

T.C.
İSTANBUL ÜNİVERSİTESİ
SOSYAL BİLİMLER ENSTİTÜSÜ
ÖZEL HUKUK ANABİLİM DALI

Yüksek Lisans Tezi

“TÜRK VE AVRUPA BİRLİĞİ HUKUKUNDA
KİŞİSEL VERİLERİN AKTARILMASI”

Nijat AMIRASLANLI

2501181428

Tez Danışmanı

Doç. Dr. Abdurrahman SAVAŞ

İSTANBUL, 2022

ÖZ

TÜRK VE AVRUPA BİRLİĞİ HUKUKUNDA KİŞİSEL VERİLERİN AKTARILMASI

Nijat AMIRASLANLI

Modern dünyada kişisel verilerimizin sürekli el değiştirmesi, hatta saniyeler içerisinde başka ülkelere aktarılabilmesi olağan bir hâl aldığı gibi, kontrolümüzden çıkan verilerimizin güvenliğinin nasıl temin edileceği endişesi de gitgide büyümektedir. 1970’lerden bu yana farklı ülkeler tarafından düzenlenmiş olmasına rağmen, kişisel verilerin aktarılması, hâlâ zaman zaman ülkeler arasında sorun olarak kalabilmektedir. Bu nedenle bu çalışmada kişisel verilerin aktarılması kavramına dair Türk ve Avrupa Birliği hukukundaki düzenlemeler incelenmiştir.

Çalışma üç bölümden oluşmaktadır. İlk bölümde temel kavramların tanımlanmasına ve bunların yer aldığı temel düzenlemelere yer verilmiştir. İkinci bölümde kişisel verilerin aktarılmasına dair Avrupa Birliği Genel Veri Koruma Tüzüğü’nde yer alan düzenlemeler incelenmiştir. Son bölümde ise konuyla ilgili 6698 sayılı Kişisel Verileri Koruma Kanunu’nda öngörülen düzenlemeler ele alınmıştır.

Anahtar kelimeler: kişisel veriler, kişisel verilerin aktarılması, yeterlilik kararı, uygun güvenlik önlemleri, açık rıza.

ABSTRACT

THE TRANSFER OF PERSONAL DATA IN TURKISH AND EUROPEAN UNION LAW

Nijat AMIRASLANLI

While the fact that our personal data is constantly being exchanged and can even be transferred to other countries in a few seconds has become normal in the modern world, the concern about how to ensure the security of personal data that is out of our control is growing. Although it has been regulated by different countries since the 1970s, the transfer of personal data still remains a problem among countries from time to time. For this reason, this thesis analyses the regulations in Turkish and the European Union law regarding the transfer of personal data.

This thesis consists of three chapters. In the first chapter, the definitions of basic concepts are placed, as well as fundamental regulations that include concepts thereof. The second chapter discusses the provisions regarding the transfer of personal data considered in the General Data Protection Regulation of the European Union. The provisions stipulated in the Personal Data Protection Law No. 6698 are examined in the last chapter.

Keywords: personal data, transfer of personal data, adequacy decisions, appropriate safeguards, explicit consent.

ÖNSÖZ

Kişisel verilerin işlenmesi türleri içerisinde niteliği gereği, verilerin korunması açısından daha fazla risk barındıran ve daha hassas koruma gerektiren kişisel verilerin aktarılması faaliyeti, hemen hemen bütün ulusal ve uluslararası düzenlemelerde daha titiz ve detaylı bir şekilde düzenlenmektedir. Veri koruma alanında örnek düzenleme olarak nitelendirilen Avrupa Birliği hukukunun aksine, ülkemizde bu alanda düzenlemelere son yıllarda gidilmiştir. Buna rağmen kişisel verilerin aktarılmasına ilişkin teorik ve pratik sorunların hâlen devam etmekte olduğu da gözlemlenmektedir. Bu nedenle çalışmamızda kişisel verilerin aktarılması faaliyetini Avrupa Birliği ve Türk hukukundaki düzenlemeler, içtihat, doktrin ve Kurul kararları ışığında değerlendirmeye ve konuyla ilgili iki hukuk sistemi arasındaki farklı yaklaşımları incelemeye çalıştık.

Öncelikle, ilk akademik çalışmam olan bu tezin danışmanlığını kabul ederek beni onurlandıran ve tez yazım süreci boyunca hiçbir desteğini esirgemeyen, yapıcı eleştirileri ve yönlendirmeleriyle bu çalışmanın ortaya çıkmasında büyük emeği olan Sayın Hocam Doç. Dr. Abdurrahman Savaş'a teşekkür etmeyi borç bilirim.

Bu tezin yazılma sürecinin bir kısmını, kütüphanesinde araştırma yapma hakkı kazandığım Saarland Üniversitesi Avrupa Enstitüsü'nde geçirdim. Bu süre zarfı için danışmanlığımı üstlenen, sıkı pandemi kısıtlamalarına rağmen düzenli bir şekilde bana zaman ayırarak teklif ve eleştirileri ile tezime katkı sağlayan Sayın Hocam Ass.iur. Mareike Fröhlich'e teşekkürlerimi arz ederim.

Ayrıca, bu süreç boyunca her türlü desteğini üzerimde hissettiğim aileme, daima beni dinleyerek görüşlerini paylaşan, kaynaklara erişimimi kolaylaştıran değerli arkadaşlarıma desteklerinden dolayı müteşekkirim.

Nijat AMIRASLANLI

İstanbul, 2022

İÇİNDEKİLER

ÖZ.....	I
ABSTRACT.....	II
ÖNSÖZ.....	III
İÇİNDEKİLER	IV
KISALTMALAR LİSTESİ.....	IX
GİRİŞ	1

BİRİNCİ BÖLÜM

TEMEL KAVRAMLAR VE TARİHSEL GELİŞİM

I. Kişisel Veri	5
A. Tanımı	5
B. Unsurları.....	7
1. Bilgi.....	7
2. Belirli veya Belirlenebilir Kişi	9
a. Kişi	9
b. Belirli veya Belirlenebilir Olma.....	11
3. Kişiyeye İlişkin Olma	12
II. Özel Nitelikli Kişisel Veriler.....	14
A. Tanımı	14
B. Kapsamı.....	15
III. Kişisel Verilerin Aktarılması	17
A. Tanımı	17
B. Kişisel Verilerin Transit Geçişi	28
C. Kişisel Verilerin Aktarılmasına Dair Hukuki Düzenlemeler	30
1. İlk Düzenlemeler.....	30
2. OECD Düzenlemeleri	31
3. Avrupa Konseyi Düzenlemeleri.....	32
4. Birleşmiş Milletler Düzenlemeleri.....	35
5. Avrupa Birliği Düzenlemeleri.....	36

6. Türk Hukukundaki Düzenlemeler.....	39
---------------------------------------	----

İKİNCİ BÖLÜM

AVRUPA BİRLİĞİ HUKUKUNDA KİŞİSEL VERİLERİN AKTARILMASI

I. Genel Olarak	43
II. Avrupa Birliği Dâhilinde Kişisel Verilerin Serbest Dolaşımı	44
III. Kişisel Verilerin Birlik Dışına Aktarılması.....	46
A. Genel Olarak	46
B. Yeterlilik Kararına Dayalı Aktarılma	50
1. Genel Olarak	50
2. Yeterlilik Değerlendirmesinde Dikkate Alınması Gereken Hususlar	52
3. Yeterlilik Kararlarının Gözden Geçirilmesi.....	55
4. Tam ve Kısmi Yeterlilik Kararları	57
a. Avrupa Birliği ve ABD Arasında “Güvenli Liman” Anlaşması	58
b. Avrupa Birliği ve ABD Arasında “Gizlilik Kalkanı” Anlaşması	62
C. Uygun Önlemlerin Alınması Kaydıyla Aktarılma	67
1. Kamu Kuruluşları Arasında Yasal Bağlayıcılığı Bulunan Belge veya İdari Düzenlemelere Eklenecek Hükümler.....	69
2. Sözleşme Hükümleri	71
3. Bağlayıcı Şirket Kuralları	78
4. Onaylanmış Davranış Kuralları.....	83
5. Onaylanmış Belgelendirme Mekanizmaları.....	86
D. Belirli Durumlar İçin İstisnalar	87
1. Açık Rıza.....	88
2. Sözleşmenin Yürütülmesi	90
3. İlgili Kişi Yararına Sözleşmenin İmzalanması veya Yürütülmesi	92
4. Kamu Yararı.....	93
5. Hukuki İddialarda Bulunulması, Bu İddiaların Uygulanması veya Savunulması	94
6. Hayati Menfaatlerinin Korunması.....	95

7. Aktarımın Kamuoyuna Açık Bir Sicilden Yapılması	96
8. Veri Sorumlusunun Zorlayıcı Meşru Menfaati	97
E. Uluslararası Anlaşmalara Dayalı Aktarımlar.....	99
1. PNR Anlaşmaları	100
2. SWIFT Anlaşması.....	103
3. Birlik Hukuku Çerçevesinde Yetkilendirilmeyen Aktarımlar	105

ÜÇÜNCÜ BÖLÜM

TÜRK HUKUKUNDA KİŞİSEL VERİLERİN AKTARILMASI

I. Genel Olarak.....	108
II. Kişisel Verilerin Aktarılmasına Dair Temel İlkeler	109
A. Veri Aktarımının Hukuka ve Dürüstlük Kurallarına Uygun Olması	109
B. Aktarılan Verinin Doğru ve Güncel Olması.....	110
C. Veri Aktarımının Belirli, Açık ve Meşru Amaçlar İçin Yapılması.....	111
D. Veri Aktarımının Amaca Bağlı, Sınırlı ve Ölçülü Olması	112
E. Aktarılan Verilerin Sınırlı Süre ile Muhafazası.....	113
III. Kişisel Verilerin Yurt İçinde Aktarılması	114
A. Genel Olarak	114
B. Açık Rızaya Dayalı Aktarımlar	116
1. Açık Rızanın Tanımı	116
2. Belirli Bir Konuya İlişkin Olma.....	118
3. Bilgilendirmeye Dayalı Olma	119
4. Özgür İradeyle Alınmış Olma.....	122
C. Açık Rızanın Aranmadığı Durumlar	124
1. Genel Nitelikli Kişisel Veriler Açısından	127
a. Kanunlarda Açıkça Öngörülme.....	127
b. Fiilî İmkansızlık Nedeniyle Rızasını Açıklayamayacak Durumda Bulunan veya Rızasına Hukuki Geçerlilik Tanınmayan Kişinin Kendisinin ya da Bir Başkasının Hayatı veya Beden Bütünlüğünün Korunması İçin Zorunlu Olması	130

c. Sözleşmenin Taraflarına Ait Kişisel Verilerin Aktarılmasının Gerekli Olması	131
d. Veri Sorumlusunun Hukuki Yükümlülüğünü Yerine Getirebilmesi İçin Zorunlu Olması	133
e. Verinin İlgili Kişinin Kendisi Tarafından Alenileştirilmiş Olması.....	134
f. Bir Hakkın Tesisi, Kullanılması veya Korunması İçin Veri Aktarımının Zorunlu Olması	136
g. Veri Sorumlusunun Meşru Menfaatleri İçin Veri Aktarımının Zorunlu Olması	136
2. Özel Nitelikli Kişisel Veriler Açısından	138
a. Sağlık ve Cinsel Hayat Dışındaki Kişisel Verilerin Aktarılması	139
b. Sağlık ve Cinsel Hayata İlişkin Kişisel Verilerin Aktarılması.....	140
(1) Kamu Sağlığının Korunması	141
(2) Koruyucu Hekimlik	142
(3) Tıbbi Teşhis, Tedavi ve Bakım Hizmetlerinin Yürütülmesi	143
(4) Sağlık Hizmetleri ile Finansmanın Planlanması ve Yönetimi.....	144
(5) Sır Saklama Yükümlülüğü Altında Bulunan Kişi veya Yetkili Kurum ve Kuruluşlar	145
c. Özel Nitelikli Kişisel Verilerin Aktarılması Zamanı Alınması Gereken Yeterli Önlemler.....	149
IV. Kişisel Verilerin Yurt Dışına Aktarılması	154
A. Genel Olarak	154
B. Yeterli Korumanın Bulunduğu Durumlarda Aktarılma	160
C. Yeterli Korumanın Bulunmadığı Durumlarda Aktarılma	163
1. Yazılı Taahhütnameler	163
a. Genel Olarak.....	163
b. Taahhütname Başvurularında Dikkat Edilmesi Gereken Hususlar.....	165
(1) Usule İlişkin Dikkat Edilmesi Gereken Hususlar.....	166
(2) Esasa İlişkin Dikkat Edilmesi Gereken Hususlar	167
c. Taahhütnamelerde Yer Alması Gereken Asgari Yükümlülükler	168
2. Bağlayıcı Şirket Kuralları	170

D. Yurt Dışına Veri Aktarımında 108 Sayılı Sözleşme'nin Yeri	174
E. Kişisel Verilerin Yurt Dışına Aktarılmasına Dair Türk ve Avrupa Birliği Hukukundaki Yaklaşımların Karşılaştırılması	177
SONUÇ	182
KAYNAKÇA	189



KISALTMALAR LİSTESİ

108 sayılı Sözleşme : 108 sayılı Kişisel Verilerin Otomatik İşleme Tabi Tutulması Karşısında Bireylerin Korunması Sözleşmesi

95/46/EC sayılı DPD: 95/46/EC sayılı Kişisel Verilerin İşlenmesi ve Bu Tür Verilerin Serbest Dolaşımına Dair Bireylerin Korunması Yönergesi (Data Protection Directive)

AB : Avrupa Birliği

ABAD : Avrupa Birliği Adalet Divanı

AEA : Avrupa Ekonomik Alanı

AK : Avrupa Konseyi

a.y. : aynı yer

bkz. : bakınız

bkz.: aş. : bakınız aşağıya

bkz.: yuk. : bakınız yukarıya

BM : Birleşmiş Milletler

bs. : baskı

CD. : Ceza Dairesi

CFR : AB Temel Haklar Şartı (The Charter of Fundamental Rights of European Union)

Çev. : Çeviren

dn. : dipnot

E. : Esas

Ed. : Editör

EDPB	: Avrupa Veri Koruma Kurulu (European Data Protection Board)
EDPS	: Avrupa Veri Koruma Denetmeni (European Data Protection Supervisor)
f.	: fıkra
GDPR	: 2016/679/EU sayılı Avrupa Birliği Genel Veri Koruma Tüzüğü (General Data Protection Regulation)
K.	: Karar
KVKK	: 6698 sayılı Kişisel Verilerin Korunması Kanunu
m.	: madde
OECD	: Organisation for Economic Co-operation and Development (Ekonomik Kalkınma ve İşbirliği Örgütü)
par.	: paragraf
RG.	: Resmî Gazete
s.	: sayfa
S.	: Sayı
T.	: Tarih
TFEU	: Avrupa Birliği'nin İşleyişi hakkında Sözleşme (the Treaty on the Functioning of the European Union)
v.d.	: ve diğerleri

GİRİŞ

Kişisel verilerin hukuki düzenlemelere konu edildiği ilk dönemlerden bu yana, verilerin korunmasını sağlamak amacıyla kişisel veriler üzerinde gerçekleştirilen her türlü eylem, yani kişisel verilerin işlenmesi, hukuki düzenlemelere tabi tutulmuştur. Başka bir deyişle, veri işlemeye sadece yasal düzenlemelerde öngörülen hâllerde ve ölçüde, aynı zamanda veri işleme ilkeleriyle uyum çerçevesinde izin verilmiştir.

Kişisel verilerin korunması tarihçesine bakıldığında, 1960'lı yıllardan itibaren veri korumaya yönelik tereddütlerin meydana çıktığı ve ilgili çevreler nezdinde tartışma konusu olduğu görülmektedir. Bu tartışmalar, 1970'li yıllara gelindiğinde yerini hukuki düzenleme çalışmalarına bırakmıştır. Çalışmaların uluslararası düzeyde sonuçları ise 1980'li yıllarda kendini göstermeye başlamıştır¹. Şöyle ki, 1980 yılında Ekonomik Kalkınma ve İşbirliği Örgütü (OECD), kişisel verilerin korunması adına rehber ilkeler yayınlamış², 1981 yılında AK, bu alanda ilk bağlayıcı uluslararası sözleşmeyi³ ihdas etmiştir. Ulusal düzeyde ilk çalışmaların da başladığı bu yıllarda Türkiye de veri koruma alanında ilk adımı atarak AK'nin bu sözleşmesini imzalamıştır.

Fakat yıllar içerisinde gelişen teknolojiye paralel olarak kişisel verilerin korunması meselesi de daha sık gündeme gelmiş ve daha detaylı düzenlemelere gidilmesi ihtiyacı ortaya çıkmıştır. Nitekim Avrupa Konseyi'nin (AK) 28 Ocak 1981 tarihli ve 108 sayılı "Kişisel Verilerin Otomatik İşleme Tabi Tutulması Karşısında Bireylerin Korunması Sözleşmesi"nin⁴ (108 sayılı Sözleşme) Türkiye tarafından onaylanarak yürürlüğe konulması ve bu alanda ilk özel kanun olan 6698 sayılı Kişisel Verileri Koruma Kanunu'nun⁵ (KVKK) kabul edilmesi de son yıllara denk

¹ Sevgi Erarslan, **Özel Nitelikli Kişisel Verilerin İşlenmesinde Açık Rızanın Aranmadığı Haller**, 2. bs., İstanbul, On İki Levha, 2020, s. 2.

² Bkz.: aş., Birinci Bölüm, "OECD Çerçevesinde Düzenlemeler" başlığı.

³ Bkz.: aş., Birinci Bölüm, "Avrupa Konseyi Çerçevesinde Düzenlemeler" başlığı.

⁴ Council of Europe, "Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data", (çevrimiçi), <https://www.coe.int/en/web/conventions/full-list/-/conventions/rms/0900001680078b37>, 27.12.2021.

⁵ RG. T. 07.04.2016, S. 29677.

gelmektedir⁶. Bunun temel sebebi, modern iletişim araçları sayesinde toplanan verilerin kişiler, kurumlar ve hatta ülkeler arasında kolayca paylaşılabılır hâle gelmiş olması ve kişisel verilerin aktarılması faaliyetinin çok ciddi boyutlara ulaşmış olmasıdır⁷. Bu nedenle hemen hemen bütün ulusal ve uluslararası mevzuatta, bir veri işleme türü olmasına rağmen aktarılma faaliyeti, genel veri işleme hükümlerinin yanı sıra özel hükümlere tabi tutulmuş ve bu bağlamda daha sıkı ve hassas düzenlemeye gidilmiştir.

Ayrıca, kişisel verilerin ülke sınırları dışından da erişilebilir duruma gelmesi, dünya ticaretini yeni boyutlara taşımıştır. Müşteri ve ürün profili, pazarlama, araştırma, geliştirme gibi faaliyetlere kolayca erişim, uluslararası şirketler açısından olumlu sonuçlar doğurduğu gibi, verilerin kontrolsüzce serbest dolaşımı, söz konusu verilerin güvenliği açısından yeni tehditleri de beraberinde getirmiştir. Fakat tahmin edilebileceği üzere, devletlerin sırf vatandaşlarının verilerini korumaya yönelik tehlikeleri bertaraf etmek amacıyla veri akışlarını tamamen engellemesi olağan değildir. Zira bu, ülkelerarası ticari ilişkilerinin felç olması ve hâliyle ekonominin de ciddi ölçüde zarar görmesi anlamına gelecektir⁸. Veri akışının hiçbir kısıtlama olmadan gerçekleşmesi ise kişilerin temel hak ve özgürlükleri açısından ciddi endişe yaratmaktadır. Zira verilerin kolayca paylaşılabılır hâle gelmesi, verileri elinde bulunduran kişilerle bu verilerin ilgili oldukları kişiler arasında menfaat dengesini veri sahipleri aleyhine bozmuştur. Şöyle ki, bu verilere erişimin kolaylaşması ile veri sahipleri maddi ve manevi zarar görmeye başlamış ve menfaatlerinin korunması ihtiyacı doğmuştur⁹. Bu anlamda dengeyi sağlayabilmek adına en iyi çözüm, veri koruma düzeyinin aktarılan verileri takip etmesini temin etmektir. Başka bir deyişle, kişisel verilerin aktarılacağı yerde de asgari olarak bir önceki düzeyde korunması sağlanmalıdır.

⁶ Bkz.: a.ş., Birinci Bölüm, “Türk Hukukundaki Düzenlemeler” başlığı.

⁷ Christopher Kuner, “Reality and Illusion in EU Data Transfer Regulation Post Schrems”, **German Law Journal**, C. 18, S. 4, 2017, s. 882; Çiğdem Ayözger Öngün, **Kişisel Verilerin Korunması Hukuku Elektronik Haberleşme Sektörüne İlişkin Özel Düzenlemeler Dahil**, 2. bs., İstanbul, Beta Basım, 2019, s. 1.

⁸ Işıl Çelik, **Kişisel Verilerin Yurt Dışına Aktarılması: 6698 Sayılı Kişisel Verilerin Korunması Kanunu ve 2016/679 Sayılı Avrupa Birliği Genel Veri Koruma Tüzüğü Kapsamında**, İstanbul, On İki Levha, 2022, s. 4.

⁹ Ayözger Öngün, a.y.

Bu noktada veri koruma mevzuatları devreye girmektedir. Veri koruma yasalarının amacı, veri aktarımlarını engellemek değil, veri aktarımlarının kişilerin temel hak ve özgürlüklerine zarar vermeyecek şekilde gerçekleştirilmesini sağlamaktır¹⁰. Bu hususta hassas tutumuyla bilinen Avrupa Birliği (AB) düzenlemelerinde de, AB mevzuatını örnek alarak Kişisel Verilerin Korunması Kanunu’nu kabul eden Türkiye’de de bu yaklaşım benimsenmiş ve aktarımdan sonra da AB’de veya Türkiye’de sağlanan asgari korumanın sürdürülebilmesi hedeflenmiştir. Buna uygun olarak, veri aktarımı mekanizmaları bu hedefe hizmet edecek şekilde düzenlenmiştir.

Üç bölümden oluşan çalışmamızın birinci bölümünde temel kavramlara ve konuyla ilgili hukuki düzenlemelere yer verilmiştir. Öncelikle; kişisel veri, kişisel veri kavramının tanımı, unsurları, özel nitelikli kişisel verilere genel olarak değinilmiştir. Devamında ise kişisel verilerin aktarılması kavramına dair doktrinde ve hukuki düzenlemelerde yer alan tanımlara, aktarılma kavramının kapsamı dışında kalan verilerin transit geçişine yer verilmiştir. Bölümün sonunda ise veri aktarımına ilişkin hükümler içeren ilk düzenlemeler, konuyla ilgili OECD, BM, AK ve AB çerçevesinde mevcut düzenlemeler ve onların tarihsel gelişimi, Türk mevzuatında kişisel verilerin aktarılmasına ilişkin hükümler içeren kanun ve yönetmelikler kısaca özetlenmiştir.

İkinci bölümde kişisel veri aktarımlarına ilişkin AB düzenlemeleri incelenmiştir. Öncelikle, AB sınırları dâhilinde verilerin serbest akışı ve buna dair dikkat edilmesi gereken hususlardan bahsedilmiştir. Bölümün geri kalan kısmında ise verilerin Birlik dışına aktarılmasına ilişkin GDPR’da öngörülen hukuki araçlar irdelenmiştir. Bu çerçevede öncelikle, bir yeterlilik kararının mevcut olduğu durumlarda yapılan aktarımlar, yeterlilik kararlarının özellikleri, söz konusu kararların kabul edilmesi sırasında dikkate alınması gereken hususlar, devamında bu kararların bulunmadığı durumlar için öngörülen uygun güvenlik önlemleri, bu önlemlerin birbirinden farkı, avantaj ve dezavantajları, akabinde hem yeterlilik

¹⁰ Oğulcan Özkan, **Kişisel Verilerin Korunması**, Ankara, Yetkin, 2020, s. 131; Nadin Sertçe, “Avrupa Birliği Genel Veri Koruma Tüzüğü (GDPR) Kapsamında AB Dışına Kişisel Veri Aktarımı”, Yüksek Lisans Tezi, İstanbul Bilgi Üniversitesi, 2022, s. 2.

kararının hem de uygun güvenlik önlemlerinin bulunmadığı durumlarda kişisel veri aktarımlarına izin verilen istisnai hâller ele alınmıştır. Bölümün sonunda ise, uluslararası anlaşmalara dayanarak kişisel verilerin Birlik dışına aktarılmasına yönelik hususlara yer verilmiştir.

Çalışmanın üçüncü ve son bölümünde ise, kişisel verilerin aktarılmasına dair Türk hukukundaki mevcut düzenlemeler incelenmiştir. Bu kapsamda öncelikle kişisel verilerin aktarılmasına dair KVKK'da yer alan hükümlere genel olarak değinilmiş ve aktarıma ilişkin temel ilkeler hakkında kısaca bilgi verilmiştir. Devamında ise kişisel verilerin Türkiye Cumhuriyeti sınırları içerisinde aktarımı, aktarım için aranan açık rızanın niteliğine dair hususlar ve aktarımı gerçekleştirmek için açık rızanın aranmadığı durumlar, genel ve özel nitelikli kişisel veriler açısından ayrı ayrı açıklanmıştır. Devamında, yeterli korumanın bulunduğu ve bulunmadığı durumlarda yurt dışına yapılan aktarımlara yer verilmiş, bu kapsamda Kişisel Verileri Koruma Kurulu (Kurul) tarafından kabul edilen taahhütname örnekleri ve henüz Türk hukuku açısından yeni olan bağlayıcı şirket kuralları değerlendirilmiştir. Daha sonra, yurt dışına yapılan aktarımlara tek başına uygulanıp uygulanamayacağı tartışma konusu olan AK'nin 108 sayılı Sözleşmesi ayrı bir başlık altında ve veri aktarımı açısından ele alınmıştır. Bölümün sonunda, kişisel verilerin aktarılmasına ilişkin Türk ve AB hukukunda mevcut olan yaklaşımlar kıyaslanmıştır.

BİRİNCİ BÖLÜM

TEMEL KAVRAMLAR VE TARİHSEL GELİŞİM

I. Kişisel Veri

A. Tanımı

Kişisel verilerin aktarılması faaliyeti kapsamında hangi tür verilerin değerlendirileceğini netleştirmek için öncelikle kişisel veri kavramının açıklanması faydalı olacaktır. Kişisel veri kavramı, teknolojiye gözlemlenen gelişmeler sonucu geçtiğimiz yıllarda hukuk dünyasında yer almış yeni bir kavramdır¹¹. Konuyla ilgili uluslararası ve ulusal düzenlemelerde benzer, hatta neredeyse aynı tanım kullanılmıştır. Şöyle ki, bu konuya ilişkin kabul edilmiş ilk uluslararası belge olan ve 23 Temmuz 1980 yılında OECD tarafından yayınlanan “Kişisel Verilerin Gizliliğinin ve Sınır Ötesi Akışlarının Korunması Hakkında Rehber İlkeler”¹² 1/b maddesinde kişisel veriler “*belirli veya belirlenebilir bir kişiye ilişkin tüm bilgiler*” olarak tanımlanmıştır. 108 sayılı Sözleşme’nin 2/a maddesinde ise kişisel veri, kimliği belirli veya belirlenebilir bir gerçek kişi hakkındaki tüm bilgiler olarak tanımlanmıştır.

Yürürlükten kalkmış olan 95/46/EC sayılı ve 24 Ekim 1995 tarihli “Kişisel Verilerin İşlenmesi ve Bu Tür Verilerin Serbest Dolaşımına Dair Bireylerin Korunması Hakkında” AB Konseyi Yönergesi (95/46/EC sayılı DPD) 2/a maddesinde öngörülen düzenleme ile kişisel veriler, “*belirli veya belirlenebilir bir gerçek kişi hakkındaki tüm bilgiler*” şeklinde tanımlanmıştır. Belirlenebilir kişi kavramı da aynı maddede “*doğrudan ve dolaylı olarak özellikle bir kimlik numarası veya kişinin fiziksel, psikolojik, ruhsal, ekonomik, kültürel veya sosyal kimliğine bir veya birden fazla spesifik faktör referans alınarak, kimliği belirlenebilen kişi*” olarak

¹¹ Elif Küzeci, **Kişisel Verilerin Korunması**, 4. bs., İstanbul, On İki Levha, 2020, s. 19-20; İbrahim Korkmaz, **Kişisel Verilerin Ceza Hukuku Kapsamında Korunması**, 2. bs., Ankara, Seçkin, 2019, s. 25.

¹² OECD, “Guidelines on the Protection of Privacy and Transborder Flows of Personal Data”, 23.09.2013, (çevrimiçi), <https://www.oecd-ilibrary.org/docserver/9789264196391-en.pdf?expires=1663051799&id=id&accname=guest&checksum=b4e43bfe7d1d64dc9d11abb4c3a470f6>, 27.12.2021, (OECD, Guidelines).

tanımlanmıştır. Bu Yönerge’yi yürürlükten kaldıran 2016/679 sayılı “AB Genel Veri Koruma Tüzüğü” (GDPR) 4. maddesinde de aynı tanım devam ettirilmiştir.

Ulusal mevzuatta kişisel veri kavramı tanımlanırken kanun koyucu, KVKK’da bütün uluslararası düzenlemelerde öngörülen tanımın nerdeyse aynısını kullanmıştır. Buna göre, “*kişisel veri: kimliği belirli veya belirlenebilir gerçek kişiye ilişkin her türlü bilgiyi*” ifade eder (KVKK m.3/f.1/d). Tanımlardan da anlaşıldığı üzere, kişisel veriler tahdidi olarak belirlenmemiştir. Kanun koyucu, böylesine geniş bir tanım kullanarak kişisel veri kapsamını mümkün olduğunca geniş tutmayı hedeflemektedir¹³. Belli bir kimsenin kimliği, etnik kökeni, fiziksel özellikleri, sağlık durumu, öğrenim veya istihdam durumuna ilişkin bilgilerin yanı sıra, bir kişinin bireysel ve aile içi yaşantısına ilişkin ve başkaları ile gerçekleştirilen haberleşmelerden ibaret bilgiler de kişisel veri olarak değerlendirilebilir¹⁴. Bir başka deyişle kişiliğin sosyal, fiziksel, duygusal ve hatta ekonomik boyutuna ait herhangi bir bilgi kişisel veri niteliğine sahip olabilir¹⁵.

