri-

ayri-yerine-getirilmesi-gerektigi-ile-ilgili-Kisisel-Verileri-Koruma-Kurulunun-26-07-2018-tarihli-ve-2018-90-sayili-Karar-Ozeti .

- Kurul'un 02.05.2019 tarihli ve 2019/125 sayılı kararı, https://www.kvkk.gov.tr/Icerik/5470/Kisisel-Verileri-Koruma-Kurulu-nun-Yeni-Yayinlanan-Karari .
- Kurulu'nun 25.03.2019 tarihli ve 2019/78 sayılı kararı, https://www.kvkk.gov.tr/Icerik/5434/2019-78 .

Ekonomik İş Birliği ve Kalkınma Örgütü (OECD)

- 23 Eylül 1980 tarihinde kabul edilen Özel Yaşamın Gizliliğinin ve Sınır Ötesi Kişisel Veri Dolaşımının Korunmasına İlişkin Rehber İlkeler (*Protection of Privacy and Transborder Flows of Personal Data*), (Çevrimiçi) https://www.oecd.org/internet/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm .
- 2013 tarihli "The OECD Privacy Framework", (Çevrimiçi) https://www.oecd.org/sti/ieconomy/oecd_privacy_framework.pdf .

3. DİĞER KAYNAKLAR

- https://www.ab.gov.tr
- https://academic.oup.com/journals
- https://www.coe.int
- https://www.cambridge.org/core
- https://curia.europa.eu
- https://www.danistay.gov.tr
- https://ec.europa.eu
- https://edpb.europa.eu/edpb_en

- https://www.europarl.europa.eu
- https://ico.org.uk/
- https://www.kvkk.gov.tr
- https://www.law.cornell.edu
- https://www.mevzuat.gov.tr
- http://www.oecd.org
- https://www.ohchr.org
- https://www.resmigazete.gov.tr
- https://www.un.org