Kanundaki tanımdan hareketle, bireyin kişisel verilerinin kapsama alanına, “*gerçek kişinin kişisel veya maddi ilişkileri hakkındaki tüm bilgilerin*” dâhil olduğunu söylemek mümkündür¹⁶. Bireyin kişisel ilişkilerine ilişkin veriler; bireyin kimliğini ortaya çıkaran (örneğin kişinin adı, soyadı, adresi, doğum tarihi, medeni durumu, mesleği, sağlık durumu, görüşleri vs.), bir kişiyi belirli kılan, onu karakterize eden verileridir¹⁷. Bireyin maddi ilişkilerine ilişkin verilere ise üçüncü kişilerle olan sözleşmesel ilişkiler, kişinin taşınmazıyla ilgili ilişkileri vs. örnek olarak gösterilebilir. Örneğin, bir otomobil plakası ile gerçek kişinin kimliğini

¹³ Şehriban İpek Aşıkoğlu, **Avrupa Birliği ve Türk Hukukunda Kişisel Verilerin Korunması ve Büyük Veri**, İstanbul, On İki Levha, 2018, s. 5.

¹⁴ Ayözger Öngün, s. 9; Hüseyin Can Aksoy, **Medeni Hukuk ve Özellikle Kişilik Hakkı Yönünden Kişisel Verilerin Korunması**, Ankara, Çakmak Yayınevi, 2010, s. 1; Aşıkoğlu, **Kişisel Veriler**, s. 5-6; Özkan, s. 9.

¹⁵ Nilgün Başalp, **Kişisel Verilerin Korunması ve Saklanması**, Ankara, Yetkin, 2004, s. 22; Erarslan, **Özel Nitelikli Kişisel Veriler**, s. 17.

¹⁶ Oğuz Şimşek, **Anayasa Hukukunda Kişisel Verilerin Korunması**, İstanbul, Beta Basım, 2008, s. 120.

¹⁷ Şimşek, s. 121.

belirleyebilmek mümkün ise, otomobil plakası da kişisel veri olarak kabul edilecektir¹⁸.

B. Unsurları

Bir verinin kişisel veri olarak değerlendirilip değerlendirilmeyeceği, kanun ve uluslararası düzenlemelerle aranan unsurların veride bulunup bulunmamasına göre belirlenir. KVKK uyarınca kişisel verilerin unsurları, uluslararası düzenlemelerle benzer şekilde belirlendiği üzere;

- bir bilginin var olması,
- belirli veya belirlenebilir bir kişinin olması,
- bilginin kişiyle ilişkili olması olarak ifade edilebilir.

1. Bilgi

Bilgi, “işlemden kullanılan uzlaşım kurallarından yararlanarak kişinin veriye yönelttiği anlam” şeklinde tanımlanmaktadır. Veri ise “olgu, kavram ya da komutların, iletişim, yorum ve işlem için elverişli biçimsel ve uzlaşım bir gösterimi” olarak tanımlanmaktadır¹⁹. Her iki tanımdan hareketle, verinin işlenmemiş bilgiyi ifade ettiği söylenilebilir²⁰. Bir başka deyişle, alıcısı tarafından kolaylıkla anlaşılabilmesi için işlenmiş veri, bilgiyi ifade etmektedir²¹. Görüldüğü üzere, bilgi daha dar kapsamlıdır ve sadece veriye yöneltilen anlamı ifade etmektedir. Yani veri, bilgi için gerekli hammaddeyi oluşturmaktadır²².

Kanun koyucu tarafından kişisel veri kavramının tanımında yer alan “bilgi” unsuruna ilişkin herhangi bir sınırlandırma öngörülmemiş, aksine oldukça geniş kapsam ifade eden “her türlü bilgi” ifadesine yer verilmiştir. Bu bağlamda, kişinin özel hayatı ve aile yaşamına ilişkin bilgiler kişisel veri niteliği taşıdığı gibi, bu kişinin iş ilişkileri, ekonomik ve sosyal yaşamına dair bilgiler de kişisel veri olarak

¹⁸ Şimşek, a.y.

¹⁹ Türk Dil Kurumu, (çevrimiçi), <https://sozluk.gov.tr/?kelime=>, 27.12.2019.

²⁰ Aydın Akgül, “Kişisel Verilerin Korunması Açısından İdarenin Hukuki Sorumluluğu ve Yargısal Denetimi”, Doktora Tezi, Kocaeli Üniversitesi, 2013, s. 10.

²¹ Küzeci, s. 10.

²² Ayözger Öngün, s. 8; Murat Volkan Dülger, **Kişisel Verilerin Korunması Hukuku**, 3. bs., İstanbul, Hukuk Akademisi Yayınları, 2020, s. 153; Erarslan, **Özel Nitelikli Kişisel Veriler**, s. 18.

kabul edilmektedir²³. Burada tek önemli olan husus söz konusu bilginin, kimliği belirli veya belirlenebilir bir kişiye ilişkin olmasıdır.

Bir bilginin kişisel veri olarak kabul edilebilmesi için gizli bir bilgi olmasına gerek yoktur. Şöyle ki kişinin cinsel hayatı, özel telefon konuşmaları veya yazışmalarının dökümü gibi gizli bilgiler kişisel veri olabileceği gibi, günlük hayatıyla ilgili giyimi, fiziksel özellikleri vs. gibi kamuya açık bilgileri de kişisel veri olabilecektir²⁴.

Bilginin kişisel veri olarak kabul edilip edilmemesi değerlendirilirken nesnel (objektif) veya öznel (subjektif) nitelikli olması herhangi bir önem taşımamaktadır²⁵. Bu anlamda, kişinin sağlık durumuna veya konum bilgilerine ilişkin nesnel bilgi kişisel veri olarak kabul edildiği gibi, o kişinin maddi durumu ya da karakter itibarıyla güvenilir veya güvenilirmez olduğu gibi öznel bilgiler, görüşler ve değerlendirmeler de kişisel veri niteliğini haizdir²⁶. Örneğin, bankaya kredi başvurusunda bulunan bir kişinin güvenilir olup olmadığı değerlendirilirken öznel bilgileri dikkate alınmaktadır.

Aranan diğer şartları karşılıyorsa, herhangi bir bilginin kişisel veri olarak kabul edilebilmesi için, gerçeği yansıtması koşulu da aranmayacaktır²⁷. Örneğin, kişinin iflas ettiğine dair bir bilgi, gerçek olmasa bile, söz konusu kişiye ilişkin kişisel veri olarak kabul edilecektir. Zira böyle bilgiyle karşılaşan banka, büyük bir ihtimalle kişinin kredi başvurusunu geri çevirebilir²⁸.

²³ Başalp, **Kişisel Veriler**, s. 22; Aksoy, s. 14; Erarslan, **Özel Nitelikli Kişisel Veriler**, s. 17.

²⁴ Dülger, **Kişisel Veriler**, s. 155; Hüseyin Murat Develioğlu, **6698 Sayılı Kişisel Verilerin Korunması Kanunu ile Karşılaştırmalı Olarak Avrupa Birliği Genel Veri Koruma Tüzüğü Uyarınca Kişisel Verilerin Korunması Hukuku**, İstanbul, On İki Levha, 2017, s. 37; Aksoy, s. 14; Türkay Henkoğlu, **Bilgi Güvenliği ve Kişisel Verilerin Korunması**, Ankara, Yetkin, 2015, s. 27; Korkmaz, s. 30.

²⁵ Dülger, **Kişisel Veriler**, s. 155; Develioğlu, s. 37; Korkmaz, s. 31; Aşıkoğlu, **Kişisel Veriler**, s. 8.

²⁶ Develioğlu, s. 37; Aksoy, s. 14; Furkan Güven Taştan, **Türk Sözleşme Hukukunda Kişisel Verilerin Korunması**, İstanbul, On İki Levha, 2017, s. 38; Canan İmançlı, **Kişisel Sağlık Verilerinin Korun(a)mamasından Doğan Özel Hukuk Sorumluluğu**, İstanbul, On İki Levha, 2020, s. 42.

²⁷ Article 29 Data Protection Working Party: Opinion 4/2007 on the Concept of Personal Data, 20.06.2007, s. 6, (çevrimiçi), <https://www.clinicalstudydatarequest.com/Documents/Privacy-European-guidance.pdf>, (Article 29 WP, Personal Data); Dülger, **Kişisel Veriler**, s. 156; Develioğlu, s. 37; Aksoy, s. 14; Korkmaz, s. 30; Aşıkoğlu, **Kişisel Veriler**, s. 9.

²⁸ Aksoy, s. 15; Korkmaz, s. 47; İmançlı, s. 42.

2. Belirli veya Belirlenebilir Kişi

Kisisel veri olarak kabul edilen bilginin, kimliği belirli veya belirlenebilir bir kişiye ilişkin olması gerektiğinden, gözden geçirilmesi gereken ikinci unsur, kimliği belirli veya belirlenebilir bir kişinin bulunmasıdır. Bu bağlamda, kişi kavramından ne anlaşılması gerektiği ve hangi hâllerde kimliği belirli veya belirlenebilir bir kişinin varlığından bahsedilebileceği hususları üzerinde durulması gerekmektedir.

a. Kişi

Hukuki anlamda kişi, *“haklara ve borçlara sahip olabilen varlıkları ifade etmek üzere kullanılan bir terimdir”*²⁹. Başka bir deyişle, kişi, *hak sahibi, hak süjesi* anlamına gelir. Türk hukuk düzeninde, haklara sahip ve borçlara ehil olan iki sùje mevcuttur. Bu hak sùjeleri, gerçek ve tüzel kişilerdir³⁰.

Kişisel verilerin korunması hakkı kapsamında ise “kişi” kavramı, sadece gerçek kişilerle sınırlandırılmıştır. Zira kişisel verilerin korunması hakkı ilk olarak özel hayatın korunması hakkı çerçevesinde değerlendirilmiş, zamanla bağımsız bir temel insan hakkı olarak kabul görmüştür. Özel hayat ise sadece gerçek kişilere özgü bir kavram olduğundan bu haktan faydalanacak olanlar da gerçek kişiler olmalıdır³¹.

OECD Rehber İlkeleri, 108 sayılı sözleşme ve GDPR gibi uluslararası düzenlemelerde olduğu gibi KVKK kapsamında da sadece gerçek kişilere dair bilgilerin, koruma altına alındığı hükme bağlanmış, tüzel kişilere ait bilgiler ise bu düzenlemelerle sağlanan koruma alanının dışında bırakılmıştır. Yürürlükten kalkmış olan 95/46/EC sayılı DPD’de de aynı yönde düzenlemeye gidilmekle birlikte (95/46/EC sayılı DPD giriş bölümü, par. 2), üye devletlerin veri koruma kanunlarında tüzel kişileri de kapsayacak şekilde düzenleme yapmalarına engel teşkil

²⁹ Jale Akipek/ Turgut Akıntürk/ Derya Ateş, **Türk Medeni Hukuku Başlangıç Hükümleri Kişiler Hukuku**, C. 1, 15. bs., İstanbul, Beta Basım, 2019, s. 231.

³⁰ M. Kemal Oğuzman/ Özer Seliçi/ Saibe Oktay Özdemir, **Kişiler Hukuku (Gerçek ve Tüzel Kişiler)**, 19. bs., İstanbul, Filiz Kitabevi, 2020, s. 1-7; Serap Helvacı, **Gerçek Kişiler**, 9. bs., İstanbul, Legal, 2021, s. 25-28; Bilge Öztan, **Medeni Hukukun Temel Kavramları**, 43. bs., Ankara, Turan Kitabevi, 2019, s. 221; Mustafa Dural/ Tufan Öğüz, **Kişiler Hukuku: Gerçek ve Tüzel Kişiler**, 22. bs., İstanbul, Filiz Kitabevi, 2021, s. 5-8.

³¹ Küzeci, s. 73-75; Dülger, **Kişisel Veriler**, s. 171; Develioğlu, s. 30.

edecek bir hüküm öngörülmemiştir³². GDPR’da ise tüzel kişilere dair bilgilerin işlenmesi hâlinde GDPR hükümlerinin uygulanmayacağı belirtilmiştir (GDPR Giriş bölümü, par. 14).

Şunu da belirtmek gerekir ki bu düzenlemelerle, münhasıran tüzel kişilere ilişkin veriler kastedilmektedir³³. Başka bir deyişle tüzel kişiye ait verilerle, gerçek kişiye de ulaşmak mümkünse, bu veriler de kanunla sağlanan koruma kapsamına alınacaktır³⁴. Nitekim ABAD da konuyla ilgili bir kararında aynı yönde karar vermiştir³⁵. Örneğin, bir şirkete ilişkin e-posta adresiyle gerçek kişiye ulaşılabiliriyorsa bu veri gerçek kişiye ilişkin kişisel veri olarak kabul edilmelidir³⁶. Fakat bir şirketin ticaret unvanı veya adresi gibi tüzel kişiye ilişkin olup bir gerçek kişiyle ilişkilendirilmesi imkânsız olan veriler, bu kapsama dâhil olmayacaktır³⁷.

Bu hususta açıklığa kavuşturulması gereken diğer bir husus ise, ölmüş kişilere ilişkin verilerin kişisel veri olarak kabul edilip edilemeyeceği meselesidir. Bununla ilgili GDPR’ın giriş bölümünde (par. 27) tüzüğün, ölen kişilerin kişisel verilerine uygulanmayacağı, üye devletlerin ise bu konuda düzenlemeler yapabilecekleri ifade edilmiştir. Örneğin, Fransa hukukuna göre ölen kişi henüz hayatta iken yasaklamadığı müddetçe o kişiye ilişkin veriler, tıbbi araştırmalara konu edilebilir³⁸. KVKK’da özellikle ölmüş kişilerin kişisel verilerine ilişkin düzenleme bulunmasa da Türk Medeni Kanunu³⁹ (TMK) m.28 uyarınca ölüm, kişiliği sona erdiğinden kişinin ölümünden sonra kendisine ait kişisel veriler, Kanun kapsamında değerlendirilmeyecektir⁴⁰. Şunu da belirtmek gerekir ki burada söz konusu olan,

³² Nitekim İtalya, Danimarka, Lüksemburg ve Avusturya gibi ülkeler bu kapsamda tüzel kişileri de içerecek şekilde düzenlemeler yapmıştır. Bkz.: Aksoy, s. 19; Develioğlu, s. 30; İmançlı, s. 44; Article 29 WP, **Personal Data**, s. 24.

³³ Küzeci, s. 295; Dülger, **Kişisel Veriler**, s. 171; İmançlı, s. 43.

³⁴ Başalp, **Kişisel Veriler**, s. 35; Dülger, **Kişisel Veriler**, s. 172; İmançlı, s. 45.

³⁵ ABAD, C-92/09 ve C-93/09 birleştirilmiş davaları.

³⁶ Article 29 WP, **Personal Data**, s. 23; Taştan, s. 29.

³⁷ Kişisel Verileri Koruma Kurumu, 100 Soruda Kişisel Verileri Koruma Kanunu, Ankara, KVKK Yayınları No 3, 2019, s. 17, (çevrimiçi), kvkk.gov.tr/SharedFolderServer/CMSFiles/185c2130-8070-4b2b-a91e-1d48322ca352.pdf, 30.03.2021; Dülger, **Kişisel Veriler**, s. 172.

³⁸ Aksoy, s. 21; Estonya ve Bulgaristan’da ölmüş kişilere ait kişisel verilerin de korunduğuna dair bkz.: Develioğlu, s. 32, dn. 12.

³⁹ RG: T. 08.12.2001, S. 24607.

⁴⁰ Kişisel Verileri Koruma Kurumu, 6698 Sayılı Kişisel Verilerin Korunması Kanunu Hakkında Doğru Bilinen Yanlışlar - 2, s. 18, (çevrimiçi), <http://www.kvkk.gov.tr/sharedfolderserver/cmsfiles/d077b665-66b6-4615-975a-249f93e084ba.pdf>,

münhasıran ölmüş kişiye ait kişisel verilerdir. Yani ölmüş kişiye ait bir veri, içerik olarak olmasa bile, amaç veya sonuç bakımından yaşayan bir kişiyi etkileyebiliyorsa veya başka bir kişi açısından da kişisel veri niteliğindeyse bu tür veriler veri koruma yasalarının sunduğu korumadan yararlanacaktır⁴¹. Örneğin, ölen kişinin genetik bir hastalık taşıyıcısı olduğuna dair bilgi, o kişinin çocuklarını da etkilediği için veri koruma kapsamında değerlendirilecektir⁴².

Tartışma konusu olan bir diğer husus ise cenine ilişkin verilerin, veri koruma kapsamında değerlendirilip değerlendirilmeyeceğidir. Madde 29 Çalışma Grubu⁴³ bu hususta devletlerin ilgili kanunlarına atıfta bulunulması gerektiğini ifade etmiştir⁴⁴. Türk hukukuna göre kişilik, cenin hâlindeyken henüz başlamamış olsa da, çocuk hak ehliyetini, tam ve sağ doğmak şartıyla anne rahmine düştüğü andan elde edecektir (TMK m.28/f.2). Dolayısıyla, söz konusu doğum şartlarının gerçekleşmesi itibarıyla çocuk geçmişe yönelik hak ehliyeti elde edeceğinden çocuğun kişisel verileri de, anne rahmine düştüğü andan itibaren korunmaya başlayacaktır⁴⁵.

b. Belirli veya Belirlenebilir Olma

Madde gerekçesine göre, “*bir kişinin belirli veya belirlenebilir olması, mevcut verilerin herhangi bir şekilde bir gerçek kişiyle ilişkilendirilmesi suretiyle, o kişinin tanımlanabilir hâle getirilmesini ifade eder*”⁴⁶. Kişinin kimliğinin belirli olması, o kişiyi bir grup insan arasından ayırt edilebilme, kişinin kimliğinin belirlenebilir olması ise henüz ayırt edilememiş olsa bile bu kişinin diğerlerinden ayırt edilmesinin

06.07.2021; Nafiye Yücedağ, “Medeni Hukuk Açısından Kişisel Verilerin Korunması Kanunu’nun Uygulama Alanı ve Genel Hukuka Uygunluk Sebepleri”, **İstanbul Üniversitesi Hukuk Fakültesi Mecmuası**, C. 75, S. 2, 2017, s. 766; Develioğlu, s. 31.

⁴¹ Kişisel Verileri Koruma Kurumu, **Doğru Bilinen Yanlılar 2**, s. 24-25; Dülger, **Kişisel Veriler**, s. 172; Develioğlu, s. 32; Mesut Serdar Çekin, **Kişisel Verilerin Korunması Hukuku: Avrupa Birliği Hukukuyla Mukayeseli Olarak 6698 Sayılı Kanun Çerçevesinde**, 3. bs., İstanbul, On İki Levha, 2020, s. 41; Taştan, s. 35; Sabire Sanem Yılmaz, **Tıp Alanında Kişisel Verilerin Korunması**, 5. bs., Ankara, Seçkin, 2021, s. 55; İmançlı, s. 46.

⁴² Article 29 WP, **Personal Data**, s. 22.

⁴³ Tam adıyla Kişisel Verilerin İşlenmesi Bağlamında Bireylerin Korunması Çalışma Grubu; Komisyona veri koruma hususunda tavsiyelerde bulunmak, veri koruma politikalarının geliştirilmesinde üye ülkelere yardımcı olmak, veri koruma alanında ortaya çıkan sorunların çözümü ve güncel konularda görüş hazırlamak amacıyla bağımsız bir çalışma grubu olarak kurulmuştur. GDPR’ın yürürlüğe girmesinin ardından 2018 yılında Avrupa Veri Koruma Kurulu ile değiştirilmiştir.

⁴⁴ Article 29 WP, **Personal Data**, s. 23.

⁴⁵ Dülger, **Kişisel Veriler**, s. 172-173; Develioğlu, s. 31-32; Taştan, s. 32-33; İmançlı, s. 46-47; Özkan, s. 13-14.

⁴⁶ Bkz.: KVKK m.3 gerekçesi.

mümkün olduğu anlamına gelmektedir⁴⁷. Başka bir ifadeyle, bir veri; herhangi işleme ihtiyaç duyulmaksızın doğrudan ya da çok basit bir yolla bir kişiyle ilişkilendirilebildiği halde *belirli bir kişiye ait*, kişinin kimliğini doğrudan ortaya koymamakla birlikte, bazı ek bilgilerle kişinin kimliğini belirlenebilir kılması hâlinde ise *belirlenebilir bir kişiye ait* veri olarak kabul edilir⁴⁸. Örneğin, kimlik numarası, isim, fotoğraf gibi veriler genelde kişinin kimliğini doğrudan ortaya çıkardığı için belirli bir kişiye ait veriler olduğu halde, doğum yeri veya doğum tarihi gibi veriler ise belirlenebilir kişiye ait verilerdir. Zira bu veriler, genelde kişinin adı, soyadı vs. verileriyle birlikte değerlendirildiğinde ait olduğu kişiyle ilişkilendirilebilecektir⁴⁹.

Herhangi bir ölçütün bir kimseyi diğerlerinden ayırt edilebilir kılıp kılmayacağı, her bir somut olay açısından bütün hususlar göz önünde bulundurularak ele alınmalıdır⁵⁰. Örneğin, belli bir yaş veya soyadı bir kişiyi aynı ülkede yaşayan diğer insanlar arasında belirlenebilir kılmasa da, aynı sınıf içerisindeki diğer öğrencilerden ayırt edilebilmesini sağlayacak ve o öğrenciyi “belirli” kılacaktır.

3. Kişiye İlişkin Olma

Kişiye ilişkin olma, bilginin o kişiyle alakalı olmasını, başka bir deyişle, veriyle bağlantı kurmak suretiyle söz konusu kişiye ulaşabilmeyi ifade eder⁵¹. Gerçek bir kişiyle ilişkilendirilemeyen veriler, anonim veri olarak nitelendirilerek hem AB mevzuatı hem de KVKK tarafından kapsam dışı bırakılmıştır⁵². Şayet veriler; kişinin kimliğine, karakterine veya davranışlarına atıfta bulunuyorsa o kişiye ilişkin olarak kabul edilir⁵³. Madde 29 Çalışma Grubu’nun konuyla ilgili raporuna göre verinin kişiye ilişkin olduğunun kabul edilmesi için söz konusu verinin; içerik, amaç veya sonuç yönünden kişi ile bağlantılı olması gerekmektedir⁵⁴. Bu unsurlar alternatif

⁴⁷ Başalp, **Kişisel Veriler**, s. 33-34; Dülger, **Kişisel Veriler**, s. 157; Aşıkoğlu, **Kişisel Veriler**, s. 17.

⁴⁸ Şimşek, s. 122; Akgül, s. 12; Dülger, **Kişisel Veriler**, s. 159; Çekin, **Kişisel Verilerin Korunması**, s. 42; İmançlı, s. 46; Erarslan, **Özel Nitelikli Kişisel Veriler**, s. 20; Yılmaz, s. 54; Taştan, s. 37; Dülger, **Kişisel Veriler**, s. 159.

⁴⁹ Akgül, s. 23-24; Erarslan, **Özel Nitelikli Kişisel Veriler**, s. 21; Ayözger Öngün, s. 12; Şimşek, a.y.; İmançlı, s. 48; Dülger, **Kişisel Veriler**, s. 151, 158;

⁵⁰ Aksoy, s. 23; Dülger, **Kişisel Veriler**, s. 158; Develioğlu, s. 33-34; Yılmaz, s. 56.

⁵¹ Dülger, **Kişisel Veriler**, s. 168; Aksoy, s. 28; Yılmaz, s. 58; Korkmaz, s. 47; Taştan, s. 39.

⁵² Dülger, **Kişisel Veriler**, s. 165; Aşıkoğlu, **Kişisel Veriler**, s. 11.

⁵³ Develioğlu, s. 38; Özkan, s. 16.

⁵⁴ Article 29 WP, **Personal data**, s. 10; Develioğlu, s. 39.

niteliklidir, herhangi birinin bulunması durumunda elde edilen bilgi kişisel veri olarak kabul edilecektir⁵⁵.

“İçerik” unsurunun tespit edilmesi oldukça kolaydır. Zira bilginin kişi “hakkında” olması, o kişiye ilişkin olduğu anlamına gelir⁵⁶. Örneğin, işçinin özlük dosyasındaki bilgiler, o işçiye ilişkin olduğu gibi, bir hastanın tahlil sonuçları da, o hastaya ilişkindir. Dolayısıyla, veri içerik olarak kolay bir şekilde kişi ile ilişkilendirilebiliyorsa bu unsurun varlığı söz konusu olacaktır⁵⁷.

“Amaç” unsuru, kişinin davranış veya durumunu değerlendirme, onun hakkında karar verme, kanaate varma veya ona karşı muamelenin belirlenmesi amacıyla kullanılan veya kullanılma ihtimali olan bilginin, o kişiye ilişkin olduğunu ifade eder⁵⁸. Örneğin, bir mağazanın güvenliğini sağlamak amacıyla giriş ve çıkışlara yerleştirilen kamera görüntüleri, çalışma saatlerinde mağaza çalışanlarının davranışlarını kontrol etmek amacıyla kullanıldığı takdirde, çalışanlar açısından kişisel veri olarak kabul edilecektir.

İçerik ve amaç unsuru olmasa bile, somut olayın tüm şartları dikkate alındığında herhangi bir verinin kullanılması, bir kişinin hakları ve menfaatlerini etkileyebiliyorsa bu bilgi sonuç itibarıyla söz konusu kişiye ilişkin kabul edilir⁵⁹. Örneğin, müşteri memnuniyetini kontrol etmek amacıyla, taksilerin uydu üzerinden takibini ve müşteriye en yakın taksinin yönlendirilmesini sağlayan bir sistem, taksi sürücüsüne dair bilgi toplamak amacı taşımasa bile, bu sistemin sunduğu bilgiler, sürücülerin trafik kurallarına uyup uymadıkları ve seyir hâlinde olup olmadıklarını da ortaya çıkardığı için, sonuç itibarıyla sürücülerin menfaatini ilgilendirmekte ve kişisel veri olarak kabul edilmektedir⁶⁰.

⁵⁵ Dülger, **Kişisel Veriler**, s. 170; Çekin, **Kişisel Verilerin Korunması**, s. 45; Aksoy, s. 29; Erarslan, **Özel Nitelikli Kişisel Veriler**, s. 21; Taştan, s. 42-43; İmançlı, s. 49.

⁵⁶ Aksoy, s. 28; Article 29 WP, **Personal data**, s. 10.

⁵⁷ Dülger, **Kişisel Veriler**, s. 170; Özkan, s. 17.

⁵⁸ Article 29 WP, **Personal data**, s. 10; Dülger, **Kişisel Veriler**, s. 170; Develioğlu, s. 39; Çekin, **Kişisel Verilerin Korunması**, s. 42; Aksoy, s. 28; Korkmaz, s. 47; Taştan, s. 39.

⁵⁹ Article 29 WP, **Personal data**, s. 11; Aksoy, s. 28; Korkmaz, s. 47; Taştan, s. 40; Özkan, s. 17.

⁶⁰ Aksoy, s. 29.

II. Özel Nitelikli Kişisel Veriler

A. Tanımı

Kişisel veri türleri içerisinde kendine has nitelikleri olan ve diğer verilere nispeten daha sıkı koruma gerektiren veriler mevcuttur. Bu tür veriler taşıdıkları özel nitelikleri itibarıyla “özel nitelikli kişisel veriler” adlandırılmaktadır⁶¹. Bazı veriler açısından bu şekilde bir ayrıma gidilmesi, bu veri türlerinin daha sıkı korumaya tabi tutulması ihtiyacından kaynaklanmaktadır. Bu ihtiyacı doğuran temel gerekçe de, söz konusu verilerin işlenmesi sonucunda kişi veya kişilerin ayrımcılığa maruz kalması ve telafisi mümkün olmayan diğer durumların ortaya çıkabilmesi riskidir⁶².

Ulusal veri koruma kanunlarında özel nitelikli kişisel verilerle ilgili sabit bir kavram kullanılmamaktadır. Şöyle ki özel nitelikli kişisel verileri ifade etmek üzere; “*hassas veriler*”⁶³, “*özel kategorili kişisel veriler*”⁶⁴, “*özel kişisel veriler*”⁶⁵ ve “*özel korumaya layık veriler*”⁶⁶ gibi kavramlar da tercih edilmektedir.

KVKK’da özel nitelikli kişisel verilerle ilgili tanıma yer verilmesine de, 6. maddenin gerekçesinde “...*Bu verilerin, başkaları tarafından öğrenildiği takdirde ilgili kişinin mağdur olabilmesine veya ayrımcılığa maruz kalabilmesine neden olabilecek nitelikte veriler olmaları dikkate alınmakta, bu sebeple bu tür veriler özel nitelikli (hassas) veri olarak kabul edilmekte...*” olduğu belirtilmiştir⁶⁷. 95/46/EC sayılı DPD’nin giriş bölümü m.33’te ise özel nitelikli kişisel verilerden “*temel özgürlükleri veya kişisel mahremiyeti ihlal eden veriler*” diye bahsedilmektedir

⁶¹ Develioğlu, s. 70; Cemil Kaya, “Avrupa Birliği Veri Koruma Direktifi Ekseninde Hassas (Kişisel) Veriler ve İşlenmesi”, **İstanbul Üniversitesi Hukuk Fakültesi Mecmuası**, C. 69, S. 1-2, 2011, s. 318; Korkmaz, s. 50; Taştan, s. 41.

⁶² Başalp, **Kişisel Veriler**, s. 43; Küzeci, s. 277; Ayözger Öngün, s. 20; Akgül, s. 18; Aksoy, s. 30; Şimşek, s. 88; Korkmaz, s. 53; Erarslan, **Özel Nitelikli Kişisel Veriler**, s. 48-50.

⁶³ Örneğin, 1998 sayılı İngiliz Kişisel Verilerin Korunması Kanunu m.2, (çevrimiçi), <https://www.legislation.gov.uk/ukpga/1998/29/contents>, 13.11.2021.

⁶⁴ Örneğin, Avrupa Birliği Genel Veri Koruma Tüzüğü, m.9, (çevrimiçi), <https://eur-lex.europa.eu/eli/reg/2016/679/oj>, 13.11.2021; Avrupa Komisyonu’nun 108 sayılı Kişisel Verilerin Otomatik İşleme Tabi Tutulması Karşısında Bireylerin Korunması Sözleşmesi, m.6, (çevrimiçi), <https://rm.coe.int/1680078b37>, 13.11.2021.

⁶⁵ Örneğin, 2000 tarihli Hollanda Veri Koruma Kanunu m.16 (Bkz.: Kaya, **Hassas Veriler**, s. 318, dn. 8).

⁶⁶ Örneğin, 2000 tarihli Avusturya Federal Kişisel Verilerin Korunması ile İlgili Kanun m. 4/f.2 (Bkz.: Kaya, **Hassas Veriler**, s. 318, dn. 9).

⁶⁷ Bkz.: KVKK m.6 gerekçesi.

Her iki açıklama göz önünde bulundurulduğunda özel nitelikli kişisel veriler, bir birey hakkında temel hak ve özgürlükleriyle ilgili olarak, işlenmesi hâlinde yüksek riskler doğurabilecek veriler olup, özel bir yaklaşım ve koruma gerektiren veriler olarak tanımlanabilir⁶⁸.

B. Kapsamı

Hem KVKK'da hem de uluslararası düzenlemelerde özel nitelikli kişisel verilerin kapsamı tahdidi sayma yoluyla belirlenmiştir. Bu bağlamda, özel nitelikli kişisel veriler, her yasal düzenlemede farklı kapsama alanına sahiptir. Örneğin; 108 sayılı Sözleşme m.6'da özel nitelikli kişisel veriler olarak sadece ırksal köken, siyasi düşünceler, dini veya diğer inançlar ve sağlık veya cinsel hayatla ilgili kişisel veriler öngörüldüğü halde; 95/46/EC sayılı DPD ile bu verilerin kapsamı genişletilerek ırksal veya etnik köken, siyasi düşünceler, dini ve felsefi inançlar, sendika üyelikleri, sağlık ve cinsel yaşam ile ilgili kişisel veriler de bu kategoriye dâhil edilmiştir (m.8/f.1).

GDPR m.9'da özel nitelikli kişisel verilerin kapsamı; ırk veya etnik köken, siyasi görüşler, dini veya felsefi inançlar, sendika üyeliğine dair veriler, genetik veriler, biyometrik veriler, sağlık ve cinsel yaşamı veya cinsel eğilimine ilişkin veriler olarak belirlenmiştir. Görüldüğü üzere, GDPR'da hassas verilerin kapsamı daha da genişletilmiş, ilk kez gerçek kişinin kimliğini belirlemek amacıyla genetik ve biyometrik verilerin işlenmesi bu kapsamda değerlendirilmiştir⁶⁹. Ayrıca, 95/46/EC sayılı DPD'de yer alan "cinsel yaşam" kategorisinin yanı sıra "cinsel eğilim" de özel nitelikli kişisel veriler olarak kabul edilmiştir. Suçlar ve cezalara ilişkin veriler ise, başka bir madde ile (m.10) düzenlense de, bu veriler için de özel koruma öngörülmüştür⁷⁰.

Türk hukukunda ise özel nitelikli kişisel verilerin kapsamı oldukça geniş tutulmuştur. Şöyle ki, KVKK m.6 uyarınca *"Kişilerin ırkı, etnik kökeni, siyasi düşüncesi, felsefi inancı, dini, mezhebi veya diğer inançları, kılık ve kıyafeti, dernek,*

⁶⁸ Küzeci, s. 277; Dülger, **Kişisel Veriler**, s. 177; Henkoğlu, s. 28; Erarslan, **Özel Nitelikli Kişisel Veriler**, s. 46.

⁶⁹ Küzeci, s. 278.

⁷⁰ Küzeci, s. 279.

vakıf ya da sendika üyeliği, sağlığı, cinsel hayatı, ceza mahkûmiyeti ve güvenlik tedbirleriyle ilgili verileri ile biyometrik ve genetik verileri özel nitelikli kişisel veridir”.

Görüldüğü üzere uluslararası düzenlemelerde yer almayan dernek ve vakıf üyeliği, kılık ve kıyafet, mezhep inancı gibi veriler de bu kapsamda değerlendirilmiştir. Fakat Kanun yürürlüğe girdikten sonra, maddede geçen “...mezhebi...”, “...kılık ve kıyafeti...” ibarelerinin, uluslararası düzenlemelerde tanımlanan kişisel veri kavramlarıyla uyumlu olmadığı, uluslararası insan hakları hukuku ile bağdaşmayacak nitelikte olduğu, mezhep, kılık ve kıyafete ilişkin verilerin toplanmasının “Her Türlü Irk Ayrımcılığının Tasfiye Edilmesine Dair Uluslararası Sözleşme”de⁷¹ sağlanan güvencelere aykırı olduğu, kanun koyucunun takdir yetkisinin aşıldığı ve yerleşik fişleme tarihi tartışmalarının olduğu ülkemizde bireyler bakımından güvence değil risk oluşturduğu, toplumsal cinsiyet ayrımcılığına neden olacak nitelikte olduğundan eşitlik ilkesine aykırılık teşkil ettiği, kişinin sahip olduğu din ve vicdan özgürlüğü ile düşünce ve ifade özgürlüğünü ihlal ettiği belirtilerek, iptal edilmesi talebiyle Anayasa Mahkemesi’nde dava açılmıştır⁷².

Anayasa Mahkemesi KVKK m.6/f.1’de yer alan “...mezhebi...”, “...kılık ve kıyafeti...” ibarelerinin iptali talebiyle açılan dava hakkında verdiği kararda⁷³, dava konusu kurallarla kanun koyucunun kişilerle ilgili mezhep, kılık ve kıyafet verilerini özel kategori verilerden kabul etmek suretiyle, bu verileri diğer verilerden ayırdığı ve daha özel bir koruma altına alarak bu verilerin işlenmesini daha özel koşullara bağladığı, kuralın amacının söz konusu verilerin toplanmasına kanuni dayanak sağlamak olmadığı ve kuralın kanun koyucunun takdir yetkisi kapsamında düzenlendiği belirtilmiştir.

Özel nitelikli kişisel verilerin kapsamının zamana ve ülkeye göre değiştiği değiştiği gözlemlenmektedir. Örneğin; Polonya, İzlanda, Estonya ve Bulgaristan’da

⁷¹ United Nations, The International Convention on the Elimination of All Forms of Racial Discrimination, 21.12.1965, (çevrimiçi), <https://www.ohchr.org/sites/default/files/cerd.pdf>, 28.12.2021.

⁷² Dava dilekçesinin tam metni için bkz.: (çevrimiçi), https://www.anayasa.gov.tr/Kararlar/GenelKurul/Dava_Dilekcesi/2017-143.pdf, 27.12.2021.

⁷³ AYM Kararı, E. 2016/125, K. 2017/143, T. 28.09.2017, par. 51-58, (çevrimiçi), <http://kararlaryeni.anayasa.gov.tr>, 27.12.2019.

genetik veriler; Slovenya, Slovakya, Çek Cumhuriyeti'nde biyometrik veriler; İtalya'da dernek üyeliği; Finlandiya'da sosyal refah ihtiyaçları ve alınan yararlanmalar ile destek ve diğer sosyal refah yardımları; Danimarka, Finlandiya, Yunanistan, Hollanda, Portekiz ve Fransa'da mali veriler; İngiltere'de işlenilen ya da işlendiği iddia edilen suçlar, bu suçlara ilişkin yürütülen kovuşturmalar, bu kovuşturulmaların sonlandırılmasına ve bu kovuşturmalar sonucunda bir mahkeme tarafından verilen mahkûmiyetlere ilişkin veriler, hassas kişisel veri olarak kabul edilmiştir⁷⁴.

Doktrinde özel nitelikli kişisel verilerin hukuki metinlerde sınırlı sayıda belirlenmesine karşı çıkan görüşler de bulunmaktadır. Bu görüşler bağlamsal ve amaçsal olarak ikiye ayrılmaktadır⁷⁵. Bağlamsal görüşe göre, kişisel verilerin ayrıma tabi tutularak bir kısmının özel nitelikli kişisel veri olarak kabul edilmesi isabetli değildir. Zira bir bilginin, özel nitelikli kişisel veri olarak kabul edilebilmesi, bu verinin işlendiği ve kullanıldığı şartlara bağlıdır⁷⁶.

Özel nitelikli kişisel verilerin amaçsal olarak belirlenmesinin gerektiğini savunan görüş ise bir verinin özel nitelikli kişisel veri olup olmadığını anlamak için söz konusu verinin işleme amacına bakılması gerektiğini savunmaktadır. Burada önemli olan nokta, verilerin işlenmesi sırasında özel nitelikli bir veriyi açığa vurup vurmama amacıdır⁷⁷.

III. Kişisel Verilerin Aktarılması

A. Tanımı

Öncelikle belirtmek gerekir ki Türk ve AB hukukunda “aktarıma” kavramı farklı kapsama alanlarına sahiptir. Şöyle ki, AB hukukunda sadece üçüncü ülkelere veya uluslararası kuruluşlara yapılan kişisel veri aktarımlarını ifade eden bu kavram⁷⁸, Türk hukukunda daha geniş anlamda kullanılarak hem yurt içinde hem de

⁷⁴ Kaya, **Hassas Veriler**, s. 320; Ayözger Öngün, s. 21;

⁷⁵ Aksoy, s. 33.

⁷⁶ Aksoy, a.y.; Akgül, s. 15.

⁷⁷ Küzeci, s. 281; Aksoy, a.y.; Akgül, s. 21.

⁷⁸ Develioğlu, s. 73; Çelik, s. 36; Gloria Gonzalez Fuster, “Un-Mapping Personal Data Transfers”, **European Data Protection Review**, C. 2, S. 2, 2016, s. 167.

yurt dışına yapılan kişisel veri aktarımlarını içermektedir. Başka bir deyişle, AB hukukunda kullanılan “aktarım”, KVKK’daki “yurt dışına aktarım” kavramına tekabül etmektedir. GDPR’da AB’ye üye bir ülkedenin sınırları dâhilinde gerçekleşen veri paylaşımları için özel bir kavram kullanılmasa da, bir üye ülkeden diğerine yapılan veri paylaşımları için “sınır ötesi veri işleme” (*cross-border processing*) kavramı kullanılmaktadır⁷⁹. Bu nedenle çalışmanın bu bölümünde öncelikle kişisel verilerin aktarılması (yurt içinde), daha sonra ise spesifik olarak kişisel verilerin yurt dışına (veya Birlik dışına) aktarılması kavramını tanımlamaya çalışacağız.

Hem Türk hem de AB hukukunda kişisel verilerin aktarılması, kişisel verilerin işlenmesi faaliyetlerinden biri olarak düzenlenmiştir. Buna rağmen ne Türk ne de AB hukukunda aktarılma kavramının hukuki tanımına yer verilmiştir. Doktrinde ise aktarılma kavramına ilişkin birbirine benzer nitelikte tanımlar yer almaktadır. Örneğin, bazı görüşlere göre kişisel verilerin aktarılması, “*bir yerde mevcut sistemde bulunan verilerin başka bir sisteme nakledilmesi*”⁸⁰, “*verilerin çeşitli yöntemlerle iletilmesi*”⁸¹, “*verilerin el değiştirmesi*”⁸² veya “*bir veri sorumlusu bünyesinde bulunan kişisel verilerin başka bir veri sorumlusunun hâkimiyeti alanına girmesi*”⁸³ olarak ifade edilmiştir. Buna karşılık, daha spesifik bir tanıma göre kişisel verilerin aktarılması, “*veriyi elinde bulunduran kişi ya da kuruluşun, bunu gerçek veya sanal ortamda üçüncü kişiye transfer etmesidir*”⁸⁴.

⁷⁹ Bkz.: GDPR m.4/f.23.

⁸⁰ Süleyman Yılmaz/ Gökçe Filiz Çavuşoğlu, **Kişisel Verileri Koruma Hukuku**, Ankara, Yetkin, 2020, s. 95; Sevgi Erarslan, “Türk Hukukunda Kişisel Verilerin Yurt Dışına Aktarılması Sorunu: Açık Rıza Kapsamında Bir Değerlendirme”, **Kırıkkale Hukuk Mecmuası**, C. 1, S. 1, 2021, s. 97.

⁸¹ İmançlı, s. 163; Ezgi Hakalmaz, **Hekimlik Sözleşmesi Bağlamında Kişisel Sağlık Verilerinin İşlenmesi ve Korunması**, İstanbul, On İki Levha, 2021, s. 40; Kişisel Verileri Koruma Kurumu, 6698 sayılı Kanunda Yer Alan Temel Kavramlar, s. 17, (çevrimiçi) <https://www.kvkk.gov.tr/Icerik/4187/6698-Sayili-Kanun'da-Yer-Alan-Temel-Kavramlar>, 23.11.2021.

⁸² Ayözger Öngün, s. 199; Hakalmaz, s. 40.

⁸³ Sevgi Ünsal Özden/ İdil Uz/ Mert Karamustafaoğlu, “Kişisel Veri Aktarımı ve Bankacılık Kanunu Madde 73 Değişikliği”, **Kişisel Verileri Koruma Dergisi**, C. 3, S. 1, 2020, s. 22.

⁸⁴ Çetin Arslan, “Avrupa Birliği Hukukunda Kişisel Verilerin Üçüncü Ülkelere Aktarılması”, **Galatasaray Üniversitesi Hukuk Fakültesi Dergisi**, C. 9, S. 1, 2010, s. 463.

Diğer tanımlara nispeten daha geniş kapsamlı ve kanaatimizce daha isabetli görüşe⁸⁵ göre ise kişisel verilerin aktarılması, üçüncü kişilere yönelik her türlü veri paylaşımı olarak ifade edilmelidir. Bu anlamda veri sorumlusuyla organik bağı bulunmayan her türlü gerçek veya tüzel kişi, aktarımın yapıldığı üçüncü kişi olabilir⁸⁶.

Tanımlardan da anlaşıldığı üzere kişisel verilerin aktarılması bakımından en önemli husus, veri sorumlusunun hâkimiyetinde olan verilerin veri sorumlusu dışında kişilerin de hâkimiyeti altına geçmesidir⁸⁷. Doktrinde mevcut olan bir görüşe göre veri işleyen kişisel verileri, veri sorumlusu adına ve onun talimatları doğrultusunda işlediğinden üçüncü kişi niteliğini haiz değildir. Dolayısıyla veri sorumlusu ile veri işleyen arasındaki veri paylaşımları da veri aktarımı olarak kabul edilmemelidir⁸⁸. Bizim de katıldığımız diğer görüşe göre ise iki veri sorumlusu arasındaki veri paylaşımları gibi, veri sorumlusu ile veri işleyen arasındaki veri paylaşımlar da veri aktarımı niteliği taşımaktadır⁸⁹. Nitekim Kişisel Verileri Koruma Kurumu'nun (Kurum) yayınladığı rehberlerde de aynı yönde açıklamalar yapılmıştır⁹⁰. Örneğin, şirket çalışanlarının maaşlarının ödenmesi için çalışanlara ait verilerin (isim, soy isim, kimlik numarası, hesap bilgileri vs.) veri sorumlusu tarafından bankaya gönderilmesi faaliyeti, çalışanlarına dair veriler açısından veri sorumlusu olan şirket ile bu faaliyet çerçevesinde veri işleyen banka arasında gerçekleşen veri aktarımıdır.

Şunu da belirtmek gerekir ki tüzel kişiliğe sahip olan veri sorumlusunun, kendi içinde farklı birimler veya kişiler arasında gerçekleştirdiği veri akışları, veri

⁸⁵ Dülger, **Kişisel Veriler**, s. 244; Bahri Öztürk/ Elif Altınok Çalışkan/ Serkan Seyhan, **Kişisel Verilerin Korunması Hukuku: Teorik ve Pratik Çalışma Kitabı**, Seçkin, 2021, s. 79.

⁸⁶ Dülger, **Kişisel Veriler**, s. 244, 432.

⁸⁷ Dülger, **Kişisel Veriler**, s. 432.

⁸⁸ Çekin, **Kişisel Verilerin Korunması**, s. 121-124.

⁸⁹ Dülger, **Kişisel Veriler**, s. 432; Ayözger Öngün, s. 199; Esra Tepe, **Kişisel Verilerin Korunması: Özel Hukuk Açısından Avrupa İnsan Hakları Mahkemesi İçtihatları Işığında**, Ankara, Adalet, 2021, s. 69; İmançlı, s. 163; Ünsal Özden/ Uz/ Karamustafaoğlu, s. 22; Hakalmaz, s. 40.

⁹⁰ Dülger, **Kişisel Veriler**, s. 244, 433; Çekin, **Kişisel Verilerin Korunması**, s. 121, 123; Kişisel Verileri Koruma Kurumu, Kişisel Verilerin Korunması Kanunu Hakkında Sıkça Sorulan Sorular, Ankara, KVKK Yayınları, 2019, s. 77, (çevrimiçi), <https://www.kvkk.gov.tr/Icerik/4196/Kisisel-Verilerin-Korunmasi-Kanunu-Hakkinda-Sikca-Sorulan-Sorular>, 20.11.2021; Kişisel Verileri Koruma Kurumu, Kişisel Verilerin Korunması Kanununa İlişkin Uygulama Rehberi, Ankara, KVKK Yayınları No 1, s. 90, (çevrimiçi), <https://www.kvkk.gov.tr/sharedfolderserver/cmsfiles/41784a70-2bac-4e4a-830f-35c628468646.pdf>, 20.11.2021.

aktarımı olarak kabul edilmemektedir⁹¹. Zira bu durumda veri alıcıları, üçüncü kişi sıfatına sahip değildir. Başka bir deyişle, şirketin kendi çalışanları ve birimleri veri işleyen olarak kabul edilmemektedir. Kurum da bir şirketin çalışanlarının veya alt birimlerinin, veri işleyen olmadığı ve veri işleyen, mutlaka veri sorumlusunun bünyesi dışında bulunması gerektiğinin altını çizmiştir⁹². Bu tür kurum dâhilî paylaşımlar, ikincil işleme faaliyeti olarak adlandırılmaktadır. İkincil işleme faaliyetleri, ilk işleme amacı ile sınırlı kalmalıdır⁹³. Örneğin, bir şirketten ürün sipariş edildiğinde sipariş edilen ürünü müşteriye ulaştırmak için şirketin pazarlama departmanının, müşterinin kişisel verilerini şirket içinde birkaç farklı birime (siparişin teslimata hazır duruma getirilmesi için operasyon birimine, fatura işlemleri için muhasebe birimine vs.) iletmesi, aktarım değil ikincil işleme faaliyetidir⁹⁴. Bunun aksine siparişin, müşterinin adresine teslim edilmesi için müşteri bilgilerinin bir kargo şirketine iletilmesi ise kişisel verilerin aktarılması faaliyeti olarak kabul edilmelidir. Zira kargo şirketi, veri sorumlusu şirketten bağımsız tüzel kişiliğe sahiptir. Şunu da belirtmek gerekir ki ikincil işlemler, ilk amaçla uyumlu olduğundan müşterinin rızasının tekrardan alınması gerekmemektedir. Fakat yukarıdaki örnekte söz konusu verilerin, müşteriye reklam mesajları göndermek için yeniden işleneceği takdirde ise, ilk amaçla bağlılık bulunmadığından bu işlem için yeniden müşterinin rızası alınmalıdır⁹⁵.

Kişisel verilerin yurt dışına aktarılmasının tanımlanması, yurt içine yapılan aktarımlarla kıyaslandığında daha fazla önem arz etmektedir. Zira kişisel veriler bulunduğu ülkeden başka bir ülkeye aktarıldığı zaman, aktarıldıkları ülkede yeterli

⁹¹ Dülger, **Kişisel Veriler**, s. 432; Halil Altındağ, **Kişisel Verileri Koruma Kurulu Tarafından Verilen İdari Para Cezaları**, Ankara, Adalet, 2021, s. 116; Göknil Özcan, **Bankacılık İş ve İşlemlerinde Kişisel Verilerin Korunması**, İstanbul, On İki Leva Yayıncılık, 2020, s. 115; İmançlı, s. 164; Ünsal Özden/ Uz/ Karamustafaoğlu, s. 22; Hakalamaz, s. 41; Kişisel Verileri Koruma Kurumu, **Sıkça Sorulan Sorular**, s. 78; Kişisel Verileri Koruma Kurumu, **Uygulama Rehberi**, s. 90.

⁹² Bkz. Kişisel Verileri Koruma Kurumu, 6698 Sayılı Kişisel Verilerin Korunması Kanunu Hakkında Doğru Bilinen Yanlışlar, KVKK Yayınları No: 31, Ankara, 2020, s. 21, (çevrimiçi), <https://kvkk.gov.tr/SharedFolderServer/CMSFiles/ca752cda-c3df-4645-8d5e-e2a507e63200.pdf>, 25.04.2021.

⁹³ Dülger, **Kişisel Veriler**, s. 432.

⁹⁴ Dülger, **Kişisel Veriler**, a.y.

⁹⁵ Dülger, **Kişisel Veriler**, a.y.

korumaya tabi tutulup tutulmayacağı endişesi gündeme gelmektedir⁹⁶. Bu nedenle hem ulusal hem de uluslararası mevzuatta kişisel verilerin yurt dışına aktarılması özel düzenlemelere tabi tutulmuştur. Maalesef hem Türk hem AB hukukunda kişisel verilerin yurt dışına aktarılmasına dair yasal bir tanım bulunmadığı gibi, doktrinde de üzerinde mutabakat sağlanan bir tanım bulunmamaktadır.

Avrupa Veri Koruma Denetmeni (EDPS)⁹⁷, henüz 95/46/EC sayılı DPD yürürlükte iken, 7 Mart 2012 tarihinde yayınlanan veri koruma reform paketinde kişisel verilerin aktarılması kavramının tanımlanması gerektiğini belirtmiştir. Ayrıca, kişisel verilerin aktarılması ve erişilebilir hâle getirilmesi sanal ağ ortamında teorik bir mesele olsa da, bu iki kavram iki farklı sonuca sebep olduğu için, aktarılma kavramının neleri kapsayıp kapsamadığının net bir şekilde düzenlenmesi gerektiğine özellikle vurgu yapmıştır⁹⁸.

EDPS'nin 2014 yılında yayınlanan görüşünde kişisel verilerin aktarılması kavramının, sadece 95/46/EC sayılı DPD ve GDPR'da değil, aynı zamanda birkaç AB düzenlemesinde⁹⁹ daha tanımlanmadan yer aldığını ve dolayısıyla kanun koyucunun bu kavramı doğal anlamında, yani “*verilerin farklı kullanıcılar arasında hareketi*” olarak kullandığının varsayılması gerektiği belirtilmiştir¹⁰⁰. Benzer şekilde

⁹⁶ Julian Wagner, “The Transfer of Personal Data to Third Countries under the GDPR: When Does a Recipient Country Provide an Adequate Level of Protection?”, **International Data Privacy Law**, C. 8, S. 4, 2018, s. 231-230; Lokke Moerel, **Binding Corporate Rules: Corporate Self-Regulation of Global Data Transfers**, Oxford University Press, 2012, s. 28; Dülger, **Kişisel Veriler**, s. 437; Çekin, **Kişisel Verilerin Korunması**, s. 114.

⁹⁷ Birincil amacı, kişisel verilerin işlenmesi zamanı AB kurumlarının kişisel verilerin korunması ve mahremiyet hakkına uyumlu davranmasını sağlamak ve gözlemlemekten ibaret olan bağımsız bir denetim kurumu.

⁹⁸ European Data Protection Supervisor, Opinion of the European Data Protection Supervisor on the Data Protection Reform Package, 07.03.2012, (çevrimiçi), https://edps.europa.eu/sites/default/files/publication/12-03-07_edps_reform_package_en.pdf, 25.01.2021, par. 108, s. 18.

⁹⁹ Bkz.: 45/2001/EC sayılı “Topluluk Kurum ve Organları tarafından Kişisel Verilerin İşlenmesi ve Verilerin Serbest Dolaşımı bakımından Bireylerin Korunması” Yönergesi, (çevrimiçi), <https://eur-lex.europa.eu/legal-content/en/txt/pdf/?uri=celex:32001r0045&from=en>, 20.01.2021; 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” Yönerge, (çevrimiçi), <https://eur-lex.europa.eu/legal-content/en/txt/pdf/?uri=celex:32016l0680&from=en>, 20.01.2021.

¹⁰⁰ European Data Protection Supervisor, The Transfer of Personal Data to Third Countries and International Organisations by EU Institutions and Bodies, 14.07.2014, (çevrimiçi), https://edps.europa.eu/sites/edp/files/publication/14-07-14_transfer_third_countries_en.pdf, 25.01.2021, s. 6.

doktrinde de kişisel verilerin yurt dışına aktarılmasına ilişkin; “*geniş anlamda verilerin, ülkeler arasında elektronik hareketi*”¹⁰¹, “*verilerin, bir yerden veya kişiden diğer yer veya kişiye iletilmesi*”¹⁰², “*işlenebilir verilerin her türlü hareket veya iletilmesi*”¹⁰³ gibi tanımlara yer verilmiştir. Fakat aktarım eyleminin belirlenmesi uygulamada her zaman bu kadar basit değildir. Zira bazı görüşlere göre, veri aktarımının gerçekleşmesi için verilerin ülke sınırlarını terk etmesi yeterli iken, karşı görüşe göre verilerin sadece ülke sınırlarının dışına çıkması yeterli olmayıp buna ek olarak verilerin bir takım işlemlere tabi tutulması gerekir. Ayrıca, internetin ortaya çıkmasıyla birlikte veriler, bir noktadan diğerine hareket etmeden de yurt dışında bulunan üçüncü kişiler tarafından erişilebilir duruma gelmiştir. Bu durumun veri aktarımı olarak değerlendirilip değerlendirilmemesi hususu doktrinde bu konuyla ilgili en çok tartışılan hususlardan biridir.

EDPS’ye göre kişisel verilerin aktarılması kavramı ile “*...Tüzük’e tabi bir gönderici tarafından, alıcının/ alıcıların erişime sahip olacağı bilgisi veya niyetiyle gerçekleştirilen kişisel verilerin iletilmesi, ifşa edilmesi veya başka bir şekilde kullanıma sunulması*” kastedilmektedir¹⁰⁴. Bu tanıma göre, veri aktarımları hem kasıtlı aktarımları (*deliberate transfers*) hem de izin verilen erişimleri (*permitted access*) ifade etmektedir¹⁰⁵.

GDPR yürürlüğe girmeden önce, Avrupa Parlamentosu’nun Sivil Özgürlükler, Adalet ve İçişleri Baş Komitesi’nin, GDPR konusunda yetkili raportörü Jan-Philippe Albrecht’in hazırladığı taslak raporda ilk kez kişisel verilerin aktarılması kavramının tanımına da yer verilmiştir. Buna göre, “*kışisel verilerin aktarılması, veri aktaranın, alıcıya verilere erişim izni verme niyeti ve bilgisi dâhilinde, sınırlı sayıda belirlenmiş taraflara aktif olarak erişilebilir hâle getirilen*

¹⁰¹ William L. Fishman, “Introduction to Transborder Data Flows”, **Stanford Journal of International Law**, S. 16, 1980, s. 1.

¹⁰² ICO, The eighth data protection principle and international data transfers (çevrimiçi), https://www.colleaga.org/sites/default/files/attachments/international_transfers_legal_guidance.pdf, 25.10.2021.

¹⁰³ Chris Amery, “The European Union Data Protection Directive – Where are we? How did we get here? What next?”, **Information on Security Technical Report**, C. 2, S. 1, 1997, s. 35.

¹⁰⁴ EDPS, **The Transfer of Personal Data**, s. 7; Sertçe, s. 7.

¹⁰⁵ EDPS, **The Transfer of Personal Data**, a.y.

her türlü kişisel veri nakli” olarak tanımlanmıştır¹⁰⁶. Maalesef bu tanım GDPR’ın Parlamento’ya sunulan nihai metninden çıkarılmış ve bu şekilde kabul edilmiştir. Böylece 95/46/EC sayılı DPD’deki boşluk devam ettirilmiştir.

Türk hukukundaki mevcut yaklaşıma göre, kişisel verilerin yurt dışına aktarılmış olarak kabul edilmesi için aranan tek şart, alıcının yurt dışında bulunması veya yurt dışı tabanlı sunucu kullanılmasıdır¹⁰⁷. Kurul’un, bu hususta aldığı bir kararda¹⁰⁸ *“Google firmasına ait G-mail e-posta hizmeti altyapısının kullanılması durumunda gönderilen ve alınan e-postaların dünyanın çeşitli yerlerinde bulunan veri merkezlerinde tutulması söz konusu olacağından, böyle bir durumda kişisel verilerin yurt dışına aktarılmış olacağı...”* belirtilmiştir. AB hukukunda ise bunun aksine, verilerin Birlik sınırlarını terk etmesi, Birlik dışına veri aktarımı için tek başına yeterli değildir. Bunun için yurt dışında bulunan verilerin bir takım işlemlere tabi tutulması gerekmektedir¹⁰⁹. Nitekim GDPR m.44’de de genel aktarım ilkesi düzenlenirken her türlü veri aktarımları değil, özellikle *“üçüncü bir ülkeye veya uluslararası bir kuruluşa aktarılmasının ardından işlenen veya işlenmesi amaçlanan kişisel veri aktarımları”* ifadesine yer verilmiştir.

Tartışmalara sebep olan diğer husus ise, verilerin yurt dışında bulunan kişilerin erişimine açık hâle getirilmesinin, yurt dışına aktarım olarak değerlendirilip değerlendirilmeyeceğidir. Bu hususla ilgili Türk hukukunda özel bir hüküm bulunmasa da doktrinde verilere yurt dışından erişimin, aktarım olarak değerlendirilmesi gerektiği ifade edilmiştir¹¹⁰. AB hukukunda ise konuyla ilgili özel bir düzenleme bulunmamakla birlikte, ABAD’ın incelemesine konu olan bir olayda

¹⁰⁶ European Parliament Committee on Civil Liberties, Justice and Home Affairs, Draft Report on the proposal for a regulation of the European Parliament and of the Council on the protection of individual with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation), 16.01.2013, (çevrimiçi), https://www.europarl.europa.eu/doceo/document/A-7-2013-0402_EN.html, 27.01.2021, s. 65.

¹⁰⁷ Dülger, **Kişisel Veriler**, s. 437.

¹⁰⁸ Bkz.: Kişisel Verileri Koruma Kurulu, 31/05/2019 Tarihli ve 2019/157 sayılı Karar, (çevrimiçi), <https://www.kvkk.gov.tr/Icerik/5493/2019-157>, 02.09.2021.

¹⁰⁹ Develioğlu, s. 73.

¹¹⁰ Dülger, **Kişisel Veriler**, s. 245.

mahkeme, erişime açık olan bir internet sitesine veri yüklemenin, yurt dışına veri aktarımı anlamına gelmeyeceğine hükmetmiştir¹¹¹.

Söz konusu olayda, kilise gönüllüsü olan Bayan Lindqvist, web sitesi oluşturarak meslektaşlarının isimlerini, işlerini, hobilerini, aile koşullarını ve telefon numaralarını açıklayan bilgileri bu internet sitesine yüklemiştir. Hatta meslektaşlarından birinin ayağını incittiği için, bir süreliğine yarı zamanlı olarak çalıştığına dair sağlık bilgilerine bile yer vermiştir. Fakat bu bilgileri paylaşırken ne meslektaşlarının rızasını almış ne de İsveç Veri Koruma Kurumu’nu bilgilendirmiştir¹¹². Bazı çalışanların bu bilgilerin paylaşılması durumundan memnun kalmaması üzerine söz konusu bilgileri internet sayfasından kaldırsa da Bayan Lindqvist, İsveç veri koruma hükümlerini ihlal ettiği için yargılanmış ve para cezasına çarptırılmıştır. Karar temyiz edilmiş ve İsveç mahkemesi, cevaplanması gereken bazı soruları ABAD’a yöneltmiştir¹¹³.

Sorulardan birinde Mahkemeden; internet sayfasına kişisel veriler yüklenmesi ve böylece bu verilerin üçüncü bir ülkede bulunan insanlar dâhil internete bağlanan herkesin erişimine açık hâle getirilmesi durumunda üçüncü bir ülkeye herhangi bir veri aktarımı gerçekleşip gerçekleşmediğinin yanıtlanması, ayrıca üçüncü ülkeden hiçbir kişi fiilen veriye erişmemiş veya söz konusu sunucu gerçekten fiziksel olarak üçüncü ülkede olsa dahi bu soruya yanıtın yine aynı olup olmayacağının cevaplanması istenmiştir¹¹⁴.

Bu dava çerçevesinde aktarım kavramının nasıl yorumlanması gerektiğine dair ABAD’a farklı yaklaşımlar sunulmuştur. Avrupa Komisyonu ve İsveç hükümeti, üçüncü ülke vatandaşlarının erişebildiği internet sitelerine kişisel veri yüklemenin, herhangi bir üçüncü ülke kullanıcısının verilere gerçekten erişip erişmediğine

¹¹¹ Bkz.: ABAD, C-101/01, 06.11.2003, (çevrimiçi), <https://eur-lex.europa.eu/legal-content/en/txt/pdf/?uri=celex:62001cj0101&from=en>, 16.02.2021.

¹¹² Nilgün Başalp, “Kişisel Verilerinin İnternette Açıklanması Üzerine Bir Avrupa Topluluğu Adalet Divanı Kararı: Kişisel Verilerin ve Özellikle Sağlık Verilerin İnternette Açıklanması 95/46 sayılı Yönergenin Uygulama Alanına Girer Mi?”, **Bilişim ve Hukuk Dergisi**, C. 1, S. 10, 2009, s. 19-20.

¹¹³ Başalp, **ABAD Kararı**, s. 20.

¹¹⁴ Þorgerður Jóhanna Sveinbjarnardóttir, “The Concept of “Transfer” of Data under European Data Protection Law: In the Context of Transborder Data Flows”, Master Thesis, University of Oslo, 2015, s. 19-20.

bakılmaksızın kişisel verilerin aktarılması olarak kabul edilmesi gerektiği yönünde görüş beyan etmiştir¹¹⁵. Bunun aksine, Hollanda hükümeti kişisel verilerin aktarılmasının, bir üye devletten üçüncü bir devlete “kasıtlı olarak” (*intentionally*) aktarılma eylemini ifade ettiği için, kişisel verilerin internet sayfasına yüklenmesinin veya herhangi başka bir şekilde üçüncü taraflar için erişilebilir duruma getirilmesinin kişisel veri aktarımı teşkil etmeyeceğini ifade etmiştir¹¹⁶. Birleşik Krallık hükümeti ise 95/46/EC sayılı DPD’nin 25. maddesinin, kişisel verilere üçüncü ülkelerden erişebilirlikle ilgili değil, aktarılma ile ilgili olduğunu ve aktarımın, kişisel verilerin bir yerden veya kişiden başka yere iletilmesi anlamına geldiğini belirtmiştir¹¹⁷.

ABAD, bu olayla ilgili Komisyon’un ve İsveç’in görüşünün aksine bir karar vermiş ve bir internet sayfasına kişisel verilerin yerleştirilmesini, bu verilerin üçüncü ülkelere aktarılması olarak nitelendirilemeyeceğine hükmetmiştir¹¹⁸. Mahkeme, kararını gerekçelendirirken öncelikle olayın teknik yönüne dikkat çekmiştir. Şöyle ki ABAD’a göre, Bayan Lindqvist’in verileri yüklediği internet sayfaları bu verileri, bu sayfalara bilerek erişmeyi istemeyen (erişim niyeti olmayan) kişilere otomatik olarak göndermek için teknik araçlar içermemekteydi. Söz konusu verilere erişmek için internet kullanıcısının, sadece internete bağlanması yeterli olmayıp, aynı zamanda bu sayfalara bakmak için kişisel olarak gerekli eylemlerde (internet girmek, web siteyi bulmak, gerekli sayfayı aratmak vs.) bulunmak zorunda kalacaktır¹¹⁹. Mahkemenin bu gerekçesi doktrinde eleştirilere sebep olmuştur. Svantesson’a göre, internete bağlı olmayan veya Lindqvist’in internet sayfasını ziyaret etmek için gerekli adımları atmak istemeyen kullanıcıya bu verilerin aktarılmamış olmasını düşünmek, televizyonunu açmayan veya televizyonun özellikle bir kanalını seçmeyen birine, TV istasyonunun TV programları sağlamadığını düşünmekten farksızdır¹²⁰.

Ayrıca, bir kişi tarafından internet sitesine yüklenen ve üçüncü ülkedeki bir kişinin bilgisayarında görüntülenen kişisel verilerin, bu iki kişi arasında *doğrudan*

¹¹⁵ ABAD, C-101/01, par. 53.

¹¹⁶ ABAD, C-101/01, par. 54.

¹¹⁷ ABAD, C-101/01, par. 55.

¹¹⁸ ABAD, C-101/01, par. 71.

¹¹⁹ ABAD, C-101/01, par. 60.

¹²⁰ Dan Jerker B. Svantesson, “Privacy, The Internet and Transborder Data Flows an Australian Perspective”, **Masaryk University Journal of Law and Technology**, C. 4, S. 1, 2010, s. 15.

aktarılmamış olduğu, sayfanın saklandığı yer sağlayıcının bilgisayar altyapısı yoluyla aktarıldığı belirtilmiştir¹²¹. Şöyle ki, 1990'lı yıllarda internette bir sayfanın yayınlanması için öncelikle sayfanın yazarının, bu sayfayı oluşturan verileri yer sağlayıcıya iletmesi gerekmektedir. İnternete bağlanarak bu verilere erişmek isteyen kullanıcılara ise söz konusu veriler, yer sağlayıcının bilgisayar altyapısı yoluyla aktarılmaktaydı¹²². Bundan hareketle, mahkeme verileri yükleyen ve bu verilere erişecek olan kullanıcılar arasında doğrudan bir aktarım gerçekleşmeyeceğini ifade etmiştir.

Mahkemenin en zayıf gerekçesi ise, Yönerge'nin veri aktarımlarını düzenleyen 25. maddesinin internetle ilgili hükümler içermemesidir¹²³. Fakat şunu belirtmek gerekir ki Yönerge'de internete ilişkin hükümlere özel olarak yer verilmemesinin sebebi, Yönerge'nin teknolojik araçlardan bağımsız bir dille yazılmış olmasıdır. Başka bir deyişle, söz konusu hükümler zaten herhangi bir teknolojiye bağlı kalmaksızın uygulanmaktaydı¹²⁴.

ABAD son gerekçesinde, yasal düzenlemelerden daha çok, hukuki sonuçlara odaklanmıştır¹²⁵. Şöyle ki ABAD'a göre, internete veri yükleme, üçüncü ülkelere aktarım olarak değerlendirileceği takdirde, internete erişim için ihtiyaç duyulan teknik araçların bulunduğu tüm üçüncü ülkelere aktarım anlamına gelecekti. Dolayısıyla, 95/46/EC sayılı DPD'de öngörülen veri aktarımlarına ilişkin özel rejim, internetteki işlemlere ilişkin olarak bir genel uygulama rejimi hâline gelecekti¹²⁶. Başka bir deyişle, internet üzerinden gerçekleştirilen bütün işlemlerin, kişisel veri aktarımlarıyla ilgili sınırlamalara tabi tutulması gerekecekti¹²⁷.

Kanaatimizce, ABAD'ın bu hususta vermiş olduğu karar sadece somut dava bağlamında değerlendirilmeli ve farklı özelliklere sahip davalar açısından doğrudan

¹²¹ ABAD, C-101/01, par. 61.

¹²² ABAD, C-101/01, par. 59.

¹²³ ABAD, C-101/01, par. 67.

¹²⁴ Svantesson, **Data Flows**, s. 15.

¹²⁵ Christopher Kuner, **Transborder Data Flows and Data Privacy Law**, Oxford, Oxford University Press, 2013, s. 12; Svantesson, **Data Flows**, s. 16.

¹²⁶ ABAD, C-101/01, par. 69.

¹²⁷ Kuner, **Data Flows**, s. 12; Paul Van den Bulck, "Transfers of Personal Data to Third Countries", **ERA Forum**, C. 18, S. 2, 2017, s. 230.

uygulanmamalıdır. Zira mahkeme, bu sonuca somut olayın koşullarını dikkate alarak ve yukarıdaki gerekçeler ışığında varmıştır¹²⁸. Başka bir deyişle, mahkemenin sunduğu gerekçeleri dikkate alarak internet sayfasına veri yükleme eyleminin ne zaman üçüncü ülkelere veri aktarımı olarak değerlendirilmesi gerektiği belirlenebilir.

İnternet sitesine veri yüklemenin, yurt dışına veri aktarımı olarak kabul edilmesi için öncelikle bu eylem, verileri yükleyen kişi tarafından kasıtlı olarak gerçekleştirilmiş olmalıdır (par. 62). Verilerin bir internet sitesine aktarım niyeti olmadan (kasıtlı olmayarak) yüklendiği durumlarda ise doğrudan bir aktarımın gerçekleşip gerçekleşmediği hususu araştırılmalıdır (par. 59, 61). Başka bir deyişle, ABAD kişisel verilerin yalnızca pasif bir eylem ile üçüncü ülkede bulunan kullanıcılar tarafından erişilebilir duruma getirilmesini yeterli bulmayarak, veri aktaranın söz konusu verileri veri alıcısına (internet kullanıcılarına) doğrudan göndermiş olmasını, veri alıcılarının da bu verilere ulaşmak için aktif eylemlerde bulunması gerektiğini ifade etmiştir¹²⁹. Kuner'e göre ise, internete veri yükleme sadece ticari amaçlarla ve büyük çapta gerçekleştirildiğinde üçüncü bir ülkeye aktarım olarak kabul edilmelidir. Hâlbuki Bayan Lindqvist'in internet sayfasına yüklediği veriler, ticari amaç taşımadığı gibi sadece bir üye devlette bulunan küçük bir grubu (kilise çalışanlarını) ilgilendirmekteydi¹³⁰.

Mahkemeye yöneltilen sorunun ikinci kısmıyla ilgili olarak ABAD, üçüncü bir ülkedeki alıcının verilere gerçekten erişip erişmediğinin veya yer sağlayıcının üçüncü bir ülkede bulunup bulunmamasının araştırılmasını gereksiz bulmuştur. Kanaatimizce, ABAD böyle bir görüş sunarken verilerin üçüncü ülkelere aktarılması açısından, yer sağlayıcının nerede bulunduğu veya verilere gerçekten erişilip erişilmediğinin değil, veri yükleyenin niyetinin belirleyici nitelikte olduğunu kastetmiştir.

¹²⁸ EDPS, **The Transfer of Personal Data**, s. 7.

¹²⁹ Sveinbjarnardóttir, s. 25; Sertçe, s. 7; Çelik, s. 77.

¹³⁰ Christopher Kuner, **European Data Protection Law: Corporate Compliance and Regulation**, 2. bs., Oxford University Press, 2007, s. 82-83.

B. Kişisel Verilerin Transit Geçişi

Doktrinde kişisel verilerin aktarılması kavramının yanı sıra, verilerin transit geçişi kavramı da karşımıza çıkmaktadır. AB hukukundaki genel yaklaşıma göre, verilerin transit geçişi, aktarılma olarak değerlendirilmemeli ve dolayısıyla, aktarılmaya ilişkin kısıtlamalardan muaf tutulmalıdır¹³¹.

Verilerin transiti, internet üzerinden gerçekleştirilen veri paylaşımlarının yaygınlaşması ile birlikte gündeme gelmiştir. Zira internet üzerinden iletilen verilerin özelliği, nihai varış noktalarına ulaştığında yeniden birleşmek üzere, genelde birkaç parçaya veya paketlere ayrılarak muhtemelen farklı ülkelerden geçen yollar kullanmak suretiyle alıcıya ulaşmasıdır¹³². Bir noktadan diğerine ulaşmak için veri paketleri tarafından kullanılacak olan yollar, İnternet dolaşım protokollerine (*routing protocols*) bağlı olarak belirlendiğinden, veri paketlerinin dolaşımının hangi ülke üzerinden gerçekleşeceği gönderenin kontrolünde değildir¹³³. AB veri koruma otoriteleri kişisel verilerin, aktarıldığı adrese ulaşmadan önce geçici süreliğine fiziksel olarak yurt dışında bulunduğu bu süreyi, kişisel verilerin transit geçişi olarak kabul etmektedir.

Kişisel verilerin yurt dışında bulunduğu sürenin “sadece transit geçiş” (*mere transit*) olarak kabul edilmesi için bu süre zarfında herhangi işleme tabi tutulmamış olması gerekmektedir¹³⁴. Verinin kaynağı ve nihai hedefi aynı ülke olsa dahi, üçüncü bir ülkede bulunduğu sırada, verilere herhangi bir müdahalede bulunulursa transit geçiş değil, aktarım söz konusu olacaktır. Bu nedenle, herhangi bir AB ülkesinden yola çıkan kişisel verilerin, üçüncü bir ülkeden geçmiş olması, söz konusu kişisel veriler üzerinde önemli bir işlem yapılmadığı sürece, kişisel verilerin aktarılması olarak nitelendirilmez¹³⁵. Aktarılma eylemi ile, kişisel verilerin kasıtlı olarak

¹³¹ Sveinbjarnardóttir, s. 49.

¹³² Stewart Room, **Data Protection and Compliance in Context**, Edinburgh, British Informatics Society Limited, 2007, s. 153; W. Kuan Hon, **Data Localization Laws and Policy: The EU Data Protection International Transfers Restriction Through a Cloud Computing Lens**, Massachusetts, Edward Elgar Publishing, 2017, s. 74.

¹³³ Hon, s. 74; Sveinbjarnardóttir, s. 50.

¹³⁴ Room, s. 153; Kuner, **European Data Protection**, s. 156.

¹³⁵ Eduardo Ustaran, “International Data Transfers”, **Data Protection: A Practical Guide to UK and EU Law** içinde, Ed.: Peter Carey, 5.bs., Oxford, Oxford University Press, 2018, s. 108; Arslan, s. 465-466; Bilgi Information Technology Law Institute, **Kişisel Verilerin Korunmasına İlişkin**

aktarılabacağı ülkede konumlandırılması amaçlansa da transit geçiş, verilerin transit ülkesinde konumlandırılmasına değil, sadece geçişine hizmet eder¹³⁶.

Transit kavramı kişisel verilerin aktarılması kapsamına dâhil edilmediği takdirde, kişisel verilerin nasıl korunacağı sorusu ortaya çıkmaktadır. Belirtildiği üzere, transitin amacı verileri işlemek veya üçüncü ülkelerdeki kişiler için erişilebilir hâle getirmek olmadığından, kendi başına veriler için herhangi bir risk oluşturmaz¹³⁷. Daha önce de belirtildiği üzere, verilerin korunmasını gerektiren herhangi bir riskten bahsedebilmek için transit durumdaki veriler üzerinde bir takım işleme faaliyeti söz konusu olmalıdır.

Bu bulgular ışığında, kişisel verilerin transit geçişinin, aktarılma kavramına dâhil edilmemesi daha isabetli olacaktır. Ayrıca, aktarılan veriler yönlendiriciler aracılığı ile paketler veya parçalar hâlinde otomatik olarak farklı yollarla hedef bilgisayara ulaştırıldığından veri sorumlusunun, internet üzerinden paylaşılan verilerin rotasını kesin olarak önceden belirleyebilmesi pratik olarak mümkün değildir¹³⁸. Bu yüzden verilerin transit geçişinin bir aktarım faaliyeti olarak kabul edileceği takdirde, veri sorumluları veri işleme faaliyeti sırasında farkında olmadan yasadışı aktarım gerçekleştirmiş olacaktır¹³⁹.

Yukarıda da belirtildiği üzere, Türk hukukunda kişisel veriler ülke sınırlarının dışına çıktığı an aktarılmış olarak kabul edildiği için, bu kavram Türk hukukunda kabul görmemektedir¹⁴⁰.

Düzenlemeler Çerçevesinde Uluslararası Veri Aktarımı: Yeni Gelişmeler ve Uygulamaya İlişkin Hukuki Değerlendirmeler, 06.03.2020, "CoE 108+ and the GDPR: A Modernised Look and Nexus at Protecting Personal Data Worldwide" Konferansı, s. 72, (çevrimiçi), https://itlaw.bilgi.edu.tr/media/2020/3/30/Final%20Veri_Aktarimi_Raporu_30.03.2020.pdf, 25.05.2021; Sertçe, s. 8-9.

¹³⁶ Cemil Kaya, **Assessing the Transfer of Personal Data in the European Union in the Light of the Data Protection Directive**, İstanbul, On İki Levha, 2011, s. 17.

¹³⁷ Kuner, **Data Flows**, s. 175; Sveinbjarnardóttir, s. 49.

¹³⁸ Hon, s. 75; Sveinbjarnardóttir, s. 50.

¹³⁹ Hon, a.y.

¹⁴⁰ Dülger, **Kişisel Veriler**, s. 438.

C. Kişisel Verilerin Aktarılmasına Dair Hukuki Düzenlemeler

1. İlk Düzenlemeler

Bilgi teknolojileri ve veri işlemedeki gelişmeler nedeniyle, veri koruma düzenlemelerine duyulan ihtiyaç 60'lı ve 70'li yıllarda ortaya çıkmıştır¹⁴¹. İlk veri koruma kanunu olarak bilinen 1970 yılında Almanya'nın Hessen federal eyaletinde kabul edilen kanun, kişisel verilerin aktarılmasına yönelik hiçbir hüküm içermemekteydi¹⁴². Veri aktarımlarıyla ilgili hükümler içeren ilk ulusal kanun 1973 yılında İsveç'te kabul edilmiştir. Bu kanuna göre, İsveç'ten yurt dışına yapılan aktarımlar, İsveç Veri Koruma Kurumundan alınan izne tabi tutulmuştur¹⁴³. Bundan sonra Avusturya, Finlandiya, Fransa, İrlanda, ve Lüksemburg gibi Avrupa ülkelerinde de, yurt dışına yapılan veri aktarımları üzerinde kısıtlamalar içeren veri koruma yasaları çıkarılmıştır¹⁴⁴.

Avrupa ülkelerinin ilk veri koruma kanunlarının her biri, yurt dışına veri aktarımını farklı şekilde kategorize etmiş ve farklı düzenlemelere tabi tutmuştur. Örneğin; Avusturya, Norveç ve İsveç'te verilerin yurt dışına aktarılması için aktarmadan önce veri koruma kurumu tarafından açık bir yetkilendirme; İrlanda'da AK 108 sayılı Sözleşmenin 12. maddesinin aynen kabul edilmesi; Finlandiya'da ya veri sahibinin rızasının alınması ya da verilerin aktarıldığı ülkede eşit düzeyde koruma mekanizmasının mevcut olması şartı aranmaktaydı¹⁴⁵. Fakat şunu da belirtmek gerekir ki bu hükümlere rağmen bahsi geçen kanunlarda kişisel verilerin yurt dışına aktarılması bir kural olarak değil, istisna olarak düzenlenmiştir¹⁴⁶.

¹⁴¹ Fuster, s. 162; Baran Kızıllırmak, "Cross-Border Transfer of Personal Data under GDPR Regime and Turkish Legal Framework", Master Thesis, University of Hamburg, 2020, s. 13.

¹⁴² Rolf H. Weber, "Transborder Data Transfers: Concepts, Regulatory Approaches and New Legislative Initiatives", **International Data Privacy Law**, C. 3, S. 2, 2013, s. 119; Kaya, **Transfer of Personal Data**, s. 3; Hon, s. 28.

¹⁴³ Wagner, s. 319; Dan Jerker B. Svantesson, "The Regulation of Cross-Border Data Flow", **International Data Privacy Law**, C. 1, S. 3, 2011, s. 180; Ian J. Lloyd, **Information Technology Law**, 6. bs., New York, Oxford University Press, 2011, s. 183.

¹⁴⁴ Christopher Kuner, "Regulation of Transborder Data Flows under Data Protection and Privacy Law: Past, Present, and Future", **OECD Digital Economy Papers**, s. 187, 2010, s. 14; Kuner, **Data Flows**, s. 26.

¹⁴⁵ Hon, s. 29.

¹⁴⁶ Kuner, **Privacy Law**, s. 14.

İlk ulusal veri koruma yasalarının ortaya çıkmasından bir müddet sonra, verilerin ülke sınırlarından öteye aktarıldığı durumlarda sorun yaşanmaması için ulusal düzenlemelerin uyumlaştırılması ihtiyacı ortaya çıkmıştır. Bu doğrultuda 1980’li yılların başından itibaren kişisel verilerin korunması bağlamında yeni bir dönemin başladığı söylenebilir. Çünkü bu yıllardan itibaren OECD, AK, BM gibi uluslararası kuruluşlar çerçevesinde kişisel verilerin korunmasına ilişkin temel ilkeler ve sınır ötesi veri aktarımlarını düzenleyen metinler kabul edilmiştir¹⁴⁷.

2. OECD Düzenlemeleri

Kişisel verilerin uluslararası düzeyde korunmasına dair ilk düzenleme OECD tarafından 1980 yılında kabul edilen “*Özel Yaşamın Gizliliğinin ve Sınır Ötesi Kişisel Veri Dolaşımının Korunmasına İlişkin Rehber İlkeler*”dir. Üye ülkeler açısından bağlayıcılığı bulunmayan tavsiye nitelikli bu ilkelerin temel amacı, ulusal veri koruma mevzuatlarını uyumlu hâle getirmekten ibarettir¹⁴⁸. İlkelerin en önemli yanı, kişisel verilerin yurt dışına aktarılmasına özel olarak yer verilmiş olmasıdır¹⁴⁹. Şöyle ki, bu ilkelere göre üye ülkeler, transit geçişler de dâhil olmak üzere kişisel verilerin diğer üye ülkelere aktarılmasının kesintisiz ve güvenli olmasını sağlamak için tüm makul ve uygun önlemleri almalıdır (madde 16). Bununla birlikte, İlkeler’de üye ülkelerin, kişisel veri aktarımlarına sınırlamalar getirilebileceği durumlar da öngörülmüştür. Bu gibi durumlara kişisel verilerin aktarılacağı ülkenin İlkeler’e önemli ölçüde uyum sağlamaması, aktarılan verilerin yeniden başka bir ülkeye aktarılmasının, ulusal gizlilik mevzuatının ihlali ile sonuçlanması ve belli kategoriden olan özel korumaya tabi tutulmuş kişisel verilerin aktarılacağı ülkede eşit düzeyde korunmaması dâhil edilmiştir (madde 17).

Ekonomik bir topluluk olan OECD, bahsi geçen düzenlemede kişisel verileri de ekonomik açıdan değerlendirmiş ve kişisel verilerin sınır ötesine aktarılmasının sosyal ve ekonomik gelişmeye katkı sağlayacağı ve kişilerin özel hayatlarının

¹⁴⁷ Küzeci, s. 131; Kaya, **Transfer of Personal Data**, s. 7.

¹⁴⁸ Başalp, **Kişisel Veriler**, s. 24; Küzeci, s. 129; Akgül, s. 114; Aksoy, s. 4. Akgül, s. 114; Aksoy, s.

4.

¹⁴⁹ Taştan, s. 10.

gizliliğine ilişkin ulusal düzenlemelerin bu sınır ötesi aktarımları aksatabileceği ifade edilmiştir¹⁵⁰.

OECD Rehber İlkeleri bağlayıcı nitelik taşımamasına ve kişisel verilerden ziyade ekonomik verilerin aktarılmasına odaklanmış olmasına rağmen, bu hususta kabul edilen ilk uluslararası düzenleme olduğundan bir çok ülkede (örneğin; Japonya, Avustralya, Yeni Zelanda, Hong Kong)¹⁵¹ kişisel verilerin korunması mevzuatının kabul edilmesinde etkili payı olmuştur¹⁵².

3. Avrupa Konseyi Düzenlemeleri

AK çerçevesinde kişisel verileri korunmasına ilişkin 1970’li yıllarda başlayan çalışmalar 28 Ocak 1981 tarihinde 108 sayılı “*Kişisel Verilerin Otomatik İşleme Tabi Tutulması Karşısında Bireylerin Korunması Sözleşmesi*”nin imzaya açılması ve 1 Ekim 1985 tarihinde yürürlüğe girmesiyle sonuçlanmıştır¹⁵³. Sözleşme’nin en önemli özelliği, OECD ve BM Rehber İlkelerinden farklı olarak bağlayıcı nitelikli olmasıdır¹⁵⁴. Ayrıca Sözleşme, AK’ya üye olmayan ülkelerin imzasına da açık olduğu için farklı bölgeler arasında veri korumasını da sağlamaya hizmet eder¹⁵⁵. Türkiye, bu Sözleşmeyi 02.05.2016 tarihi itibarıyla iç hukuka aktarmış ve 01.09.2016 tarihi itibarıyla de yürürlüğe koymuştur. AK’ya üye olmayan ülkelere; Arjantin, Uruguay, Senegal, Yeşil Burun Adaları, Tunus, Fas, Mauritius, Meksika, Rusya¹⁵⁶ Sözleşme’yi onaylamış, Japonya ve Güney Kore ise gözlemci olarak katılmıştır¹⁵⁷.

¹⁵⁰ Aksoy, s. 5.

¹⁵¹ Michael Erbschloe/ John Vacca **Net Privacy (A Guide to Developing and Implementing an Ironclad Ebusiness Privacy Plan)**, Mc-Graw Hill, s. 30’dan aktaran Küzeci, s. 131.

¹⁵² Frits W. Hondius, “A Decade of International Data Protection”, **Netherlands International Law Review**, C. 30, S. 2, 1983, s. 106; Küzeci, s. 130-131; Yılmaz, s. 121.

¹⁵³ İmançlı, s. 15; Bilgi Information Technology Law Institute, s. 91.

¹⁵⁴ Lee Andrew Bygrave, **Data Protection Law, (Approaching Its Rationale, Logic and Limits)**, The Hague, Kluwer Law International, 2002, s. 32; Mehmet Bedii Kaya, “Kişisel Verilerin İşlenmesi ve Korunması Arasında Denge”, **Güncel Gelişmeler Işığında Kişisel Verilerin Korunması Hukuku** içinde, Ed.: Leyla Keser Berber, Ali Cem Bilgili, İstanbul, On İki Levha, 2019, s. 36.

¹⁵⁵ Aksoy, s. 5; Küzeci, s. 144.

¹⁵⁶ Rusya Federasyonu, 108 sayılı Sözleşme’yi imzaladığı 07.11.2001 tarihinde AK üyesi olsa da, 2022 yılında Ukrayna üzerine gerçekleştirdiği saldırı nedeniyle 42 üye ülkenin oyçokluğuyla üyeliğinin askıya alınmasına tepki olarak, 15 Mart 2022 tarihinde AK’dan çekildiğini duyurmuştur. AK Bakanlar Komitesi, 23 Mart 2022 yılında kabul ettiği kararında Rusya Federasyonu’nun, üye olmayan ülkelerin imzasına açık olan sözleşmelere taraf olarak kalabileceğini ifade etmiştir. (Bkz.: The Committee of Ministers, Resolution CM/Res(2022)3 on legal and financial consequences of the

Bu Sözleşme ile, sözleşmeye taraf olan ülkeler arasında kişisel verilerin serbest dolaşımı öngörülmüş ve böylece, üye ülkeler arasında kişisel verilerin bütünleştirici ve güvenli olarak kullanımını öngören bir yaklaşım benimsenmiştir¹⁵⁸. Taraf olan ülkeler arasında verilerin serbest dolaşımına bazı istisnalar da getirilmiştir. Bunlardan ilki, taraf devletlerin iç hukukunun, belli kişisel veri kategorileri veya otomatik işleme tabi tutulmuş kişisel veri dosyaları için özel bir koruma getirmiş olması ve aktarım yapılacak olan diğer devlette eşdeğer bir korumanın bulunmamasıdır (m.12/f.3/a). Bir diğer istisna ise Sözleşme'ye taraf olan ülkelere birinin, diğer ülkenin iç hukukundaki boşluktan yararlanarak Sözleşme'ye taraf olmayan bir ülkeye yaptığı aktarımı engellemekten ibarettir (m.12/f.3/b).

2001 yılında Sözleşme'nin 181 sayılı Ek Protokolü¹⁵⁹ de kabul edilmiştir. Türkiye, bu protokolü 11.07.2016 tarihinde iç hukuka aktarmış ve 01.11.2016 tarihinde de yürürlüğe koymuştur. Ek protokol ile kişisel verilerin taraf olmayan devletlere aktarılmasına ilişkin hükümler geliştirilmiştir¹⁶⁰. Buna göre, Sözleşmeye taraf olmayan ülke veya kurumların yetki alanına tabi olan alıcıya veri aktarımları, bu ülke veya kurumların yeterli düzeyde koruma sağlaması durumunda gerçekleştirilebilecektir (m.2/f.1). Yeterli düzeyde koruma, sözleşmeye taraf olmayan ülke veya kurum tarafından sağlanmadığı durumlarda kişisel veri aktarımları; ilgili kişinin özel bir menfaati veya özel menfaati aşan üstün hukuki yarar (örneğin, kamu yararı) nedeniyle iç hukukun izin verdiği durumlarda (m.2/f.2/a) veya veri sorumlusu tarafından sağlanan ve ilgili otorite tarafından yeterli bulunan koruma tedbirlerinin bulunması (m.2/f.2/b) hâlinde gerçekleştirilebilecektir.

cessation of membership of the Russian Federation in the Council of Europe, 23.03.2022, (çevrimiçi), https://search.coe.int/cm/pages/result_details.aspx?objectid=0900001680a5ee2f, 25.04.2022; European Data Protection Board, Statement 02/2022 on Personal Data Transfers to the Russian Federation, 12.07.2022, s. 1-2, (çevrimiçi), https://edpb.europa.eu/system/files/2022-07/edpb_statement_20220712_transferstorussia_en.pdf, 15.07.2022.

¹⁵⁷ Akçalı Gür, s. 853; Kaya, **Kişisel Verilerin İşlenmesi**, s. 36.

¹⁵⁸ Henkoğlu, s. 54.

¹⁵⁹ Council of Europe, 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, 08.11.2001, (çevrimiçi), <https://rm.coe.int/1680080626>, 25.02.2020.

¹⁶⁰ Lee A. Bygrave, **Data Privacy Law: An International Perspective**, New York, Oxford University Press, 2014, s. 32; Arslan, s. 460; İmançlı, s. 21.

Sözleşme'nin kabul edildiği tarihten itibaren bilişim teknolojilerinde meydana gelen gelişmelerin, insan hakları ve özellikle özel hayatın gizliliği hakkında ilgili yeni tehlikeler yaratması ve bu tehlikelere yönelik önlemler alınması amacıyla Sözleşme'nin yenilenmesi ihtiyacı ortaya çıkmıştır¹⁶¹. 108 sayılı Sözleşmenin modernize edilmesine ilişkin 108 Sayılı Sözleşme Komitesi tarafından hazırlanan teklifler, devletlerarası bir komite tarafından incelenmiş ve sonuç olarak AK Bakanlar Komitesi'ne tadil protokolü taslağı sunulmuştur¹⁶². 18 Mayıs 2018 tarihinde doktrinde Sözleşme 108+ olarak da bilinen 223 sayılı “108 sayılı Kişisel Verilerin Otomatik Olarak İşleme Tabi Tutulması Karşısında Bireylerin Korunması Sözleşmesi’ni yenileyen Protokol”¹⁶³ kabul edilmiştir. Modernizasyon sonucunda 108 sayılı Sözleşme ile GDPR arasında içerik olarak paralellik sağlanmış ve AB'nin de 108+ sayılı Sözleşme'ye taraf olabileceği kabul edilmiştir (108+ sayılı Sözleşme m.26)¹⁶⁴. Modernize edilmiş Sözleşme 10 Ekim 2018 tarihinde imzaya açılrsa da Türkiye tarafından imzalanmadığı gibi bu yönde yapılan herhangi bir çalışma da bulunmamaktadır¹⁶⁵.

Sözleşme 108+ ile taraf devletlerin, münhasıran kişisel verinin korunması amacıyla taraf devletlerle yapılan kişisel veri aktarımlarını özel izne tabi tutamayacağı ve yasaklayamayacağı hükme bağlanmıştır. Fakat taraf devletlerden birinin diğerine veya taraf olmayan bir devlete veri aktarımı gerçekleştirmesi, Sözleşme hükümlerinin uygulanamamasına gerçek ve ciddi bir risk oluşturduğunda veya bölgesel bir uluslararası organizasyona mensup ülkeler tarafından kabul edilen uyumlaştırılmış koruma kurallarına tabi olması hâlinde bu taraf, aktarımı yasaklayabilir veya özel izne tabi tutabilir (m.14).

¹⁶¹ Dülger, **Kişisel Veriler**, s. 92; Sezen Kama Işık, **Avrupa Veri Koruma Hukukuna Anayasal Bir Bakış: 2016/679 sayılı GVKT (GDPR) ile 6698 sayılı KVKK'nın Detaylı Analiz ve Karşılaştırılması** ile, İstanbul, On İki Levha, 2020, s. 80; Sevede Pelen, “AB’de Kişisel Verilerin Üçüncü Ülke ve Uluslararası Kuruluşlara Aktarılması”, **Bahçeşehir Üniversitesi Hukuk Fakültesi Dergisi**, C. 16, S. 205, 2021, s. 1733.

¹⁶² Bilgi Information Technology Law Institute, s. 112.

¹⁶³ Council of Europe, Protocol amending the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, 10.10.2018, (çevrimiçi), <https://rm.coe.int/16808ac918>, 21.11.2021.

¹⁶⁴ Bilgi Information Technology Law Institute, s. 114.

¹⁶⁵ Dülger, **Kişisel Veriler**, s. 92; Kaya, **Kişisel Verilerin İşlenmesi**, s. 36; Yılmaz, s. 133; İmançlı, s. 21; Pelen, s. 1733.

Sözleşmeye taraf olmayan devletlere yapılacak kişisel veri aktarımlarında aranan eşdeğer koruma düzeyinin temin edilmesi şartı Sözleşme 108+'de de devam etmektedir. Böyle bir koruma; uluslararası sözleşmeler dâhil olmak üzere, ilgili ülkenin iç hukuku veyahut ad hoc (özel) veya onaylanmış standart güvencelerle temin edilebilir (m.14/f.3). Düzenlemede bu güvenceler bulunmasa dahi veri aktarımlarının gerçekleştirilebileceği durumlara da yer verilmiştir. Buna göre; ilgili kişinin açık, belirli ve özgür rızasını vermesi, ilgili kişinin belirli menfaatlerinin gerektirmesi, üstün meşru menfaatin kanunda öngörülmesi, demokratik toplumun ifade özgürlüğü açısından orantılı ve gerekli olması durumlarında da taraf olmayan devlete veri aktarımı yapılabilir (m.14/f.4). Ayrıca bu düzenleme ile veri koruma otoriteleri, kişisel verilerin yurt dışında aktarımlarını ilgili kişilerin temel hak ve özgürlüklerini korumak amacıyla yasaklayabilir, askıya alabilir veya şarta bağlayabilirler (m.14/f.6).

4. Birleşmiş Milletler Düzenlemeleri

BM insan hakları belgelerinde yer verilen düzenlemelerin yanı sıra, Örgüt'ün özel hayatın gizliliği hakkında bağımsız olarak, doğrudan kişisel verilerin korunmasına yönelik girişimleri de mevcuttur¹⁶⁶. Bunlardan en önemlisi 14 Aralık 1990 tarihinde Birleşmiş Milletler Genel Kurulu tarafından kabul edilen *“Bilgisayarla İşlenen Kişisel Veri Dosyalarına İlişkin Rehber İlkeler”*dir¹⁶⁷. Rehber İlkeler'e göre, iki veya daha fazla ülkenin sınır ötesi veri akışıyla ilgili mevzuatı, gizliliğin korunması açısından karşılaştırılabilir güvenceler içeriyorsa, veriler bu ülkelerde serbestçe dolaşabilmelidir. Söz konusu İlkeler'in kabul edilmesinden bu yana, BM sınır ötesi veri akışının düzenlenmesi konusunda çok aktif olmamıştır. Çünkü bu ilkelerin hukuki bağlayıcılığı yoktur ve sadece tavsiye niteliklidir¹⁶⁸. Bu nedenle, farklı ülkelerin ulusal veri koruma yasaları kabul edilirken, BM'den ziyade OECD, AB ve AK tarafından yayınlanan düzenlemelerden etkilenmiştir¹⁶⁹. Bu hususta BM tarafından atılan önemli adımlardan biri de 2017 yılında Uluslararası Hukuk Komisyonu'nun (ILC) uzun dönemli çalışma programına “Sınır ötesi

¹⁶⁶ Dülger, **Kişisel Veriler**, s. 90.

¹⁶⁷ United Nations, Guidelines for the Regulation of Computerized Personal Data Files, 21.07.1988, (çevrimiçi), <https://digitallibrary.un.org/record/43365>, 06.03.2021.

¹⁶⁸ Weber, s. 119.

¹⁶⁹ Kuner, **Data Flows**, s. 34.

aktarımlarda kişisel verilerin korunması” başlığının dâhil edilmesi olmuştur. Malum olduğu üzere ILC uluslararası düzeyde henüz düzenlenmemiş alanları, anlaşma taslakları hazırlayarak geliştirmeyi ve yazılı kurallara dönüştürmeyi hedeflemektedir. Bu noktadan hareketle ILC tarafından kişisel verilerin korunmasına dair bir uluslararası anlaşma hazırlanması ihtimali olduğunu söylemek mümkündür¹⁷⁰.

5. Avrupa Birliği Düzenlemeleri

AB dâhilinde kişisel verilerin akışını düzenlemek amacıyla atılan ilk adım 1973 yılında “Veri İşlemeye İlişkin Topluluk Politikası”nın yayınlanması olmuştur¹⁷¹. Bu belge daha çok konunun ekonomik yönüne odaklanmıştır¹⁷². Bu dönemde Komisyon’un beklentisi, 108 sayılı Sözleşmenin tamamlanması ve üye devletlerin bu Sözleşme’yi onaylaması yönündeydi. Fakat ülkelerin bir çoğunun Sözleşme’yi onaylamaması ve ilgili ulusal mevzuatlarının farklı olması AB dâhilinde entegrasyon ve iç pazarda kişisel verilerin aktarılmasının önünde engel oluşturmaktaydı¹⁷³. Bu nedenle Komisyon 1990 yılında bu mevzuatların uyumlu hâle getirilmesinin önemine işaret etmiş ve bu konuda bir yönerge hazırlanmasını teklif etmiştir. Yönergenin hazırlanıp kabul edilmesi beş yıl sürmüş ve 24 Aralık 1995 tarihinde “Kişisel Verilerin İşlenmesi ve Serbest Dolaşımına İlişkin Olarak Kişilerin Korunmasına İlişkin” 95/46/EC sayılı Yönerge kabul edilmiştir.

AB iç pazarının işleyişi malların, kişilerin, hizmetlerin ve sermayenin serbest dolaşımı temeline dayanmaktadır. 95/46/EC sayılı DPD, bu bahsi geçen özgürlüklerin sağlanabilmesi için verilerin de serbestçe akışı ve aynı anda kişilerin temel haklarının da korunması gerektiği mantığı üzerine kabul edilmiştir (95/46/EC sayılı DPD Giriş par. 3). Bu sebeple Yönerge, kişisel verilerin korunmasına ilişkin ulusal mevzuatların uyumlaştırılarak kişisel verilerin tüm AB ülkelerinde aynı

¹⁷⁰ Berna Akçalı Gür, “Uluslararası Hukuk ve AB Hukuku Boyutuyla Kişisel Verilerin Yurt Dışına Aktarılması”, *Marmara Üniversitesi Hukuk Fakültesi Hukuk Araştırmaları Dergisi*, C. 25, S. 2, 2019, s. 863.

¹⁷¹ Commission of the European Communities, Community Policy on Data Processing, 21.11.1973, (çevrimiçi), <http://aei.pitt.edu/6337/1/6337.pdf>, 06.03.2021.

¹⁷² Kızılırmak, *Cross-Border Transfer*, s. 14.

¹⁷³ Akçalı Gür, s. 857.

düzeyde korunması ve böylece kişisel verilerin söz konusu ülkelerde herhangi bir güvenlik riski bulunmaksızın serbest dolaşımını sağlamayı amaçlamaktaydı¹⁷⁴.

95/46/EC sayılı DPD’de kişisel verilerin, sadece Komisyon tarafından yeterli korumayı sağladığına kanaat getirilen ülkelere aktarılabilceği kuralı benimsenmiştir (madde 25). Fakat bu kurala; ilgili kişinin açık rızası, sözleşmenin ifası veya sözleşmeden doğan diğer yükümlölüklerin yerine getirilmesi, toplumsal çıkar, kanuni hakların ispat edilmesi, savunulması, ilgili kişinin menfaatlerinin korunması gibi istisnalar da getirilmiştir (madde 26.1). Aynı zamanda veri sorumlusunun sözleşme ile kişilerin özel hayatının korunması ve ilgili temel hak ve hürriyetlerinin korunacağını taahhüt ettiğı durumlarda da AB üyeleri bu veri sorumlularına veri aktarılmasına izin verebileceklerdir (madde 26.2).

95/46/EC sayılı DPD kişisel verilerin korunması alanında tüm dünyada kabul gören bir çerçeve sunmuş olsa da her üye devlet kendi veri koruma yasasını uygulamaktaydı. Çünkü AB hukukunda yönergeler doğrudan iç hukukun yerini almadığı için üye ülkelerin mevzuatlarını uyumlu hâle getirmeleri gerekmektedir¹⁷⁵. Uyulması gereken birçok farklı mevzuatın varlığı hem Birlik dâhilinde hem de üçüncü ülkelere gerçekleşecek veri akışını uzun ve karışık bir hâle getirdiğinden, üye ülkelerde uygulanmakta olan veri koruma ilkelerin modernize edilmesi ve gelecekte vatandaşların mahremiyet hakkının garanti altına alınması amacıyla, kapsamlı bir reforma gidilmesi ihtiyacı ortaya çıkmıştır. Bu kapsamda düzenlenen “Genel Veri Koruma Tüzüğü” Avrupa Parlamentosu tarafından 14 Nisan 2016 tarihinde onaylanmıştır.¹⁷⁶ Tüzüğün amacı, AB sınırlarında verilerin korunmasına ilişkin doğrudan uygulanabilen tek bir mevzuat yaratmaktan ibarettir. Böylece birkaç üye devlette veri işleme faaliyetinde bulunan veri sorumlusunun aynı anda birkaç yerel mevzuata uyum sağlaması gerekmeyecektir. Ayrıca, Birlik içerisinde serbest veri

¹⁷⁴ Wagner, s. 319; Moerel, s. 18; Kama Işık, s. 118; Ayşe Nur Akıncı, **Avrupa Birliği Genel Veri Koruma Tüzüğü’nün Getirdiğı Yenilikler ve Türk Hukuku Bakımından Değerlendirilmesi**, Kalkınma Bakanlığı, Ankara, 2017, s. 5.

¹⁷⁵ Murat Volkan Dülger, “Avrupa Birliği Genel Veri Koruma Tüzüğü Bağlamında Kişisel Verilerin Korunması”, **Yaşar Hukuk Dergisi**, C. 1, S. 2, 2019, s. 71-172, s. 79; Pelen, s. 1715; Çelik, s. 5.

¹⁷⁶ Akıncı, s. 2; Akçalı Gür, s. 858.

dolaşımı ile daha hızlı ve güvenilir bir ticari hayatın temin edileceği hedeflenmiştir¹⁷⁷.

GDPR, kişisel verilere ilişkin hazırlanmış en kapsamlı mevzuat olmakla birlikte, kişisel verilerle ilgili işlem yapan tüm kamu kurumlarına ve özel kuruluşlara ağır sorumluluklar getirmiştir. Bu sebeple GDPR hükümlerine uyum sağlayabilmeleri için AB üyelerine 2 yıl geçiş süresi tanınmıştır¹⁷⁸. 25 Mayıs 2018 tarihinde GDPR'ın yürürlüğe girmesiyle birlikte 95/46/EC sayılı DPD yürürlükten kalkmıştır. GDPR'ın en önemli özelliği, üye ülkelerde doğrudan bağlayıcı etkisinin bulunmasıdır. Başka bir deyişle, üye ülkelerin bu düzenlemede yer alan temel ilkeleri içeren ulusal mevzuat hükümlerini kabul etmelerine gerek kalmamaktadır¹⁷⁹.

GDPR hazırlanırken iki temel hedef üzerinde durulmuştur. Bunlardan ilki ilgili kişilerin veri koruma haklarının geliştirilmesi, ikincisi ise üye ülkeler arasındaki mevzuat farklılıklarını uyumlu hâle getirerek kamu kurumlarının ve ticari işletmelerin faaliyetleri kapsamında gerçekleştirilen veri aktarımını kolaylaştırmak olmuştur¹⁸⁰. Bu kapsamda sadece AB üyeleri arasındaki kişisel veri akışı değil, üçüncü ülkelere yapılacak veri aktarımları da düzenlenmektedir.

AB dışına yapılan aktarımlarla ilgili hükümler GDPR'ın 5. bölümünde ele alınmıştır. Bu bölümde Yönerge ile öngörülen kısıtlamalar değiştirilmemiş, sadece bazı yenilikler getirilmiştir. 45. madde ile yeterlilik denetiminin şartları geniş detaylandırılmış, ayrıca bu denetimin her dört senede bir tekrarlanacağı ve şartların değişmesi hâlinde uygunluk kararının iptal edilebileceği eklenmiştir. Diğer önemli fark ise Yönerge'de yer almasa da uygulamada yaygın olarak kullanılan “bağlayıcı şirket kuralları”nın GDPR'da doğrudan düzenlenmesidir (GDPR madde 47). Aynı zamanda standart sözleşme hükümleri GDPR'da da güvenlik önlemi olarak kalsa da

¹⁷⁷ Rüya Tuna Toparlak, **Veri Koruması Hukukunda Bağlayıcı Şirket Kuralları: 2016/679 sayılı Genel Veri Koruma Tüzüğü ve 6698 sayılı Kişisel Verilerin Korunması Kanunu Karşılaştırılması**, İstanbul, On İki Levha, 2021, s. 7.

¹⁷⁸ Akçalı Gür, s. 860.

¹⁷⁹ Akıncı, s. 5.

¹⁸⁰ European Commission, Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation), 25.01.2012, Brussels, (çevrimiçi), <https://eur-lex.europa.eu/legal-content/en/txt/pdf/?uri=celex:52012pc0011&from=en>, 25.06.2021.

denetleme kurumu tarafından onay alınması şartı kaldırılmıştır (GDPR madde 46.2). Bunların yanı sıra, onaylanmış davranış kuralları, onaylanmış sertifikasyon mekanizması, idari düzenlemeler gibi yeni uygun güvenlik önlemleri öngörülmüştür. Yönerge’de yer alan istisnalar da GDPR’da daha detaylı düzenlenmiş, ayrıca veri sorumlusunun zorlayıcı meşru menfaatleri de istisnalara eklenmiştir (GDPR madde 49).

6. Türk Hukukundaki Düzenlemeler

1960’lı yıllardan itibaren dünyada tartışılan bir konu hâline gelen kişisel verilerin korunması hakkı, Türkiye’de ancak 1990’lı yıllarda gündeme gelebilmiştir. 2010 yılında yapılan Anayasa değişikliği ile birlikte kişisel verilerin korunması hakkı, ilk kez Anayasa’nın “Özel hayatın gizliliği” başlıklı 20. maddesine eklenen 3. fıkrasıyla anayasal güvenceye kavuşmuştur. Buna göre:

“Herkes, kendisiyle ilgili kişisel verilerin korunmasını isteme hakkına sahiptir. Bu hak; kişinin kendisiyle ilgili kişisel veriler hakkında bilgilendirilme, bu verilere erişme, bunların düzeltilmesini veya silinmesini talep etme ve amaçları doğrultusunda kullanılıp kullanılmadığını öğrenmeyi de kapsar. Kişisel veriler, ancak kanunda öngörülen hâllerde veya kişinin açık rızasıyla işlenebilir. Kişisel verilerin korunmasına ilişkin esas ve usuller kanunla düzenlenir.”

Anılan hüküm ile kişisel verilerin korunması ilkesine müdahalenin sınırları çizilmiştir. Kişisel verilerin korunmasına ilişkin hususların kanunla düzenleneceği belirtilmiş ve bu kapsamda 6698 sayılı Kişisel Verilerin Korunması Kanunu kabul edilmiştir¹⁸¹.

Hâlihazırda kişisel verilerin korunmasını düzenleyen temel kanun olan Kişisel Verilerin Korunması Kanunu, 24 Mart 2016 tarihinde TBMM’de kabul edilmiş ve 7 Nisan 2016 tarihinde yürürlüğe girmiştir. Kanunun metni hazırlanırken OECD Rehber İlkeleri, 108 sayılı Sözleşme ve AB Yönergesi dikkate alınmıştır. Nitekim kanunun kabul edilmesinin esas sebeplerinden biri de, Türkiye’nin AB’ye üyelik müzakereleri sürecinde AB’nin Türkiye’ye yönelik ilerleme raporlarında bu

¹⁸¹ İmançlı, s. 29.

konudaki boşluğu özellikle vurgulaması ve müzakerelerin devam etmesi için bu boşluğun doldurulması ihtiyacıdır¹⁸².

Kanunda kişisel verilerin aktarılması, yurt içinde ve yurt dışına aktarılma olmakla iki ayrı maddede düzenlenmiştir. Her iki durumda kişisel verilerin aktarılması, ilgili kişilerin açık rızasına tabi kılınmış ve açık rıza olmadan kişisel veri aktarımı gerçekleştirilebilecek durumlar kesin olarak belirlenmiştir. Bu kanunun yanı sıra elektronik haberleşme, sağlık ve bankacılık sektörlerine ilişkin mevzuatta da kişisel verilerin aktarılmasına ilişkin düzenlemelere yer verilmiştir. Bu düzenlemelerin genel olarak KVKK düzenlenmeleri ile büyük ölçüde paralel olduğu görülmektedir¹⁸³.

KVKK'nın yanı sıra diğer kanunlarda ve ikincil mevzuatta da kişisel verilerin aktarılmasına ilişkin hükümler yer almaktadır. Örneğin, 5809 sayılı Elektronik Haberleşme Kanunu¹⁸⁴ m.51/f.6 uyarınca, trafik ve konum verileri, sadece veri sahibi açık rıza verdiği takdirde yurt dışına aktarılabilir. Elektronik Haberleşme Sektöründe Kişisel Verilerin İşlenmesi ve Gizliliğin Korunmasına İlişkin Yönetmelik'te de trafik ve konum verilerin yurt dışına aktarılmasına ilişkin düzenleme yer almaktadır. Yönetmeliğin m.5/f.2 uyarınca, *“milli güvenlik gerekçesiyle trafik ve konum verilerinin yurt dışına çıkarılmaması esastır”*. Aynı zamanda m.8/e uyarınca, trafik ve konum verilerinin üçüncü kişilere aktarılacağı durumlarda açık rıza; aktarılabilecek verinin kapsamı, aktarımın amacı ve süresi, aktarılabilecek tarafın adı ve açık adresi, üçüncü taraf yurt dışında ise verinin aktarılacağı ülkenin adı şeklinde bilgilendirme yapıldıktan sonra alınır.

5070 sayılı Elektronik İmza Kanunu¹⁸⁵ m.12/c uyarınca, elektronik sertifika hizmet sağlayıcısı, sertifika sahibinin onayı olmaksızın kişisel verileri üçüncü kişilere aktaramayacaktır.

5502 sayılı Sosyal Güvenlik Kurumuna İlişkin Bazı Düzenlemeler Hakkında Kanun¹⁸⁶ m.35 ile Kurumun, görevlerini yerine getirmek amacıyla işlediği kişisel

¹⁸² Bkz.: KVKK Genel Gerekçe.

¹⁸³ Ünsal Özden/ Uz/ Karamustafaoğlu, s. 26.

¹⁸⁴ RG. T. 10.11.2008, S. 27050 (mükerrer).

¹⁸⁵ RG. T. 23.01.2004, S. 25355.

verileri veya ticari sır niteliğindeki verileri paylaşması, veri sahibinin noter onaylı muvafakati veya e-Devlet uygulaması üzerinden kimlik teyidi ile verilen izne tabi tutulmuştur.

7222 sayılı Bankacılık Kanunu¹⁸⁷ m.73 ile, sıfat ve görevleri dolayısıyla banka veya müşterilere dair sırları öğrenen kişilere, öğrendikleri sırları bu konuda kanunen yetkili kılınan mercilerden başkasına açıklamama yükümlülüğü getirilmiştir. Üstelik bu yükümlülük görevden ayrıldıktan sonra da devam eder.

Maddede belirtilen sır saklama yükümlülüğünden istisna tutulan hâller haricinde, KVKK uyarınca müşteriden açık rıza alınmış olsa dahi, müşteri sırrı niteliğindeki bilgiler müşteriden gelen bir talep ya da talimat olmaksızın yurt içindeki ve yurt dışındaki üçüncü kişilerle paylaşılamaz ve bunlara aktarılamaz. Aynı nitelikte düzenlemeye Bankaların Bilgi Sistemleri ve Elektronik Bankacılık Hizmetleri Hakkında Yönetmelik'te¹⁸⁸ de yer verilmiştir (m.10). Kanunda sır saklama yükümlülüğünden istisna tutulan hâller de dâhil olmak üzere, müşteri sırrı niteliğindeki verilerin, amaçla sınırlılık ve ölçülülük ilkelerine uygun paylaşılması gerektiği de belirtilmiştir.

6563 sayılı Elektronik Ticaretin Düzenlenmesi Hakkında Kanun¹⁸⁹ m.10 ile, hizmet sağlayıcı ve aracı hizmet sağlayıcının, veri sahibinin onayı olmaksızın kişisel verileri üçüncü kişilere aktarması veya başka amaçlarla kullanması yasaklanmıştır.

2920 sayılı Türk Sivil Havacılık Kanunu¹⁹⁰ m.40'da, havayolu ile seyahat edecek kişilerin seyahatini kolaylaştırmak veya güvenlik ve risk değerlendirmesi yapmak amacıyla, kişisel verilerin KVKK kapsamında toplanabileceği, kaydedilebileceği ve paylaşılabileceği belirtilmiştir. Talep edileceği takdirde yolcu bilgileri, İçişleri Bakanlığının görüşünü almak kaydıyla havayolu işletmeleri veya kurumlar tarafından üçüncü ülkelerle paylaşılabilir.

¹⁸⁶ RG. T. 20.05.2006, S. 26173.

¹⁸⁷ RG. T. 01.11.2005, S. 25983 (mükerrer).

¹⁸⁸ RG. T. 05.11.2004, S. 29166.

¹⁸⁹ RG. T. 05.11.2004, S. 29166.

¹⁹⁰ RG. T. 19.10.1983, S. 18196.

5464 sayılı Banka Kartları ve Kredi Kartları Kanunu¹⁹¹ m.23 uyarınca, “Üye işyerleri, kartın kullanımı sonucunda kart ve kart hamili ile ilgili edindikleri bilgileri, kanunla yetkili kılınan kişi, kurum ve kuruluşlar hariç olmak üzere kart hamilinin yazılı rızasını almadan başkasına açıklayamaz, saklayamaz ve kopyalayamaz. Üye işyerleri, kart bilgilerini üye işyeri anlaşması yaptığı kuruluş dışındaki şahıs veya kuruluşlarla paylaşamaz, satamaz, satın alamaz ve takas edemez”.

7223 sayılı Ürün Güvenliği ve Teknik Düzenlemeler Kanunu¹⁹² m.23’te kişisel verilerin gizliliğini korumakla yükümlü olan yetkili kuruluşun, bu verileri açıklayabileceği hâller belirtilmiştir. Buna göre, “Yetkili kuruluş, bu Kanunu uygularken kişisel verilere dair, ticari sır niteliğindeki veya fikrî ve sınai mülkiyet hakkına ilişkin edindiği bilgilerin gizliliğini korumakla yükümlüdür. Ancak, insan sağlığı ve güvenliğinin gerektirdiği hâllerde bu bilgilerin açıklanması bu kapsamda sayılmaz”.

Kişisel veri aktarımına dair düzenlemelere “Kişisel Sağlık Verileri Hakkında Yönetmelik”te¹⁹³ (KSYV) de yer verilmiştir. Yönetmelikte kişisel sağlık verilerinin işlenmesi Kişisel Verilerin Korunması Kanunu’na dayandırıldığı için, aktarım sözü konusu olduğunda da Kanun’un yurt içinde ve yurt dışına veri aktarımlarını düzenleyen hükümlerine atıf yapılmaktadır (KSVY m.15/f.1). Bunun yanı sıra kişisel sağlık verilerinin, KVKK m.8/2, m.8/3 ve m.28 kapsamında kamu kurum ve kuruluşlarına aktarımı için bir protokol düzenleneceği öngörülmüştür (KSVY m.15/f.2)¹⁹⁴.

¹⁹¹ RG. T. 01.03.2006, S. 26095.

¹⁹² RG. T. 12.03.2020, S. 31066.

¹⁹³ RG. T. 21.06.2019, S. 30808.

¹⁹⁴ Hamza Bayındır, **Özel Sağlık Kurumları Kapsamında Kişisel Sağlık Verilerinin İşlenmesi ve Korunması**, İstanbul, On İki Levha, 2020, s. 16-17.

İKİNCİ BÖLÜM

AVRUPA BİRLİĞİ HUKUKUNDA KİŞİSEL VERİLERİN AKTARILMASI

I. Genel Olarak

1970’li yıllardan itibaren bazı Avrupa ülkelerinde kişisel verilerin aktarılmasına ilişkin ulusal düzeyde düzenlemeler yapılmış olsa da, bu hususta AB düzeyinde gerçekleştirilen ilk düzenleme 95/46/EC sayılı DPD olmuştur. Hâlihazırda AB’de bütün kişisel veri aktarımları GDPR hükümleri ile düzenlenmektedir. Şunu da belirtmek gerekir ki suçların önlenmesi, soruşturulması, tespiti veya kovuşturulması ya da cezaların infaz edilmesi kapsamında kişisel verilerin yetkili makamlar tarafından aktarılması GDPR’ın kapsamı dışında kalmaktadır. Zira bu tür kişisel veri aktarımları 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” Yönerge¹⁹⁵ ile düzenlenmektedir.

Hem mülga 95/46/EC sayılı DPD’nin 4. bölümünde hem de GDPR’ın 5. bölümünde yer alan kişisel veri aktarımlarına ilişkin hükümler gözden geçirildiğinde KVKK’nın aksine, söz konusu düzenlemelerin sadece üçüncü ülkelere yapılan kişisel veri aktarımlarına ilişkin olduğu görülmektedir. Her ne kadar GDPR’ın kişisel veri aktarımlarına ilişkin hükümleri üçüncü ülkelerin yanı sıra uluslararası kuruluşlara yapılan aktarımları da kapsayacak şekilde genişletilse de, sadece Birlik dışına yapılan aktarımları ile sınırlı kalmıştır. Bunun temel sebebi, her iki düzenlemede kişisel verilerin Birlik sınırları dâhilinde dolaşımının serbest kılınması ve dolayısıyla üçüncü ülkelere ve uluslararası kuruluşlara yapılan aktarımlar zamanı uygulanacak olan kısıtlamalardan muaf tutulmasıdır. Bu nedenle çalışmanın bundan sonraki bölümlerinde AB bağlamında kişisel veri aktarımlarından bahsederken sadece AB üyesi olmayan üçüncü ülkelere ve uluslararası kuruluşlara yapılan aktarımlar

¹⁹⁵ Directive 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, (çevrimiçi), <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016L0680>, 25.10.2021.

kastedilecek, kişisel verilerin AB dâhilinde aktarılması ise kişisel verilerin serbest dolaşımı (*free flow of personal data*) kavramı ile ifade edilecektir.

II. Avrupa Birliği Dâhilinde Kişisel Verilerin Serbest Dolaşımı

Kişisel verilerin, bir Birlik dâhilinde serbest dolaşımını düzenleyen ilk uluslararası düzenleme OECD tarafından gerçekleştirilmiştir. 1980 yılında kabul edilen bağlayıcı olmayan Rehber İlkeler'e göre, üye ülkeler, transit geçişler de dâhil olmak üzere kişisel verilerin diğer üye ülkelere aktarılmasının kesintisiz ve güvenli olmasını sağlamak için tüm makul ve uygun önlemleri almalıdır¹⁹⁶. Üye ülkeler, mahremiyetin ve bireysel özgürlüklerin korunması adına, bu tür koruma için gereksinimleri aşacak kişisel veri akışlarının engellenmesine engel olacak yasalar, politikalar ve uygulamalar geliştirmekten kaçınmalı¹⁹⁷ ve Rehber İlkeler'de belirtilen durumlar istisna olmakla, diğer üye ülkelerle arasındaki veri akışına kısıtlamalar getirmekten çekinmelidir¹⁹⁸.

Verilerin üye ülkeler arasında serbest dolaşımını öngören bir diğer düzenleme de AK'nın 108 sayılı Sözleşmesi'dir. Buna göre, Sözleşme'ye taraf olan devlet, münhasıran özel hayatın korunması amacıyla diğer tarafa yapılan veri akışını yasaklayamaz veya özel bir izne tabi tutamaz (m.12/f.2). Sadece iç hukukta özel veri kategorileri için özel düzenlemelerin öngörüldüğü ve diğer taraf devletin eşdeğer korumayı sağlamadığı durumlarda ve bir taraf devletin, diğer taraf devlet üzerinden taraf olmayan devlete veri aktarımı yapmasını engellemek amacıyla veri akışı yasaklanabilecektir (108 sayılı Sözleşme m.12/f.3).

AB kapsamında kişisel verilerin serbest dolaşımı ise ilk kez 95/46/EC sayılı DPD m.1/f.2'de öngörülmüştür. Yönerge yürürlükten kalktıktan sonra ise aynı yaklaşım GDPR'da da devam ettirilmiştir. Buna göre, kişisel verilerin işlenmesiyle ilgili olarak gerçek kişilerin korunmasına yönelik sebeplerle Birlik içerisinde kişisel verilerin serbest dolaşımına, kısıtlamalar ve yasaklar getirilemez (GDPR m.1/f.3).

¹⁹⁶ OECD, **Guidelines**, par. 16.

¹⁹⁷ OECD, **Guidelines**, par. 18.

¹⁹⁸ OECD, **Guidelines**, par. 17.

Kişisel verilerin Birlik dâhilinde serbest dolaşımı, AB'nin temel unsurlarından biri olan iç pazarın gelişimini sağlamak amacıyla belirlenmiştir¹⁹⁹. Şöyle ki, ortak bir pazarın kurulmasını amaçlayan 1957 tarihli Avrupa Ekonomik Topluluğu'nu kuran Roma anlaşması²⁰⁰ ile bu amaç doğrultusunda *malların, hizmetlerin, sermayenin ve kişilerin serbest dolaşımı* kabul edilmiştir (m.2 ve m.3/b). İç pazarın işleyişi söz konusu dört unsura dayanmaktadır. Zaman içerisinde elektronik ticaretin gitgide artması ve veri tabanlı ekonominin ciddi boyutlara ulaşması sonucunda iç pazarın işleyişini temin etmek için kişisel verilerin de serbest dolaşımının hayati önem arz ettiği anlaşılmıştır²⁰¹. Bu nedenle kişisel verilerin serbest dolaşımı, bazı yazarlar tarafından iç pazarın beşinci unsuru olarak nitelendirilmektedir²⁰².

Kişisel verilerin AB sınırları dâhilinde serbest dolaşımının kabulü, iç pazarın işleyişini temin etme amacına hizmet ettiğinden verilerin serbest dolaşım alanı da sadece AB ülkeleri ile sınırlandırılmamış, 1992 yılında akdedilen anlaşma²⁰³ ile AB üyesi olmasa bile Avrupa Ekonomik Alanı'na (AEA) dâhil olan ülkeleri de kapsayacak şekilde genişletilmiştir²⁰⁴. Anlaşmayı imzalayan ülkelere bazıları (Avusturya, İsveç, Finlanda) bir süre sonra AB'ye üye olarak kabul edilse de, hâlihazırda AB üyesi olmayan Norveç, İzlanda ve Lihtenştayn gibi ülkeler iç pazara dâhil edildiyinden, söz konusu ülkelere yapılan aktarımlar üçüncü ülkelere yapılan aktarımlar için öngörülen kısıtlamalardan muaftır²⁰⁵.

Kanaatimizce, verilerin serbest dolaşımı, kişisel verilerin AB dâhilinde hiçbir kural gözetmeksizin hareket ettiği anlamına gelmemelidir. Zira serbest dolaşım

¹⁹⁹ W. Gregory Voss, "Cross-Border Data Flows, the GDPR, and Data Governance", **International Law Journal**, C. 29, S. 3, 2020, s. 504-505; Wagner, s. 320; Kaya, **Transfer of Personal Data**, s. 20; Çelik, s. 63.

²⁰⁰ Treaty establishing the European Economic Community, 25.03.1957, (çevrimiçi), https://www.ab.gov.tr/files/ardb/evt/1_avrupa_birligi/1_3_antlasmalar/1_3_1_kurucu_antlasmalar/1957_treaty_establishing_eec.pdf, 04.05.2021.

²⁰¹ Arslan, s. 460.

²⁰² Voss, s. 504.

²⁰³ Agreement on the European Economic Area, 02.05.1992 (çevrimiçi), <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A31994D0001>, 04.05.2021.

²⁰⁴ Bu nedenle bu çalışmada kişisel verilerin aktarılması bağlamında AB ülkelerinden bahsedildiğinde AEA ülkeleri kastedilmektedir.

²⁰⁵ Christos Giakoumopoulos/ Giovanni Buttarelli/ Michael O'Flaherty, **Handbook on European Data Protection Law**, Lüksemburg, Publications Office of the European Union, 2018, s. 252; Arslan, s. 465.

kavramı ile kastedilen, verilerin üçüncü ülkelere ve uluslararası kuruluşlara yapılan aktarımlar zamanı uygulanacak olan kısıtlamalara (yetetlilik kararı, uygun güvenlik önlemleri, uluslararası anlaşma, veri sahibinin açık rızası vs.) tabi tutulmadan iletilmesi imkânıdır²⁰⁶. Ayrıca GDPR m.4/2 uyarınca, otomatik yöntemlerle olsun veya olmasın, kişisel verileri iletim yoluyla açıklama, yayma veya herhangi başka bir şekilde kullanıma sunma kişisel verilerin işlenmesi olarak nitelendirilecektir²⁰⁷. Bu bağlamda kişisel verilerin Birlik sınırları içerisinde dolaşımı da bir çeşit veri işlemeyi teşkil ettiğinden yasal bir dayanağının bulunması gerekmektedir²⁰⁸. Başka bir deyişle, kişisel verilerin Birlik dâhilinde serbestçe dolaşabilmesi için GDPR m.6 ile m.11’de öngörülen hukuka uygunluk sebeplerinden birinin mevcut olması gerekmektedir. Aynı zamanda GDPR m.5’te belirtilen kişisel verilerin işlenmesinin genel ilkeleri verilerin AB dâhilinde serbest dolaşımı açısından da saklıdır²⁰⁹.

III. Kişisel Verilerin Birlik Dışına Aktarılması

A. Genel Olarak

Yukarıda²¹⁰ da belirtildiği üzere sınır ötesi veri aktarımlarıyla ilgili hükümler içeren ilk kanun 1973 yılında İsveç’te kabul edilmiştir. Bu kanunun hükümlerine göre İsveç’ten yurt dışına yapılan aktarımlar, İsveç Veri Koruma Kurumu’ndan alınan izne tabi tutulmuştur²¹¹. Daha sonra Avusturya, Finlandiya, Fransa, İrlanda, ve Lüksemburg gibi ülkelere kabul edilen kanunlarda da, başka ülkelere yapılan veri aktarımlarına yönelik farklı kısıtlamalar uygulanması öngörülmüştür²¹². İlk ulusal veri koruma kanunların hepsinin ortak özelliği, sınır ötesi kişisel veri aktarımlarının kural olarak değil, istisna olarak öngörülmesidir²¹³.

²⁰⁶ Çelik, s. 36.

²⁰⁷ Sertçe, s. 8.

²⁰⁸ Küzeci, s. 192.

²⁰⁹ Kuner, **European Data Protection**, s. 89.

²¹⁰ Bkz.: yuk., Birinci bölüm “İlk Düzenlemeler” başlığı.

²¹¹ Wagner, s. 319; Svantesson, **Cross-Border Data Flow**, s. 180; Christopher Kuner/ Lee A. Bygrave/ Christopher Docksey/ Laura Drechsler, **The EU General Data Protection Regulation: A Commentary**, Oxford University Press, Oxford, 2020, s. 758 (Kuner v.d., **Commentary**).

²¹² Kuner, **Privacy Law**, s. 14; Kuner, **Data Flows**, s. 26.

²¹³ Kuner, **Privacy Law**, s. 208.

Bu hususta ilk bağlayıcı belge olan 108 sayılı Sözleşme ve onun ek protokolünde, bir taraf devletten taraf olmayan devlete veri aktarımları, taraf olmayan devlette eşdeğer koruma düzeyinin bulunması şartına tabi tutulmuştur. Modernize edilmiş 108+ sayılı Sözleşme ile de aranan bu şart devam ettirilmiş ve yeterli korumanın temin edilmesi yöntemlerine de yer verilmiştir (Sözleşme 108+ m.14/f.3).

AB düzeyinde kişisel verilerin üçüncü ülkelere aktarılması ise ilk kez 95/46/EC sayılı DPD ile düzenlenmiştir. Bu Yönerge ile yeterli korumanın bulunmadığı ülkelere veri aktarımına kısıtlamalar getirilmiştir. Bir başka deyişle, AB'nin veri koruma yaklaşımının temel hedeflerinden biri, AB'deki yüksek veri koruma seviyesini muhafaza etmek amacıyla, daha düşük veri koruma seviyesine sahip üçüncü ülkelere kişisel verilerin aktarılmasını yasaklayan yasalar kabul etmek olmuştur²¹⁴.

AB'nin bu sıkı yaklaşımı başta Amerika Birleşik Devletleri (ABD) olmak üzere birçok ülkenin tepkisine sebep olmuştur²¹⁵. Bu doğrultuda AB'ye yöneltilen suçlamalar, Birlik çerçevesinde kurduğu sistemini tüm dünya geneline dayatması, sanal ticarete ABD ile yarışabilmek adına vakit kazanmaya çalışması ve serbest rekabete zarar vermesi yönünde olmuştur²¹⁶. Fakat bu tepkilere rağmen AB, kendi sistemini uluslararası alanda etkili bir model olarak kabul ettirebilmiş ve birçok dünya devleti, AB ile ticaret ve ekonomik ilişkilerini sürdürebilmek adına, AB düzenlemelerine benzer düzenlemeler kabul etmişlerdir²¹⁷. GDPR'ın giriş bölümünde uluslararası işbirliği ve ticaretin genişletilmesi için sınır ötesi veri akışlarının önemi kabul edilse de, kişisel verilerin üçüncü ülke veya uluslararası kuruluşlara aktarılması sırasında, GDPR'la sağlanan gerçek kişilerin korunması seviyesinin göz ardı edilmemesi gerektiği belirtilmiştir (GDPR Giriş par. 101).

95/46/EC sayılı DPD'nin yerine geçen GDPR'da da kişisel verilerin aktarılması açısından neredeyse aynı hükümler yer almaktadır. Sadece GDPR'da yer

²¹⁴ Wagner, s. 319; Bygrave, **Data Protection**, s. 79-80; Hon, s. 46; Çelik, s. 63.

²¹⁵ Andrew Charlesworth, "Information Privacy Law in the European Union: E Pluribus Unum or Ex Uno Plures?", **Hastings Law Journal**, C.54, S. 4, 2003, s. 65; Küzeci, s. 193.

²¹⁶ Küzeci, s. 193.

²¹⁷ Hon, s. 158; Küzeci, s. 194.

alan hükümler daha da detaylandırılmıştır²¹⁸. Örneğin, 95/46/EC sayılı DPD'den farklı olarak, GDPR'da aktarımların kapsamı daha da genişletilerek yalnızca AEA'ya dâhil olmayan ülkelere değil, uluslararası kuruluşlara ve üçüncü ülkedeki bir bölge veya özel bir sektöre de yapılan aktarımlara yönelik kısıtlamalar öngörülmüştür (GDPR m.44-50). Kanaatimizce, madde metninin bu şekilde genişletilmesi, yeterlilik kararlarının kabul edilme sürecini hızlandırmak amacıyla hizmet etmektedir. Zira bütün bir ülke hakkında yeterlilik kararı çıkarmak daha fazla mali kaynak ve süre gerektirmektedir²¹⁹. Bunun dışında, birçok ülkede, farklı sektörlerde veri işlemeyi kapsayan özel yasalar bulunmaktadır ve koruma düzeyi farklı sektörler arasında önemli ölçüde farklılık gösterebilir. Ayrıca, ABD gibi federal devletlerde bazı eyaletlerin veri koruma yasası bulunsun da, ABD hiçbir zaman federal düzeyde yasa çıkarmaya olumlu yaklaşmamıştır²²⁰.

GDPR'da kişisel verilerin aktarılmasına yönelik bir diğer yenilik ise, Tüzük'te sadece AB üyesi bir ülkeden üçüncü ülkeye yapılan ilk aktarımlar değil, aynı zamanda ileri aktarımlar²²¹ (*onward transfers*) da düzenlenmiştir. Şöyle ki, 95/46/EC sayılı DPD'de, örneğin kişisel verilerin, bu verileri ithal etmiş olan ülkeden başka bir ülkeye yeniden aktarıldığı durumlarda ne gibi önlemler alınması gerektiğine dair bir hüküm bulunmamaktaydı²²². Buna rağmen Madde 29 Çalışma Grubu'nun raporunda, kişisel verilerin aktarılmış olduğu ülkeden başka bir üçüncü ülkeye aktarılmasına yalnızca ikinci ülkenin yeterli seviyede korumayı sağladığı durumlarda izin verilmesi gerektiği belirtilmiştir²²³.

²¹⁸ Sanjay Sharma/ Pranav Menon, **Data Privacy and GDPR Handbook**, New Jersey, John Wiley & Sons Inc., 2020, s. 162.

²¹⁹ Christopher Kuner, "Developing an Adequate Legal Framework for International Data Transfers", **Reinventing Data Protection?** İçinde, Ed.: Serge Gutwirth, Yves Poullet, Paul de Hert, Cecile de Terwagne, Sjaak Nouwt, Springer, 2009, s. 263-273.

²²⁰ Küzeci, s. 199.

²²¹ "... verilerin aktarıldığı üçüncü ülke veya kuruluştan, aynı veya farklı üçüncü ülke veya kuruluştaki veri sorumlusu veya veri işleyene yapılan aktarımlar..." (GDPR par. 101 ileri aktarımlar).

²²² Kuner, **Data Flows**, s. 44; Voss, 506.

²²³ European Commission, First Orientations on Transfers of Personal Data to Third Countries - Possible Ways Forward in Assessing Adequacy, 26.06.1997, par. 6, (çevrimiçi), https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/1997/wp4_en.pdf, 04.04.2021.

EDPB tarafından 18 Kasım 2021 tarihinde yayınlanan ve 31 Ocak 2022 tarihine kadar istişareye açık olan Kılavuz'da²²⁴ bir veri işleme faaliyetinin üçüncü ülkelere veya uluslararası kuruluşlara aktarım olarak değerlendirilmesi için bulunması gereken kriterler belirlenmiştir. Bu kriterlere göre, kişisel verilerin, GDPR'a tabi olan veri sorumlusu veya veri işleyen (veri aktaran) tarafından GDPR'a tabi olup olmaması farketmeksizin üçüncü ülkede veya uluslararası kuruluşta bulunan bir veri sorumlusu, ortak veri sorumlusu veya veri işleyene (veri alıcısına) iletilmesi veya kullanılabilir duruma getirilmesi hâlinde bir aktarımdan bahsedilebilecektir²²⁵.

GDPR'da kişisel verilerin üçüncü ülkelere veya uluslararası kuruluşlara aktarılabilmesi bağlamında temel ilke, söz konusu verilerin aktarılacağı ülkelerde yeterli koruma düzeyinin sağlanmış olmasıdır. Bunun için öncelikle verilerin aktarılacağı ülkede yeterli korumanın mevcut olduğuna dair yeterlilik kararının (*adequacy decision*) bulunup bulunmadığı aranacaktır (GDPR m.45). Böyle bir kararın bulunmadığı durumlarda, veri sahibi için uygulanabilir haklar ve yasal çözümler de dâhil olmak üzere, veri sorumlusu veya veri işleyen tarafından alınan uygun önlemler (*appropriate safeguards*) doğrultusunda kişisel veri aktarımı gerçekleştirilebilir (GDPR m.46). Aynı zamanda, hem yeterlilik kararının hem de uygun önlemlerin alınmadığı bir takım belirli durumlarda (*derogations for specific situations*) da kişisel veri aktarımının gerçekleştirilebileceği öngörülmüştür (GDPR m.49).

Görüldüğü üzere, kişisel verilerin AB dışına aktarılabilmesinin hukuki dayanağını teşkil eden bu mekanizmalar arasında bir hiyerarşi söz konusudur. Şöyle ki, GDPR'da yeterli koruma kararı diğerlerinden üstün tutularak, sadece böyle bir

²²⁴ European Data Protection Board, Guidelines 05/2021 on the Interplay between the Application of Article 3 and the Provisions on International Transfers as per Chapter V of the GDPR, 18.11.2021, (çevrimiçi) https://edpb.europa.eu/our-work-tools/documents/public-consultations/2021/guidelines-052021-interplay-between-application_en, 26.12.2021.

²²⁵ EDPB, **Guidelines 05/2021**, s. 4-7.

kararın olmadığı durumlarda diğer hukuki dayanakların mevcut olup olmadığının aranacağı düzenlenmiştir²²⁶.

Şunu da belirtmek gerekir ki sınır ötesi veri aktarımlarına yönelik iki farklı yaklaşım bulunmaktadır. Bu yaklaşımları coğrafi temelli (*geographically-based*) ve örgütsel temelli (*organizationally-based*) olarak ikiye ayırmak mümkündür²²⁷. Coğrafi temelli yaklaşım, yurt dışına yapılan aktarımları, veri aktarımının yapıldığı ülkenin yasal sistemi tarafından belirli bir koruma düzeyinin temin edilip edilmediğinin ve uygulamadaki uyumun değerlendirilmesine dayalı olarak düzenler. Bu bakımdan, Komisyon tarafından alınan yeterlilik kararlarına dayalı olarak yukarıda belirtilen üçüncü ülkelere veri aktarımı buna bir örnek teşkil etmektedir²²⁸. Örgütsel temelli yaklaşım ise, veri aktaranları, yurt dışındaki veri alıcılarına aktardıkları kişisel verilerin sürekli olarak korunmasını sağlamak için gerekli önlemleri almaktan sorumlu kılar. Bazen bu nedenle “hesap verebilirlik yaklaşımı” olarak da adlandırılır²²⁹. GDPR’da bahsedilen veri sorumluları ve veri işleyenler tarafından alınan uygun güvenlik önlemlerine dayalı aktarımlar, örgütsel temelli yaklaşıma örnek olarak gösterilebilir. Görüldüğü üzere, GDPR yurt dışı aktarımları düzenlerken karma yaklaşım benimsemiştir.

B. Yeterlilik Kararına Dayalı Aktarılma

1. Genel Olarak

GDPR m.45/f.1 uyarınca, Komisyon’un bir üçüncü ülke veya söz konusu üçüncü ülke dâhilindeki bir bölge veya bir ya da daha fazla sayıda sektörün ya da uluslararası bir kuruluşun yeterli düzeyde bir koruma sağladığına karar verdiği hâllerde, bu ülke veya uluslararası kuruluşla yönelik bir kişisel veri aktarımı gerçekleşebilir. Hakkında yeterli koruma kararının bulunduğu ülkelere veri aktarımını gerçekleştirmek, veri sorumluları açısından oldukça kolay bir yoldur. Çünkü böyle durumlarda, veri sorumlusu veya veri işleyen tarafından ek güvenlik

²²⁶ Hon, s. 152; Kuner, **European Data Protection**, s. 158; Kuner v.d., **Commentary**, s. 764-765; Bilgi Information Technology Law Institute, s. 72-73; Sertçe, s. 11-12.

²²⁷ Kuner, **Data Flows**, s. 64; Murat Volkan Dülger/, Cansu Ceren Kahraman, “GDPR ve KVKK Ekseninde Bağlayıcı Şirket Kuralları”, Hukuk ve Daha Fazlası, 2021, s. 67, (çevrimiçi), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3853724, 23.10.2021.

²²⁸ Kuner, **Data Flows**, s. 64.

²²⁹ Kuner, a.y.

önlemleri alınmasına gerek kalmamaktadır ve aktarım kişisel verilerin AB içindeki bir alıcıya aktarılması gibi gerçekleştirilebilir²³⁰. Ayrıca bu durumda aktarımı gerçekleştirmek için spesifik bir izin alınması gerekmez.

“Yeterli düzeyde koruma” kavramının neyi ifade ettiğine dair GDPR’da herhangi bir açıklama bulunmasa da, ABAD’ın bir kararında²³¹ söz konusu kavramdan ne anlaşılması gerektiğine yer verilmiştir²³². Buna göre, yeterli düzeyde koruma temel hak ve özgürlüklerin, AB hukukunun temin ettiği güvencelere “temelde eşdeğer” (*essentially equivalent*) korunmasının, üçüncü ülkeler tarafından taahhüt edilmesini ifade etmektedir²³³. Karardan da anlaşıldığı üzere, verilerin aktarılacağı ülke mevzuatının, AB mevzuatı ile aynı olması değil, ona eşit düzeyde olması şartı aranmaktadır. Başka bir deyişle, üçüncü ülke yeterli veri koruma seviyesini sağlarken AB standartlarını aynen takip etmeden, bunu farklı uygulamalarla da gerçekleştirebilir²³⁴.

Yeterlilik kararları sadece Komisyon tarafından verilmektedir ve hukuken bağlayıcı niteliktedir²³⁵. Başka bir deyişle, AB Resmî Gazetesi’nde belirli bir ülkenin yeterli koruma düzeyi sağladığına dair Komisyon kararı yayınlandığında bütün AEA’ya üye ülkeler bu karara uymakla yükümlüdür²³⁶.

Komisyon tarafından yeterli koruma sağladığına karar verilen ülkeler²³⁷ AB’nin “Beyaz Liste”sini oluşturmaktadır²³⁸. Şimdiye kadar az sayıda ülke hakkında yeterlilik kararı verilmiştir. Bunun esas sebebi hukuk sistemleri arasındaki farklılıklar ve inceleme sürecinin uzun sürmesidir. Yeterlilik kararının alınması için;

²³⁰ Wagner, s. 320; Pelen, s. 1720; Sertçe, s. 13; Çelik, s. 82, 117.

²³¹ ABAD, C-362/14, 06.10.2015, par. 96, (çevrimiçi) <https://eur-lex.europa.eu/legal-content/en/txt/?uri=celex:62014cj0362>, 15.05.2021.

²³² Kuner, **Reality and Illusion**, s. 895.

²³³ Giakoumopoulos/ Buttarelli/ O’Flaherty, **Handbook**, s. 254; Sertçe, s. 12.

²³⁴ Giakoumopoulos/ Buttarelli/ O’Flaherty, a.y.; Sertçe, s. 14.

²³⁵ 95/46/EC sayılı DPD’ye göre, AB Komisyonundan başka üye ülkeler de yeterlilik kararı alma yetkisini haizdi.

²³⁶ Giakoumopoulos/ Buttarelli/ O’Flaherty, a.y.; Bilgi Information Technology Law Institute, s. 18.

²³⁷ Ülkelerin tam listesi için bkz.: (çevrimiçi), https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en, 20.10.2021.

²³⁸ Kaya, **Transfer of Personal Data**, s. 27; Nikolaos I. Theodorakis, “Cross Border Data Transfers Under the GDPR: The Example of Transferring Data from the EU to the US”, Transatlantic Technology Law Forum Working Papers №39, Ed.: Siegfried Fina, Mark Lemley, and Roland Vogl, 2018, s. 7; Bilgi Information Technology Law Institute, s. 74; Arslan, s. 468.

Komisyon tarafından teklif sunulması, Avrupa Veri Koruma Kurulu'ndan (EDPB) görüş alınması ve kararın Komisyonerlerce kabul edilmesi gerekmektedir²³⁹. Ayrıca bu kararların kabulünde politik nedenlerin varlığı da inkâr edilemez²⁴⁰. Örneğin, Arjantin'le ilgili değerlendirme yapılırken veri koruma otoritelerinin, bu ülkedeki yeterli koruma seviyesiyle ilgili ciddi endişeleri olsa da sırf politik nedenlerin etkisiyle Komisyon'un, Arjantin hakkında kararı olumlu yönde olmuştur²⁴¹. Bunun dışında, 2010 yılında İrlanda, İsrail hükümetinin, sahte İrlanda pasaportlarının oluşturulmasında rol aldığı iddiasına dayanarak İsrail için yeterlilik kararı alınmasına engel olmuştur²⁴².

Hâlihazırda 95/46/EC sayılı DPD yürürlükten kaldırılmış olmasına rağmen, GDPR'ın yürürlüğe girdiği tarihten önce Komisyon tarafından alınan yeterlilik kararları hâlâ geçerliliğini korumaktadır. Tüzüğün yürürlüğe girmesinin ardından sadece Japonya, Birleşik Krallık ve son olarak da Güney Kore hakkında yeterlilik kararları kabul edilmiştir. 31 Aralık 2020 tarihinde Birleşik Krallık'ın AB'den ayrılmasının ("Brexit") ardından Birleşik Krallık da kişisel veri aktarımları açısından AB için üçüncü ülke konumuna gelmiş ve m.45 kapsamında bir yeterlilik kararı alınması ihtiyacı doğmuştur. Bu doğrultuda 28 Haziran 2021 tarihinde Komisyon, GDPR ve 2016/680 sayılı Yönerge uyarınca Birleşik Krallık'a aktarılan kişisel verilerin yeterli düzeyde korunduğuna dair yeterlilik kararlarını onaylamıştır²⁴³.

2. Yeterlilik Değerlendirmesinde Dikkate Alınması Gereken Hususlar

Yeterli düzeyde korumanın varlığına ilişkin karar alınırken dikkate alınması gereken hususlar açısından GDPR, 95/46/EC sayılı DPD'den daha ayrıntılıdır²⁴⁴. Şöyle ki, Yönerge'nin m.25/f.2 uyarınca, üçüncü ülke tarafından sağlanan veri koruma düzeyinin yeterliliği belirlenirken, veri aktarım faaliyetleri dizisinin veya bir

²³⁹ Bilgi Information Technology Law Institute, s. 74.

²⁴⁰ Kuner, **European Data Protection**, s. 178.

²⁴¹ Kuner, **International Data Transfers**, s. 4; Paul Roth, "Adequate Level of Data Protection in Third Countries Post-Schrems and under the General Data Protection Regulation", **Journal of Law, Information and Science**, C. 25, S. 1, 2017, s. 61; Christopher Wolf, "Delusions of Adequacy? Examining the Case for Finding the United States Adequate for Cross-Border EU-U.S. Data Transfers", **Washington University Journal of Law & Policy**, C. 43, S. 227, 2014, s. 241.

²⁴² Wolf, a.y.; Laurence Peter, "Ireland delays EU deal with Israel on data transfers", 03.09.2010, (çevrimiçi), <https://www.bbc.com/news/world-europe-11176926>, 25.03.2021.

²⁴³ Pelen, s. 1722; Sertçe, s. 17.

²⁴⁴ Kuner v.d., **Commentary**, s. 775.

veri aktarım faaliyetini çevreleyen tüm koşulların ışığında değerlendirilecektir. Özellikle, o ülkeyle uyumlu meslek kuralları ve güvenlik tedbirleri ve söz konusu üçüncü ülkedeki yürürlükte olan hem genel hem sektörel hukuki düzenlemeler, son varış ülkesi ve menşe ülke, önerilen faaliyet veya faaliyetlerin süresi ve amacı, verilerin yapısına önem verilecektir²⁴⁵.

Bu genel kriterlere ek olarak, Madde 29 Çalışma Grubu, 1987 yılında yayınladığı Çalışma Belgesi'nde²⁴⁶ yeterlilik kararı için dikkate alınması gereken ilkelere yer vermiş, 1998 yılında yayınlanan Çalışma Belgesi'nde²⁴⁷ ise bu ilkeler daha da detaylandırılmıştır²⁴⁸. Her iki belgede de, söz konusu ilkeler Yönerge'nin ve diğer uluslararası düzenlemelerin hükümleri göz önünde bulundurularak *içerik ve uygulamaya yönelik* ilkeler olarak kategorize edilmiştir. Bu kriterlerin hukuki bağlayıcılığı olmasa da, bağlayıcı nitelikli Komisyon kararları için önemli bir yere sahiptirler²⁴⁹. Çünkü "yeterlilik" kavramının neyi kapsadığına dair Avrupa Veri Koruma Otoritelerinin görüşlerini ve esas olarak 95/46/EC sayılı DPD ve diğer uluslararası veri koruma düzenlemelerindeki gereklilikleri ifade etmektedir²⁵⁰.

Verilerin aktarılacağı üçüncü ülkede yeterli koruma düzeyi saptanırken sadece ilgili hukukta konuya ilişkin olarak belirlenmiş kurallar değil, bu kuralların işlerliğini sağlamak amacıyla oluşturulmuş sistemin de dikkate alınması gerekir²⁵¹. Komisyon'un yeterlilik kararları açısından önemli bir çıkış noktası oluşturmasına rağmen, söz konusu kriterler ne kesin bir şekilde formüle edilmiş ne de katı bir şekilde uygulanmıştır²⁵².

GDPR'da ise yeterlilik kararı alınırken dikkate alınması gereken unsurlar daha ayrıntılı ifade edilmiş ve üç grupta sınıflandırılmıştır (m.45/f.2):

²⁴⁵ Kama Işık, s. 127.

²⁴⁶ European Commission, **First Orientation on Transfers**, par. 3/I, 3/II.

²⁴⁷ European Commission, **Transfers of Personal Data to Third Countries : Applying Articles 25 and 26 of the EU Data Protection Directives**, 24.07.1998, s. 5, (çevrimiçi), ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/1998/wp12_en.pdf, 20.05.2021.

²⁴⁸ Lloyd, s. 186.

²⁴⁹ Wagner, s. 326.

²⁵⁰ Roth, s. 52.

²⁵¹ Küzeci, s. 195.

²⁵² Lee A. Bygrave, "Privacy and Data Protection in an International Perspective", **Scandinavian Studies in Law**, 2010, C. 56, s. 193.

1. Yasal düzenlemeler - Komisyon'un deęerlendirmesi gereken ilk husus, kişisel verilerin aktarılacağı ülkelerin, bu verilerin hukuki korumasını sağlamaya yetecek yasal bir sisteme sahip olup olmadığıdır. Komisyon bu kapsamda yabancı ülkedeki; hukukun üstünlüğü, insan hakları ve temel özgürlüklerine saygı, kamu güvenliği, savunma, milli güvenlik ve ceza hukuku ile kamu kuruluşlarının kişisel verilere erişimi de dâhil olmak üzere hem genel hem de sektörel mevzuatın yanı sıra söz konusu mevzuatın uygulanması, bir ülke veya uluslararası kuruluşta toplanan kişisel verilerin başka bir üçüncü ülke veya uluslararası kuruluşa ileri aktarımına yönelik kurallar da dâhil olmak üzere veri koruma kuralları, mesleki kurallar ve güvenlik tedbirleri, içtihadın yanı sıra etkili ve uygulanabilir veri sahibi hakları ile kişisel verileri aktarılmakta olan veri sahiplerine yönelik etkili idari ve adli tazmini deęerlendirecektir (GDPR m.45/f.2/a).

2. Denetim makamları - Komisyon'un deęerlendirmesi gereken dięer husus; yeterli uygulatma yetkileri de dâhil olmak üzere veri koruma kurallarına uyum sağlanması ve sağlatılması, haklarının kullanımı hususunda veri sahiplerine destek olunması ve tavsiyede bulunulması ve üye devletlerin denetim makamları ile işbirliği yapılmasından sorumlu olan bir veya daha fazla sayıda bağımsız denetim makamının varlığı ve etkili bir şekilde işlev göstermesidir (GDPR m.45/f.2/ b).

3. Uluslararası yükümlölükler - Komisyon'un dikkate alacağı dięer husus, verilerin aktarılacağı ülke veya uluslararası kuruluşun üstlendięi uluslararası taahhütler veya yasal bağlayıcılığı olan sözleşmeler veya belgelerin yanı sıra kişisel verilerin korunması ile ilgili olanlar başta olmak üzere çok taraflı veya bölgesel sistemlere katılımından kaynaklanan dięer yükümlölüklerdir (GDPR m.45/f.2/c).

Bu noktada belirtmek gerekir ki, GDPR'ın 45.2. maddesinde bu kriterlere istinaden kullanılan “... Komisyon ... özellikle aşağıdaki hususları dikkate alır” ifadesinden, bu listenin kesin ve tam olmadığı anlaşılmaktadır²⁵³. Başka bir deyişle Komisyon, yeterlilik deęerlendirmesi yaparken ek olarak dięer hususları da dikkate alabilecektir.

²⁵³ Wagner, s. 321; Van den Bulck, s. 235; Sertçe, s. 17.

Bu konuda açıklık getirilmesi gereken bir husus da 108 sayılı Sözleşme'yi onaylayan fakat AB'ye üye olmayan ülkelerin yeterli koruma sağlayan ülke olarak kabul edilip edilmeyeceğidir. Yukarıda da bahsedildiği üzere, Sözleşmeye taraf olan ülkeler arasında kişisel verilerin dolaşımı serbest kılınmıştır. Fakat bu Sözleşme ve Ek Protokolü imzalayan ülkelerden 19'u AB üyesi değildir. Malum olduğu üzere, GDPR'da kişisel verilerin serbest dolaşımı sadece AB sınırları içerisinde kabul edilmektedir. Bu durumda, bir AB üyesi olan ülkeden AB üyesi olmayan fakat Sözleşme ve Ek Protokole aynı zamanda taraf olan ülkelere kişisel verilerin aktarılması zamanı söz konusu ülkelerin yeterli düzeyde koruma sağlayan ülke olarak kabul edilip edilmediği sorunu ortaya çıkmaktadır. Greenleaf'e göre, uygulamada bu gibi ülkeler için spesifik bir yeterlilik kararı kabul etmeye gerek yoktur. Çünkü Sözleşme ve Ek Protokolün hükümleri birlikte gözden geçirildiğinde GDPR hükümlerine eşit düzeydedir. Dolayısıyla bu gibi ülkeler de facto yeterli ülkeler olarak kabul edilmelidir²⁵⁴. Fakat GDPR giriş bölümünde 108 sayılı Sözleşme ve Ek protokolün sadece yeterlilik kararı kabul edilirken dikkate alınacak kriterlerden biri olarak değerlendirileceği belirtilmiştir (para.105)²⁵⁵.

3. Yeterlilik Kararlarının Gözden Geçirilmesi

Koruma düzeyinin yeterliliğini değerlendirdikten sonra Komisyon, bir uygulayıcı işlem (*implementing act*) yoluyla, üçüncü ülkenin, söz konusu ülke içerisindeki bir bölge veya bir ya da daha fazla sayıda sektörün veya uluslararası bir kuruluşun, yukarıda bahsi geçen kriterler bağlamında koruma sağladığına karar verebilir (GDPR m.45/3). Üçüncü ülkelerdeki veya uluslararası kuruluşlardaki koruma düzeyi değerlendirilirken Kurul, kendi inisiyatifiyle veya Komisyon'un talebi üzerine görüşünü Komisyon'a sunar. Bu nedenle Komisyon, üçüncü ülkenin hükümeti ile yapılan yazışmalar da dâhil olmak üzere söz konusu üçüncü ülke veya uluslararası kuruluşla ilgili gerekli tüm belgeleri EDPB'ye sağlar (GDPR m.70/f.1/s).

95/46/EC sayılı DPD'den farklı olarak GDPR'da, yeterlilik kararlarının en az dört yılda bir olmak üzere, üçüncü ülkedeki veya uluslararası kuruluşdaki tüm ilgili

²⁵⁴ Graham Greenleaf, "The influence of European data privacy standards outside Europe: Implications for globalisation of Convention 108?", **International Data Privacy Law**, C. 2, S. 2, 2012, s. 14-15.

²⁵⁵ Bilgi Information Technology Law Institute, s. 42; Sertçe, s. 102.

gelişmeleri dikkate alan periyodik bir incelemeye tabi tutulması gerektiği öngörülmüştür (GDPR m.45/f.3). Komisyona’a böyle bir yükümlülüğün getirilmesi, ABAD’ın “Schrems I” kararının sonucunda ortaya çıkmıştır²⁵⁶. Şöyle ki, söz konusu kararda ABAD, üçüncü ülke tarafından sağlanan koruma düzeyinin değişebileceği gerçeğini göz önündü bulundurarak bu ülkeler hakkında yeterlilik kararlarının periyodik olarak gözden geçirilmesi gerektiğini ifade etmiştir²⁵⁷. Bu doğrultuda Komisyon, Aralık 2016’da Andorra, Arjantin, Kanada, Faroe Adaları, Guernsey, Man Adası, İsrail, Jersey, Yeni Zelanda, İsviçre ve Uruguay hakkında yeterlilik kararlarını değiştiren bir karar²⁵⁸ yayınlamıştır²⁵⁹. AB’nin Türkiye’ye ilişkin bir yeterlilik kararı ise henüz bulunmamaktadır.

Hükümde belirtilen süre, her üçüncü ülkeye veya uluslararası kuruluşu göre ayarlanması gereken genel bir zaman dilimidir. Başka bir deyişle, üçüncü ülke veya uluslararası kuruluşdaki somut şartlar göz önünde bulundurularak yeterlilik kararında daha erken bir incelemeye gidilebilir. Şöyle ki, Komisyon, 95/46/EC sayılı DPD kapsamında kabul edilenler de dâhil olmak üzere, herhangi bir yeterlilik kararının işleyişini etkileyebilecek üçüncü ülkelerdeki ve uluslararası kuruluşlardaki gelişmeleri sürekli olarak gözden geçirmektedir (GDPR m.45/f.4). Dolayısıyla, Komisyon, üçüncü ülkenin veya uluslararası bir kuruluşun artık yeterli düzeyde koruma sağlamadığını ortaya çıkardığı durumlarda kararını değiştirebilir, askıya alabilir veya yürürlükten kaldırabilir. Bu gibi kararların geriye dönük etkisi olmayacaktır (GDPR m.45/f.5). Yeterlilik kararlarının kabulü gibi değiştirilmesi, askıya alınması ve yürürlükten kaldırılması hakkında kararlar da Komisyon tarafından AB Resmî Gazetesi’nde ve internet sitesinde yayımlanır (GDPR m.45/f.8). Aynı zamanda Komisyon, problemin çözümü için üçüncü ülke veya uluslararası kuruluşlarla görüşmeler de yapabilir (GDPR m.45/f.6).

²⁵⁶ Sertçe, s. 22.

²⁵⁷ ABAD, C-362/14, par. 76.

²⁵⁸ Commission Implementing Decision (EU) 2016/2295 of 16 December 2016 amending Decisions 2000/518/EC, 2002/2/EC, 2003/490/EC, 2003/821/EC, 2004/411/EC, 2008/393/EC, 2010/146/EU, 2010/625/EU, 2011/61/EU and Implementing Decisions 2012/484/EU, 2013/65/EU on the adequate protection of personal data by certain countries, pursuant to Article 25(6) of Directive 95/46/EC of the European Parliament and of the Council, (çevrimiçi), <https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX%3A32016D2295>, 20.10.2021.

²⁵⁹ Sertçe, s. 29.

Hakkında yeterlilik kararı bulunan üçüncü ülkenin hukuku ve uygulamalarının yeterli koruma düzeyini temin etmediğine yönelik iddiaları inceleme yetkisi bulunan diğer kurum ise ABAD'dır. Bu yetki çerçevesinde ABAD “Schrems I”²⁶⁰ ve “Schrems II” kararlarında²⁶¹ AB ve ABD arasında veri transferini düzenleyen “Güvenli Liman” (*Safe Harbor*) ve “Gizlilik Kalkanı” (*Privacy Shield*) anlaşmalarının yeterli koruma düzeyini temin etmediğine karar vermiş ve adı geçen anlaşmaları yürürlükten kaldırmıştır²⁶². Şunu da belirtmek gerekir ki, bu madde kapsamında verilen yürürlükten kaldırma kararları, kişisel verilerin üçüncü ülkelere aktarılmasını tamamen engellemez, sadece yeterlilik kararına dayalı aktarımı ortadan kaldırır. Başka bir deyişle, veri sorumlusu veya veri işleyen tarafından sağlanan uygun önlemler veya madde 49'da öngörülen istisnai durumlara dayalı aktarımlara hâlel getirmez (GDPR m.45/f.7).

4. Tam ve Kısmi Yeterlilik Kararları

Komisyon bir ülke veya ülke içerisindeki bir bölgenin (örneğin, Danimarka'nın özerk bir parçası olan Faroe adaları) yeterli korumayı tamamen sağladığına dair karar (*tam yeterlilik kararı*) verebileceği gibi, sadece belirli bir sektör ile sınırlandırılmış *kısmi yeterlilik kararları* da verebilir²⁶³. Örneğin, Kanada hakkında yeterlilik kararında, bu kararın sadece ticari faaliyet sırasında kişisel verileri toplayan, kullanan veya aktaran özel kuruluşları kapsadığı belirtilmiştir. Kamu kuruluşları ve kâr amacı olmayan kuruluşlar, yeterlilik kararının kapsamı dışında kalmıştır²⁶⁴.

Yürürlükten kaldırılmış olan ABD yeterlilik kararları da kısmi nitelikte olmuştur²⁶⁵. Zira bütün ülkenin değil, sadece “Güvenli Liman” (daha sonra “Gizlilik

²⁶⁰ ABAD, C-362/14 sayılı ve 06.10.2015 tarihli kararı, (çevrimiçi), <https://curia.europa.eu/juris/document/document.jsf?text=&docid=169195&pageIndex=0&doclang=en&mode=lst&dir=&occ=first&part=1&cid=33793811>, 15.05.2021.

²⁶¹ ABAD, C-311/18 sayılı ve 16.07.2020 tarihli kararı, (çevrimiçi), <https://curia.europa.eu/juris/document/document.jsf?text=&docid=228677&pageIndex=0&doclang=en&mode=lst&dir=&occ=first&part=1&cid=33793324>, 15.05.2021.

²⁶² Giakoumopoulos/ Buttarelli/ O'Flaherty, **Handbook**, s. 254.

²⁶³ Kuner v.d., **Commentary**, s. 786; Bilgi Information Technology Law Institute, s. 74; Kızıllırmak, **Cross-Border Transfer**, s. 25-26; Sertçe, s. 14.

²⁶⁴ European Commission, 20.12.2001 tarihli ve 2002/2/EC sayılı karar, par. 5, (çevrimiçi), <https://eur-lex.europa.eu/legal-content/en/txt/pdf/?uri=celex:32002d0002&from=en>, 01.06.2021.

²⁶⁵ Roth, s. 62; Theodorakis, s. 3.

Kalkanı”) anlaşmasına uyum sağlamak için gönüllü olarak bu sisteme katılım sağlayan şirketlerin yeterli koruma sağladığına karar verilmiştir²⁶⁶. Bunun temel sebebi, ABD’de kişisel verileri koruma alanında genel bir federal kanunun bulunmaması, bunun yerine sadece spesifik sektörler için eyalet düzeyinde kanunlar ve kamu sektöründe kişisel verilerin korunmasını düzenleyen federal kanunun mevcut olmasıdır. Hem bütün ülke için geçerli federal düzeyde bir yasanın yürürlüğe konulmaması hem de bir veri koruma otoritesinin bulunmamasından dolayı ABD’nin, AB mevzuatında öngörülen yeterlilik kriterlerini karşılayamayacağı düşünülmüş ve bu nedenle hiçbir zaman ABD’li yetkililer tarafından yeterlilik tespiti için başvuru yapılmamıştır²⁶⁷. Fakat ABD, AB’nin en büyük ticari ortağı olarak kaldığı için, ABD’ye yapılan aktarımları gözardı etmek mümkün olmamıştır. Bu nedenle, 1998’den itibaren AB Komisyonu ve ABD Ticaret Bakanlığı, transatlantik veri aktarımları için alternatif bir çerçeve üzerinde görüşmelere başlamıştır. Bu kapsamda AB ve ABD arasında daha önce “Güvenli Liman”, daha sonra ise “Gizlilik Kalkanı” diye adlandırılan iki anlaşma imzalanmıştır.

Her iki anlaşma ABAD tarafından geçersiz kılınmış olsa da, uzun yıllar AB ve ABD arasında büyük bir veri trafiğinin hukuki temellerini oluşturduğu için bu çalışma kapsamında kısaca bahsedilecektir.

a. Avrupa Birliği ve ABD Arasında “Güvenli Liman” Anlaşması

İki yıl devam eden müzakerelerden sonra AB Komisyonu, 25 Temmuz 2000 yılında “Güvenli Liman” Anlaşması’nın son hâlini yayınlamış ve bu anlaşmaya dayanarak ABD’nin yeterli korumayı sağladığına kanaat getirmiştir²⁶⁸.

“Güvenli Liman” Anlaşması, belirli ilkelere uyum sağlamayı taahhüt eden ABD şirketlerinin, 95/46/EC sayılı DPD’yi ihlal etme riski olmaksızın AB menşeli verileri transfer etmesine izin veren bir mekanizma sunmuştur²⁶⁹. Bir self-regülasyon

²⁶⁶ European Commission, 26.07.2000 tarihli ve 2000/520/EC sayılı karar, par. 5, (çevrimiçi), <https://eur-lex.europa.eu/legal-content/en/txt/pdf/?uri=celex:32000d0520&from=en>, 01.06.2021.

²⁶⁷ Hon, s. 162; Toparlak, s. 32-33.

²⁶⁸ European Commission, 26.07.2000 tarihli ve 2000/520/EC sayılı karar, (çevrimiçi), <https://eur-lex.europa.eu/legal-content/en/txt/pdf/?uri=celex:32000d0520&from=en>, 06.06.2021.

²⁶⁹ İkbâl Gür, **Kişisel Verilerin Korunması Hususunda AB İle ABD Arasında Çıkan Uyuşmazlıklar ve Çözüm Yolları**, Ankara, Turhan Kitabevi, 2010, s. 166; Kuner, **Reality and Illusion**, s. 886.

sistemi olan “Güvenli Liman”ın işleyişinden ABD Ticaret Bakanlığı sorumlu tutulmuştur²⁷⁰. Şöyle ki, ABD şirketlerinin AB nezdinde yeterli korumayı sağladığının kabul edilmesi, söz konusu şirketlerin AB menşeli kişisel verileri işlerken anlaşmada öngörülen prensiplere bağlı kalacaklarını taahhüt ederek ABD Ticaret Bakanlığından alınan lisansa bağlı kılınmıştır²⁷¹.

“Güvenli Liman” Anlaşması temel olarak OECD’nin rehber ilkelerini baz alarak hazırlanan yedi prensipden (bildirim, seçim, ileriye yönelik aktarım, veri güvenliği, veri bütünlüğü, erişim, uygulama) oluşmuştur. Buna göre, AB’den veri aktarımı gerçekleştirecek olan ABD şirketlerinin; aktarılabilecek verilerin hangi amaçla toplandığına dair veri sahiplerini bilgilendirmek, veri sahiplerinin rızası bulunmadıkça bu verileri üçüncü kişilerle paylaşmamak, bildirim ve seçim şartı yerine getirilmiş olsa bile bu verileri aynı düzeyde koruma sağlamayan üçüncü kişilere aktarmamak, verilerin güvenliği ve sadece toplanma amaçları ile uyumlu bir şekilde işlenmeleri için uygun önlemler almak, veri sahiplerine kendi verilerine erişim imkânı sağlamak, veri sahiplerinin şikâyetlerini çözmek üzere bağımsız mekanizmalar geliştirmek gibi yükümlülükleri bulunmaktadır.

Söz konusu prensiplere katılım gönüllü olsa da, şirketler bu prensiplere bir kere katıldıktan sonra hatta “Güvenli Liman” sisteminden ayrılırlar bile sisteme dâhil oldukları süre içerisinde işlenen veriler için bu prensiplere uyum sağlamaları zorunlu kılınmıştır²⁷².

Söz konusu ilkelere uyum katılımcı şirketler için zorunlu olsa da, bu ilkelere uyumun; a) ulusal güvenlik, kamu yararı veya kanun uygulama gerekliliklerini karşılamak için gerekli olduğu ölçüde; b) ilkelere uyumsuzluğun, öncelikli meşru menfaatleri karşılamak için gerekli olan kapsamla sınırlı olduğu kanıtlanabildiği halde, kanun, hükûmet düzenlemesi veya içtihatla c) üye devletlerin hukukunun bu tür istisnalara izin verdiği durumlarda sınırlandırılabilmesi öngörülmüştür.

²⁷⁰ Kama Işık, s. 126.

²⁷¹ Gür, s. 166; Sertçe, s. 26.

²⁷² Gür, s. 166.

Her ne kadar “Güvenli Liman” ABD merkezli şirketlerin AB’den veri akışını gerçekleştirebilmesi için elverişli bir araç olsa da, sistemin uygulanmasına ve etkin olmasına dair tartışmalar her zaman mevcut olmuştur²⁷³. Bu tartışmalar, 2013 yılında ABD Ulusal Güvenlik Ajansı (NSA) çalışanı Edward Snowden tarafından NSA’nın kişisel verilere usulsüzce erişimini ifşa eden bazı belgelerin basına sızdırılmasını müteakiben daha da şiddetlenmiştir. Sızdırılan bazı belgelere göre NSA; Microsoft, Yahoo, Google, Facebook, Paltalk, AOL, Skype, YouTube, Apple gibi ABD hizmet sağlayıcılarının sunucularına doğrudan erişimi bulunan PRISM ve UPSTREAM adında programlar aracılığıyla e-postalar, sohbet görüşmeleri, sesli aramalar, belgeler ve daha fazla kayıtlara erişebilmekteydi. NSA’nın verilere müdahalesi AB’de eleştirilere sebep olmuş ve ABD’nin ulusal güvenlik mevzuatıyla ilgili inceleme başlatılmıştır. Altı ay devam eden inceleme sonucunda Mart 2014 tarihinde Avrupa Parlamentosu, ABD’ye yapılan veri aktarımlarının derhâl durdurulması yönünde karar kabul etmiştir²⁷⁴.

ABD’nin verilere aşırı ve ölçsüz müdahalede bulunmasına karşı hukuki mücadele, aslında Snowden’in ifşalarından çok daha önce zaten başlatılmıştı. Şöyle ki, henüz 2011 yılında Avusturya’lı bir hukuk öğrencisi olan Maximillian Schrems tarafından Facebook’un gizlilik politikasına karşı kâr amacı gütmeyen bir kuruluş oluşturulmuşur²⁷⁵. AB’de ikamet eden ve Facebook kullanan herkesin kişisel verileri, ABD’de bulunan Facebook’a ait sunuculara “Facebook Ireland” adlı bir yan kuruluş aracılığıyla aktarıldığı için, 2013 yılına kadar Schrems’in kurduğu şirket Facebook’a karşı İrlanda Veri Koruma Komiseri’ne 20’den fazla şikâyetle bulunmuştur. Snowden’in ifşalarından günler sonra ise 25 Haziran 2013 tarihinde Schrems, İrlanda Veri Koruma Komiseri’ne yeni bir şikâyetle bulunarak, Komiser’den Facebook’un kişisel verileri NSA’ya yönlendirme sebebinin ulusal

²⁷³ Küzeci, s. 203.

²⁷⁴ European Parliament, US NSA: stop mass surveillance now or face consequences, MEPs say, 12.03.2014, (çevrimiçi), <https://www.europarl.europa.eu/news/en/press-room/20140307IPR38203/us-nsa-stop-mass-surveillance-now-or-face-consequences-meps-say>, 12.07.2021.

²⁷⁵ Mary Ellen McIntire, “How a Law Seminar Inspired a Student to Bring a Case to Europe’s Top Court”, 07.10.2015, (çevrimiçi), <https://www.chronicle.com/article/how-a-law-seminar-inspired-a-student-to-bring-a-case-to-europes-top-court/>, 15.07.2021; Robert Levine, “Behind the European Privacy Ruling That’s Confounding Silicon Valley”, 09.10.2015, (çevrimiçi), <https://www.nytimes.com/2015/10/11/business/international/behind-the-european-privacy-ruling-thats-confounding-silicon-valley.html>, 15.07.2021.

güvenlik mi yoksa NSA ile Facebook arasında gönüllü bir işbirliği mi olup olmadığını araştırmasını talep etmiştir²⁷⁶.

Schrems, şikâyetinde Snowden'in sızdırdığı belgelere atıfta bulunarak, ABD'de bulunan kişisel verileri kamu müdahalesinden koruyan yeterli korumanın bulunmadığını iddia etmiştir. Aynı zamanda, Facebook kişisel veri aktarımı için "Güvenli Liman"ı kullandığından, "Güvenli Liman"ın ulusal güvenlik muafiyetinin 95/46/EC sayılı DPD ve AB Temel Haklar Şartı (CFR)²⁷⁷ ile uyumlu olup olmadığını sorgulayarak, "Güvenli Liman" Anlaşması'nın geçerliliğinin yeniden gözden geçirilmesini talep etmiştir²⁷⁸. Veri Koruma Komiseri ise, "Güvenli Liman"ın yeterli korumayı sağladığının Komisyon Kararı ile onaylandığını ve bu kararın, ulusal makamlar tarafından veri aktarımlarının bağımsız olarak incelenmesini engellediğini ve Schrems'in kendi verilerine erişildiğine dair hiçbir kanıt sunmadığını öne sürerek bu şikâyeti reddetmiştir²⁷⁹.

Şikâyetinin reddedilmesi üzerine Schrems, İrlanda Yüksek Mahkemesi'ne başvuruda bulunmuş ve şikâyetinin araştırılmasını talep etmiştir²⁸⁰. Yüksek Mahkeme; Komisyonun kabul ettiği yeterlik kararından sonra CFR'nin yürürlüğe girmesini, sosyal medyanın gelişmesini ve Snowden tarafından sızdırılan belgelere göre ABD güvenlik kuruluşlarının verilere orantısız müdahalede bulunduğunu öne sürerek ABAD'a başvuruda bulunmuştur. İrlanda Yüksek Mahkemesi, yaptığı başvuruda 1) Komisyon'un "Güvenli Liman" kararından sonra, hâlâ ulusal denetim makamlarının, AB ve ABD arasında veri aktarımlarını incelemesine izin verilip verilmediği ve 2) "Güvenli Liman" Anlaşması'nın, CFR m.7, 8 ve 47 ile güvence

²⁷⁶ Pelen, s. 1737.

²⁷⁷ Charter of Fundamental Rights of the European Union, 02.10.2000, (çevrimiçi), https://www.europarl.europa.eu/charter/pdf/text_en.pdf, 23.09.2021.

²⁷⁸ Marcelo Corrales Compagnucci/ Mateo Aboy/ Timo Minssen, "Cross-Border Transfers of Personal Data after Schrems II: Supplementary Measures and New Standard Contractual Clauses (SCCs)", 27.10.2021, s. 4, (çevrimiçi), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3951085, 25.12.2021; Complaint against Facebook Ireland Ltd, (çevrimiçi), <http://www.europe-v-facebook.org/prism/facebook.pdf>, 22.09.2021.

²⁷⁹ The High Court Judicial Review, Record No. 2013/ 765 JR, (çevrimiçi), http://europe-v-facebook.org/JR_First_Response_DPC.pdf, 22.09.2021.

²⁸⁰ The High Court Judicial Review, Record No. 2013/ 765 JR, (çevrimiçi), http://europe-v-facebook.org/JR_Grounding_Documents.pdf, 22.09.2021.

altına alınan temel hakları ihlal edip etmediğine dair sorulara cevap verilmesini istemiştir²⁸¹.

ABAD, herhangi bir üçüncü ülke ile ilgili Komisyon'un yeterlilik kararının, ulusal denetim makamlarının yetkilerini azaltamayacağını veya ortadan kaldıramayacağını öne sürerek ulusal denetim makamlarının, AB'den üçüncü ülkeye yapılan aktarımın Yönerge hükümlerine uyumlu olup olmadığını kontrol etme yetkisine sahip olduğuna hükmetmiştir²⁸². Bununla beraber, ulusal mahkemeler ve denetim makamları bir Komisyon kararının geçerliliğini denetleme yetkisine sahip olsa da, sadece ABAD'ın, Komisyon kararını geçersiz kılma yetkisine sahip olduğuna vurgu yapılmıştır²⁸³.

ABAD; ulusal güvenlik, kamu yararı gibi genelleştirilmiş gerekçelerle kamu kurumlarının verilere müdahalesini mümkün kılan düzenlemenin, AB vatandaşlarının temel hak ve özgürlüklerini ihlal ettiği yönünde karar vermiştir. Şöyle ki ABAD, ABD istihbarat servislerinin aktarılan verilere gereğinden fazla ve aktarılma amaçlarıyla uyumsuz bir şekilde erişim sağladığını ve bu tür müdahaleye karşı AB vatandaşlarının temel hak ve özgürlüklerini korumak için herhangi etkili hukuki çözüm bulunmadığını öne sürerek "Güvenli Liman" Anlaşması'nın geçersiz olduğuna hükmetmiştir²⁸⁴.

b. Avrupa Birliği ve ABD Arasında "Gizlilik Kalkanı" Anlaşması

Henüz "Güvenli Liman" Anlaşması ABAD tarafından iptal edilmeden önce Komisyon, Snowden'in etkisiyle anlaşmanın güvenilirliğini kaybetmesini dikkate alarak "Güvenli Liman"ı güçlendirmek için çalışmalara başlamış ve bu doğrultuda 13 tavsiye kabul etmiştir²⁸⁵. Bunun üzerine Komisyon ve ABD Ticaret Bakanlığı

²⁸¹ ABAD, C-362/14, par. 35.

²⁸² ABAD, C-362/14, par. 54-57.

²⁸³ ABAD, C-362/14, par. 61-62.

²⁸⁴ ABAD, C-362/14, par. 67.

²⁸⁵ Dülger/ Kahraman, **GDPR ve KVKK Ekseninde**, s. 70; European Commission, Communication from the Commission to the European Parliament and the Council on the Functioning of the Safe Harbour from the Perspective of EU Citizens and Companies Established in the EU, Brussels, 27.11.2013, s. 18-19, (çevrimiçi), <https://eur-lex.europa.eu/legal-content/en/txt/?uri=celex%3a52013dc0847>, 20.08.2021.

arasında müzakereler başlamış ve “Güvenli Liman” Anlaşması’nın yerine geçen “Gizlilik Kalkanı” anlaşmasının kabul edilmesiyle sonuçlanmıştır.

29 Şubat 2016 tarihinde Komisyon, “Gizlilik Kalkanı” Anlaşmasıyla ilgili taslak karar²⁸⁶ ve destekleyici belgeleri yayınlaması üzerine, Madde 29 Çalışma Grubu, 14 Nisan tarihinde yayınladığı raporla “Gizlilik Kalkanı” Anlaşması’nın, Schrems davasındaki eksikleri tam olarak ortadan kaldırmadığına kanaat getirmiştir²⁸⁷. Eleştiriler üzerine revize edilen anlaşmanın son hâli, 12 Temmuz 2016 tarihinde Komisyon tarafından kabul edilmiştir.

Temel olarak “Güvenli Liman” prensiplerinin devamı olarak kabul edilse de “Gizlilik Kalkanı” Anlaşması, AB vatandaşlarının bireysel hakları üzerine daha fazla yoğunlaşmış ve veri aktarımı gerçekleştirecek ABD şirketleri için daha sert yükümlülükler belirlemiştir²⁸⁸. İki anlaşma arasındaki farklar, kişisel veri aktarımlarının doğasını değiştirecek nitelikte olmasa da, aktarımdan kaynaklanabilecek sorunların çözüm yöntemleri açısından yenilikler göze çarpmaktadır.

Önemli değişikliklerden biri üçüncü kişilere yapılan aktarımlarla (ileri aktarımlar) ilgilidir. Şöyle ki, bir önceki anlaşmaya göre, kişisel verileri üçüncü tarafa aktarmak isteyen şirketin, sadece bildirim ve seçim ilkelerine riayet etmesi şartı arandığı halde, yeni anlaşma ile aynı zamanda amaç sınırlandırması ilkesine de uyması, üçüncü tarafın ise “Gizlilik Kalkanı” ile sağlanan koruma düzeyi ile aynı düzeyde koruma sağlaması şartı aranmıştır. Ayrıca bu gereksinimler karşılanmış olsa bile kişisel veriler, “Gizlilik Kalkanı” ilkeleriyle uyumlu bir şekilde işlenmemişse üçüncü taraf, kişisel verilere zarar veren herhangi olaydan sorumlu olmadığını kanıtlamadığı müddetçe aktarımı gerçekleştiren şirketin hukuki sorumluluğu devam edecektir.

²⁸⁶ European Commission, “Restoring trust in transatlantic data flows through strong safeguards: European Commission presents EU-U.S. Privacy Shield”, 29.02.2016, (çevrimiçi), https://ec.europa.eu/commission/presscorner/detail/en/IP_16_433, 20.09.2021.

²⁸⁷ Article 29 Data Protection Working Party, Opinion 01/2016 on the EU – U.S. Privacy Shield Draft Adequacy Decision, 13.04.2016, (çevrimiçi), <https://ec.europa.eu/newsroom/article29/items/640157>, 25.09.2021.

²⁸⁸ Kama Işık, s. 160.

“Gizlilik Kalkanı” ile veri sahiplerine, birkaç farklı şikâyet mekanizması sunulmuştur. Bunlara; doğrudan şirketin kendisine başvuru, bağımsız bir üçüncü tarafça sağlanan alternatif çözüm yolu (arabuluculuk), AB veri koruma otoritelerine başvuru ve bu mekanizmalar tüketildikten sonra tahkim yolu dâhildir²⁸⁹. Ayrıca, “Gizlilik Kalkanı” ile ilk kez veri sahiplerinin şikâyet ve soruşturmalarını takip etmek ABD istihbarat servislerinden tam bağımsız Ombudsman’ın atanması öngörülmüştür²⁹⁰.

Bir diğer yenilik ise ilk kez ABD hükümeti tarafından anlaşmanın nasıl uygulanacağına dair bir dizi yazılı güvenceler ibraz edilmesidir. Bunlara kamu kurumlarının verilere erişimine uygulanacak sınırlandırmalar ve güvenlik önlemlerine dair taahhütnameler dâhildir. Aynı zamanda sertifika almış şirketlerden yılda bir kez gizlilik politikalarını ABD Ticaret Bakanlığına ibraz ederek sertifikalarını yenilemeleri istenmiştir.

ABAD’ın 6 Ekim 2015 tarihli ve C-362/14 sayılı (“Schrems I”) kararını müteakiben İrlanda Yüksek Mahkemesi, Schrems tarafından yapılan şikâyetin İrlanda Veri Koruma Komiseri tarafından reddedilmesine dair kararı iptal etmiş ve bu kararı Komiser’e geri göndermiştir. Bunun üzerine Komiser bir soruşturma başlatmış ve sonuçta “Güvenli Liman”ın iptalinden sonra Facebook Ireland şirketinin, kişisel verilerin büyük bir kısmının Facebook Inc.’e aktarmak için Komisyon’un standart sözleşme hükümleri ile ilgili kararını kullanmaya başladığı ortaya çıkmıştır²⁹¹. Bu yüzden Schrems’ten şikâyetini bu temelde yeniden formüle etmesi talep edilmiştir²⁹².

1 Aralık 2015 tarihinde Schrems, yeniden düzenlenmiş şikâyetinde Facebook Inc.’in, AB’den aktarılan kişisel verilere çeşitli izleme programları vasıtasıyla NSA ve FBI gibi istihbarat makamlarının erişimine izin verdiğini ve bu erişimin CFR’in 7, 8 ve 47. maddelerini ihlal edecek nitelikte olduğunu, bu nedenle Facebook Inc.’e

²⁸⁹ Bilgi Information Technology Law Institute, s. 77.

²⁹⁰ Sertçe, s. 31.

²⁹¹ Compagnucci/ Aboy/ Minssen, s. 4-5.

²⁹² ABAD, C-311/18, par. 54 .

yapılan aktarımların yasaklanmasını veya askıya alınmasını talep etmiştir²⁹³. Bu şikâyetle ilgili İrlanda Veri Koruma Komiseri, 24 Mayıs 2016 tarihinde yayınladığı taslak kararında²⁹⁴ ABD’ye aktarılan AB vatandaşlarının kişisel verilerine erişimin Şart’ın 7 ve 8. maddelerini ihlal ettiğini ve bu ihlale karşılık herhangi bir etkili hukuki çözüm mekanizması bulunmadığını, ayrıca standart sözleşme hükümlerinin bu kusuru giderecek yeterlilikte olmadığını da ifade etmiştir. Zira standart hükümler, sözleşmesel niteliğinden dolayı sözleşmeye taraf olmayan ABD kamu makamları açısından bağlayıcı değildir. Başka bir deyişle standart sözleşme hükümleri, veri sahibine yalnızca veri aktaran ve veri alıcısına karşı haklar sağlamaktadır²⁹⁵.

Bundan sonra Schrems, 31 Mayıs 2016 tarihinde şikâyetine standart sözleşme hükümleri ile ilgili Komisyon kararının geçerliliğine dair hususu da ekleyerek İrlanda Veri Koruma Komiseri’ne sunmuştur. “Schrems I” kararında da belirtildiği üzere ulusal denetim makamlarının, bir Komisyon kararının geçerliliğini denetlemek yetkisi bulunsa da, sadece ABAD böyle bir kararın geçersizliğine hükmetmek yetkisini haizdir²⁹⁶. Bu nedenle Komiser, standart sözleşme hükümleriyle ilgili Komisyon kararının geçerli olup olmadığına dair meseleyi ABAD’a taşıması için İrlanda Yüksek Mahkemesi önünde dava açmıştır²⁹⁷.

Yüksek Mahkeme de konuyla ilgili görüşünü sunarken ABD yasalarının, CFR m.7 ve m.8. ile sağlanan korumaya eşdeğer bir koruma sağlamadığını, ayrıca AB vatandaşlarının ABD vatandaşlarıyla aynı hukuki koruma hakkının bulunmadığını, Ombudsmanın ise madde 47 anlamında değerlendirilecek bir merci olmadığını ifade etmiştir²⁹⁸. Bu durumda Yüksek Mahkeme 12 Nisan 2018 tarihinde, özetle standart sözleşme hükümlerinin geçerli olup olmadığı ve bu hükümlerin CFR’nin 7, 8 ve 47. maddelerini ihlal edip etmediğini cevaplaması için ABAD’a başvuruda bulunmuştur.

²⁹³ ABAD, C-311/18, par. 55.

²⁹⁴ Draft Decision of the Data Protection Commissioner under Section 10(1)(b)(ii) of the Data Protection Acts, 1988 & 2003, (çevrimiçi), <https://epic.org/privacy/intl/schrems/20160524-dpc-draft-decision.pdf>, 28.08.2021.

²⁹⁵ ABAD, C-311/18, par. 56.

²⁹⁶ ABAD, C-362/14, par. 62.

²⁹⁷ Kuner, **Reality and Illusions**, s. 884.

²⁹⁸ ABAD, C-362/14, par. 65.

ABAD, standart sözleşme hükümlerine dair Komisyon kararının geçerliliğini etkileyecek bir sebep bulunmadığına karar vermiştir²⁹⁹. Mahkeme, yeterlilik kararından farklı olarak standart sözleşme hükümlerinin, herhangi üçüncü bir ülkenin tamamı ile ilgili olmadığı ve bu yüzden de Komisyon'un bu tür bir karar kabul etmeden önce üçüncü ülkelerdeki veri koruma düzeyini değerlendirme gibi bir yükümlülüğünün bulunmadığına vurgu yapmıştır³⁰⁰. Bu nedenle mahkeme, bu hükümlere dayalı olarak gerçekleştirilecek veri aktarımları için daha sıkı kurallar belirlemiştir. Şöyle ki, standart sözleşme hükümleri kapsamında aktarım gerçekleştirecek olan veri aktaran, verilerin aktarılacağı ülkenin mevzuatını her transfer için ayrıca değerlendirmeli³⁰¹ ve sözleşme hükümlerinin, yeterli korumayı temin edemeyeceği durumlarda ek önlemler almalıdır³⁰².

Her ne kadar Schrems'in talepleri standart sözleşme hükümlerinin geçerliliğiyle ilgili olsa da ve "Gizlilik Kalkanı" Anlaşması'nın geçersizliğine hükmedilmesiyle ilgili bir talebi bulunmasa da ABAD, İrlanda Yüksek Mahkemesi'nin sorularını cevaplarken "Gizlilik Kalkanı" Anlaşması'nın da geçerliliğinin incelenmesine karar vermiştir.

ABAD, "Gizlilik Kalkanı" Anlaşması'nın ulusal güvenlik, kamu yararı gibi gerekçelerle sınırlandırmalara tabi tutulabileceğini öngören Ek II 1(5) maddesini değerlendirirken bu düzenlemenin, ABD kamu kurumlarının AB vatandaşlarının verilerine erişimi için imkân oluşturduğuna kanaat getirmiştir³⁰³. Kişisel verilere erişim kendi başına bir ihlal teşkil etmese de, sorun bu erişimin niteliğinden kaynaklanmaktadır. Şöyle ki Mahkeme; 1) ABD kanunları ile bu erişime kaşılık herhangi bir sınırlandırma veya güvenlik önlemleri öngörülmediğini, 2) ABD tarafından kişisel verilerine müdahale edilen AB vatandaşlarının bir ABD mahkemesine başvuramayacağını ve 3) Ombudsman'ın, CFR m.47 kapsamında "mahkeme" standartını karşılamadığını öne sürerek AB vatandaşlarının temel

²⁹⁹ ABAD, C-362/14, par. 149.

³⁰⁰ ABAD, C-362/14, par. 130-132.

³⁰¹ ABAD, C-362/14, par. 134.

³⁰² ABAD, C-362/14, par. 133.

³⁰³ ABAD, C-362/14, par. 165.

haklarının (CFR m.7, 8 ve 47) ihlal edildiğine karar vermiş³⁰⁴ ve bu bulgular ışığında “Gizlilik Kalkanı” Anlaşması’nın geçersiz olduğuna hükmetmiştir³⁰⁵.

“Gizlilik Kalkanı” Anlaşması’nın iptal edilmesiyle birlikte serbestçe veri aktarma imkânından mahrum kalan ABD şirketleri, bunun için daha maliyetli olan alternatif yöntemler kullanmak zorunda kalmıştır. Bu nedenle ABAD’ın kararının hemen ardından ABD ile AB arasında veri aktarımlarını düzenleyen yeni anlaşmanın ihdas edilmesine dair müzakereler başlamıştır³⁰⁶. Uzun bir süreden sonra ilk kez 25 Mart 2022 tarihinde bu doğrultuda bir duyuru yayımlanmıştır. Duyuru metninde AB ve ABD’nin kişisel veri aktarımlarına ilişkin yeni “Trans Atlantik Veri Gizliliği Çerçevesi” üzerinde prensipte anlaştıkları belirtilmiştir³⁰⁷. AB’den ABD’ye kişisel verilerin aktarımı için yasal bir mekanizmanın yeniden tesis edildiği bu anlaşma ile ABAD’ın “Schrems II” kararında ifade ettiği veri güvenliğine ilişkin endişelerinin giderileceği ifade edilmiştir³⁰⁸. Şöyle ki, bu anlaşma çerçevesinde ABD’nin daha önceki anlaşmalarda yer verilmeyen taahhütlerde bulunduğu belirtilmiştir. Bu doğrultuda ABD; elektronik istihbarat faaliyetlerini yönetirken mahremiyet ve temel hakların korunmasına ilişkin tutumunu güçlendirecek, bağımsız ve bağlayıcı yetkiye sahip yeni bir tazminat mekanizması kuracak, elektronik istihbarat faaliyetlerine ilişkin mevcut titiz ve katmanlı gözetimini geliştirecektir³⁰⁹. Bu çalışmanın yapıldığı tarih itibarıyla Trans Atlantik Veri Gizliliği Çerçevesi’nin hukuku metninin oluşturulması üzerine AB ve ABD arasında işbirliği devam etmektedir.

C. Uygun Önlemlerin Alınması Kaydıyla Aktarılma

Yukarıda da belirtildiği üzere, bugüne kadar az sayıda ülke hakkında yeterlilik kararı çıkarılmıştır. Bunun temel sebebi bu sürecin çok uzun sürmesi ve

³⁰⁴ ABAD, C-362/14, par. 168, 181.

³⁰⁵ ABAD, C-362/14, par. 201.

³⁰⁶ Sertçe, s. 37.

³⁰⁷ European Commission, “European Commission and United States Joint Statement on Trans-Atlantic Data Privacy Framework”, 25.03.2022, (çevrimiçi), https://ec.europa.eu/commission/presscorner/detail/en/ip_22_2087, 20.04.2022.

³⁰⁸ White House, “Fact Sheet: United States and European Commission Announce Trans-Atlantic Data Privacy Framework”, 25.03.2022, (çevrimiçi), <https://www.whitehouse.gov/briefing-room/statements-releases/2022/03/25/fact-sheet-united-states-and-european-commission-announce-trans-atlantic-data-privacy-framework/>, 20.04.2022.

³⁰⁹ White House, Trans-Atlantic Data Privacy Framework.

yeteri kadar pratik olmamasıdır. Fakat bu, AB'nin söz konusu ülkeler dışında kalan ülkelere veri aktarımı gerçekleştirmede anlamına gelmemelidir. Zira bu gibi durumlar, AB hukukunda kişisel verilerin aktarılması için alternatif yolların geliştirilmesini tetiklemiştir³¹⁰. Yeterlilik kararı bulunmayan üçüncü ülkelere veya uluslararası kuruluşlara veri aktarımı gerçekleştirmek isteyen veri sorumlusu veya veri işleyen, bu ülkelerdeki veri koruma eksikliğini telafi etmek için güvenlik önlemleri almalıdır³¹¹. Ancak GDPR m.46'da öngörülen bu önlemlerden birinin sağlanmış olması hâlinde ve uygulanabilir veri sahibi hakları ve veri sahiplerine yönelik etkili kanun yollarının mevcut olması koşuluyla yeterlilik kararı bulunmayan üçüncü ülkeye aktarım gerçekleştirilebilir (GDPR m.46.1). ABAD'ın "Schrems II" kararında, uygun güvenlik önlemlerinin de yeterlilik kararları gibi "temelde eşdeğer" düzeyde koruma sağlaması gerektiği belirtilmiştir³¹².

Uygun güvenlik önlemlerini almak için, GDPR m.46'da "denetim makamının spesifik iznine gerek olmayan" ve "denetim makamının iznine tabi" mekanizmalar öngörülmüştür. Buna göre, uygun güvenceler bir denetim makamından spesifik bir izin alınmasına gerek olmaksızın aşağıdakilerle sağlanabilir (m.46/2):

- kamu kuruluşları veya organları arasında yasal bağlayıcılığı bulunan ve uygulanabilir bir belge;
- bağlayıcı şirket kuralları;
- Komisyon tarafından kabul edilen standart veri koruma hükümleri;
- denetim makamı tarafından kabul edilen ve Komisyon tarafından onaylanan standart veri koruma hükümleri;
- onaylanmış davranış kuralları;
- onaylanmış belgelendirme mekanizması.

Uygun güvenlik önlemleri, yetkili denetim makamından alınan izne tabi olarak aşağıdakilerle de sağlanabilir (m.46/f.3):

³¹⁰ Theodorakis, s. 26; Sertçe, s. 38.

³¹¹ Çelik, s. 123.

³¹² ABAD, C- 311/18, par. 105.

- veri sorumlusu veya veri işleyen ile üçüncü ülke veya uluslararası kuruluştaki veri sorumlusu veya veri işleyen arasındaki sözleşme maddeleri;
- kamu kuruluşları ya da organları arasındaki idari düzenlemelere eklenecek olan uygulanabilir ve etkili veri sahibi haklarını kapsayan hükümler.

1. Kamu Kuruluşları Arasında Yasal Bağlayıcılığı Bulunan Belge veya İdari Düzenlemelere Eklenecek Hükümler

Veri aktaran kamu kurumu, yeterli korumanın bulunmadığı üçüncü ülkede bulunan başka bir kamu kurumuna kişisel veri aktarımı gerçekleştirecekse her iki kamu kurumu yasal olarak bağlayıcı ve icra edilebilir bir sözleşme veya başka bir belge (*a legally binding and enforceable instrument between public authorities or bodies*) imzalamak suretiyle, sınırlı bir aktarım yapabilirler (GDPR m.46/f.2/a). Bu tür sözleşmeler için aranan en önemli şart, kişisel verileri aktarılan veri sahipleri için uygulanabilir haklar ve etkin hukuki çözüm yöntemleri içermesidir.

Şu noktada belirtmek gerekir ki GDPR m.2/f.2/d uyarınca, kamu güvenliğine yönelik tehditlere karşı güvence sağlanması, suçların önlenmesi, soruşturulması, tespiti veya kovuşturulması ya da cezaların infaz edilmesiyle ilgili olarak yetkili makamlar tarafından kişisel verilerin işlenmesi GDPR'ın kapsamı dışındadır. Zira bu hususlar 2016/680/EU sayılı Yönerge ile düzenlendiğinden kamu kurumları arasındaki kişisel veri aktarımlarına dair sözleşmelere konu edilemez. Ayrıca veri aktaran ve veri alıcısı özel bir kuruluş veya bir gerçek kişi ise, bu durumda söz konusu düzenlemenin, kişisel veri aktarımına hukuki dayanak teşkil etmesi mümkün olmayacaktır³¹³.

Veri aktaran veya veri alıcısı kamu kuruluşlarından herhangi biri, yasal olarak bağlayıcı ve uygulanabilir sözleşme yapmak yetkisini haiz değilse, GDPR m.46/f.3/b'de öngörülen düzenlemeyi de alternatif olarak kullanabilirler³¹⁴. Şöyle ki m.46/f.3/b uyarınca kamu kuruluşları veya organları, kendi aralarındaki idari

³¹³ European Ddata Protection Board, Guidelines 2/2020 on Articles 46 (2) (a) and 46 (3) (b) of Regulation 2016/679 for Transfers of Personal Data between EEA and non-EEA Public Authorities and Bodies, 18.01.2020, par. 4, s. 4, (çevrimiçi) https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-22020-articles-46-2-and-46-3-b-regulation_en, 15.09.2021.

³¹⁴ Bilgi Information Technology Law Institute, s. 84.

düzenlemelere aktarıma ilişkin hükümler eklemek kaydıyla kişisel verilerin aktarımına hukuki bir dayanak oluşturabilirler. Taraflar arasında yasal bağlayıcılığı olmayan herhangi düzenleme, (örneğin, mutabakat zabtı) idari düzenleme olarak gözden geçirilebilir (GDPR Giriş bölümü par. 108). Bu hükümlerin uygulanabilir ve etkili veri sahibi haklarını içermesi gerekmektedir. Kamu kurumları arasında yasal bağlayıcılığı olan ve uygulanabilir belgeye dayalı veri aktarımları için yetkili denetim makamından onay alınmasına şartı aranmasa da (m.46/f.2/1), kamu kuruluşları arasındaki idari düzenlemelerin, gerçekleştirilecek aktarımlar için hukuki bir dayanak teşkil edebilmesi için önceden yetkili denetim makamının onayının alınması şarttır (GDPR m.46/f.3). Aktarımın, birden fazla AB ülkesinden yapılacağı takdirde ilgili denetim makamının yanı sıra, EDPB'nin³¹⁵ de görüşü ve onayı alınmalıdır³¹⁶.

Yetkili denetim makamı, onay vermeden önce veri işlemenin amacı ve aktarılacak olan verilerin niteliği göz önünde bulundurularak kamu sektöründe yeterli koruma sağlamak için yasal olarak bağlayıcı olmayan idari düzenlemelerden yararlanılıp yararlanılmayacağını değerlendirmelidir. Veri sahipleri için veri koruma hakları ve tazminat, üçüncü ülkenin iç hukukunda öngörülmemişse, yasal olarak bağlayıcı bir anlaşma yapılması tercih edilmelidir. Kabul edilen düzenlemenin türüne bakılmaksızın, alınan önlemlerin uygun uygulama, yaptırım ve denetimi sağlamak için etkili olması gerekmektedir³¹⁷. Şöyle ki, ya veri alıcısı olan kamu kurumu, veri sahibi haklarının iç hukukla tamamen sağlandığını ve veri sahiplerinin, vatandaşlar için öngörülen aynı koşullarda bu haklardan yararlanabileceğini göstermeli ya da belirli taahhütlerle ve ihlal edilen hakların tazmin edilmesi için öngörülen mekanizmalarla birlikte güvence sağlamalıdır³¹⁸. Aktarımdan kaynaklanan ihtilafların ve iddiaların dostane çözümünün mümkün olmadığı durumlar için, tahkim veya arabuluculuk gibi alternatif mekanizmalar da sağlanmalıdır³¹⁹. Şunu da

³¹⁵ 2018 yılında Madde 29 Çalışma Grubu'nun yerini alan Avrupa Veri Koruma Kurulu, esas amacı GDPR'ın istikrarlı bir şekilde uygulanmasını ve üye ülkelerin veri koruma otoriteleri arasında işbirliğini sağlamaktan ibaret olan bağımsız bir AB kurumudur.

³¹⁶ Bilgi Information Technology Law Institute, s. 28.

³¹⁷ EDPB, **Guidelines on articles 46/2a and 46/3b**, par. 67, s. 14.

³¹⁸ EDPB, **Guidelines on articles 46/2a and 46/3b**, par. 68, 69, s. 14.

³¹⁹ EDPB, **Guidelines on articles 46/2a and 46/3b**, par. 71, s. 15.

belirtmek gerekir ki yetkili denetim makamı, duruma göre inceleme yaparak onay vereceği için, bahsi geçen güvencelerden daha fazlasını talep edebilir³²⁰.

GDPR m.46/f.2/a ve m.46/f.3/b ile öngörülen aktarım mekanizmaları, yalnızca kamu kuruluşları arasında gerçekleşecek olan kişisel veri aktarımları ile sınırlı olduğundan uygulamada aktif olarak tercih edilen bir aktarım yöntemi olmamıştır. Buna rağmen yeterlilik kararı bulunmayan üçüncü ülke veya uluslararası kuruluşlara veri aktarımı imkânı sunması nedeniyle kamu kuruluşları açısından önemli bir düzenlemedir³²¹.

2. Sözleşme Hükümleri

Yeterlilik kararının bulunmadığı durumlarda üçüncü ülkelere veya uluslararası kuruluşlara yapılan veri aktarımlarına hukuki dayanak teşkil edebilecek uygun güvenlik önlemlerinden biri de veri aktaran ve üçüncü ülkede bulunan veri alıcısı arasındaki sözleşme hükümleridir (GDPR m.46/f.2, m.46/f.3). Sözleşme hükümlerine dayalı olarak gerçekleştirilen aktarımlarda yeterli korumanın sözleşme taraflarınca (veri aktaran ve veri alıcısı) sağlanması beklenmektedir. Bu nedenle bu tür aktarımlarda sağlanan veri koruma somut aktarım için geçerlidir ve veri alıcısının bulunduğu üçüncü ülkenin tamamen güvenli olduğu anlamına gelmez³²². Sözleşme hükümlerine dayalı aktarımlar, AB çerçevesinde henüz 95/46/EC sayılı DPD yürürlükteyken kabul edilmiş olsa da (m.26/f.2), GDPR'ın kabul edilmesiyle hem bu hususta bazı değişiklikler getirilmiş hem de sözleşme hükümlerinin kapsamı daha da genişletilmiştir.

Veri aktarımlarına ilişkin sözleşmesel hükümleri, standart sözleşme hükümleri (*standart contractual clauses*) ve özel sözleşme hükümleri olarak ikiye ayırmak mümkündür. Genellikle yeterli düzeyde koruma sağlamadığı düşünülen ülkelere veri aktarımlarını gerçekleştirmek için en sık kullanılan mekanizma “standart sözleşme hükümleri” veya “model hükümler”dir³²³. Yeterli düzeyde koruma vaad etmeyen ülkelere kişisel veri aktarımını düzenlemenin bir aracı olarak

³²⁰ EDPB, **Guidelines on articles 46/2a and 46/3b**, par. 73, s. 15.

³²¹ Çelik, s. 132.

³²² Paul Voigt/ Axel von dem Bussche, **The EU General Data Protection Regulation (GDPR): A Practical Guide**, Berlin, Springer International Publishing, 2017, s. 119.

³²³ Ustaran, s. 115; Bilgi Information Technology Law Institute, s. 82.

sözleşme hükümleri, 95/46/EC sayılı DPD'nin yürürlüğe girmesinden önce kullanılmaya başlamıştır. Şöyle ki, 1992 yılında AK, AB Komisyonu ve Milletlerarası Ticaret Odası, “Sınır Ötesi Veri Akışları Bağlamında Eşdeğer Koruma Sağlamak için Model Sözleşme” adlı ortak bir çalışma yayınlamıştır. Söz konusu model sözleşmenin amaçları; farklı veri koruma rejimlerine tabi olan kişisel veri aktarımının ardından ortaya çıkan sorunların çözümüne bir örnek sunmak, uluslararası veri aktarımını kolaylaştırmak, uluslararası ticaretin geliştirilmesi adına veri aktarımına izin vermek, uluslararası işlemlerin güvenliğini ve kesinliğini arttırmak olarak belirlenmiştir³²⁴. Hem bu hükümlerin müzakere sürecinde AB Komisyonu'nun aktif katılımı hem de Milletlerarası Ticaret Odası tarafından da benzer hükümlerin kabul edilmesi, 95/46/EC sayılı DPD'nin taslağı hazırlanırken sözleşme hükümlerinin de kabul edilmesini tetiklemiştir³²⁵.

Standart sözleşme hükümleri, kişisel verilerin AB standartlarına uygun olarak korunmasını amaçlayan hem veri aktaran hem de veri alıcısı için geçerli olan belirli yükümlülükler tesis eden hükümlerdir³²⁶. Standart hükümler her şeyden önce, veri aktarımı sürecini kolaylaştırır. Şöyle ki, taraflar sıfırdan bir taslak hazırlamak yerine, mevcut olan kalıpları kullanabilirler³²⁷. Bu tür sözleşmeler, esasen aktarılan bir veri grubunu, bu aktarımın amaçlarını ve her iki tarafın bu verilerle ilgili hak ve yükümlülüklerini ayrıntılı olarak ortaya koyar³²⁸. Bu tür sözleşmelerin bir diğer özelliği, uyumsuzluk hâlinde veri alıcısının, veri aktaran veri sorumlusunun ulusal denetim makamına ve/veya mahkemelerine tabi olmayı kabul etmesidir³²⁹.

Standart sözleşme hükümleri, Komisyon tarafından (GDPR m.46/f.2/c) veya ulusal veri koruma kurumu tarafından kabul edilebilir. Fakat ulusal veri koruma kurumlarının kabul ettiği hükümlerin, daha sonra Komisyon tarafından onaylanması

³²⁴ Yves Poullet/ Sophie Louveaux/ Maria Veronica Perez Asinari, “Data Protection and Privacy in Global Networks: a European Approach”, **Electronic Data Interchange Law Review**, C. 8, S. 2-3, 2001, s. 172; Kuner v.d., **Commentary**, s. 799.

³²⁵ Kuner v.d., **Commentary**, s. 800.

³²⁶ Ustaran, s. 115.

³²⁷ Paul M. Schwartz, “The EU-U.S. Privacy Collision: A Turn to Institutions and Procedures”, **Harvard Law Review**, C. 126, S. 7, 2013, s. 1981.

³²⁸ Rosa Barcelo, “Seeking Suitable Options for Importing Data from the European Union”, **The International Lawyer**, C. 36, S. 3, 2001, s. 996.

³²⁹ Giakoumopoulos/ Buttarelli/ O’Flaherty, **Handbook**, s. 261.

gerekmektedir (GDPR m.46/f.2/d). Ayrıca ulusal denetim makamlarının hazırlamış olduğu standart sözleşme hükümlerini kabul edilebilmesi için söz konusu hükümlerle ilgili EDPB'nin görüşünün alınması gerekmektedir (GDPR m.64/f.1/d). Ulusal denetim makamları tarafından kabul edilen ve Komisyon tarafından onaylanan standart sözleşme hükümleri, Tüzük'le getirilen yeniliklerden biri olmasıyla birlikte, yeteri kadar uygulama alanı bulamamıştır. Zira şimdiye kadar hiçbir AB ulusal veri koruma kurumu, onaylanması üzere Komisyon'a standart veri koruma hükümleri sunmamıştır³³⁰.

ABAD'ın "Güvenli Liman" Anlaşması'nı iptal etmesiyle birlikte standart sözleşme hükümleri, ABD ile yapılan veri aktarımlarında en çok kullanılan hukuki araç hâline gelmiştir³³¹. Yukarıda da bahsedildiği üzere "Güvenli Liman" yürürlükten kaldırıldıktan sonra Schrems, standart sözleşme hükümlerinin iptaline dair dava açsa da ABAD bir aktarım mekanizması olarak standart sözleşme hükümlerinin yeterli korumayı sağladığını onaylamıştır³³². Söz konusu kararda standart sözleşme hükümlerine ilişkin bazı önemli hususlara da yer verilmiştir.

"Schrems II" kararında öncelikle yeterlilik kararlarının esasını teşkil eden temelde eşdeğer korumanın, standart sözleşme hükümlerine dayalı aktarımlar için de geçerli olduğu belirtilmiştir³³³. Bu doğrultuda ABAD, GDPR m.46 kapsamında dikkate alınması gereken kriterlerin, GDPR m.45/f.2 kapsamında yeterlilik değerlendirilmesinde dikkate alınması gereken kriterlerle aynı olduğunu ifade etmiştir. Standart sözleşme hükümlerine dayalı aktarımlar açısından bir değerlendirme yapılırken özellikle, AB'de yerleşik veri sorumlusu veya veri işleyen ile üçüncü ülkede bulunan veri alıcısı arasındaki sözleşme hükümleri ve üçüncü ülkenin kamu kuruluşlarının aktarılan verilere erişimi ile ilgili olarak söz konusu ülkenin mevzuatındaki ilgili hususlar dikkate alınmalıdır³³⁴.

³³⁰ Bilgi Information Technology Law Institute, s. 26.

³³¹ Hon, s. 190; Dülger/ Kahraman, **GDPR ve KVKK Ekseninde**, s. 70; Compagnucci/ Aboy/ Minssen, s. 4.

³³² ABAD C-311/18, par. 136.

³³³ ABAD C-311/18, par. 96.

³³⁴ ABAD C-311/18, par. 104.

Kişisel verilerin aktarıldığı üçüncü ülkede AB hukukuna eşdeğer korumanın sağlanıp sağlanmadığının belirlenmesi veri aktaran veri sorumlusu veya veri işleyenin sorumluluğundadır³³⁵. Bu nedenle, standart sözleşme hükümlerine dayanarak veri aktaran, AB hukuku ile sağlanan korumaya eşdeğer korumanın üçüncü ülkede de sağlanıp sağlanmadığını, olay bazında (*case-by-case*) veri alıcısı ile işbirliği içerisinde değerlendirmelidir³³⁶. Yeterli koruma düzeyinin sağlanamayacağı durumlarda veri aktaran, AB'deki korumaya eşdeğer korumayı temin etmek için ek önlemler (*supplementary measures*) alınmasını talep edebilir³³⁷. EDPB tarafından yayınlanan kılavuzda ek önlemlerin teknik, sözleşmesel ve organizasyonel nitelikli olabileceği belirtilmiştir³³⁸. Söz konusu önlemlerden hangisinin somut aktarım için daha etkili olacağı; verilerin formatı (örneğin; şifrelenmiş, anonimleştirilmiş veya düz metin), niteliği, veri işleme faaliyetinin süresi, verilerin aktarılmasından sonra yeniden aktarılma ihtimali (ileri aktarımlar) gibi hususlar dikkate alınarak veri aktaran tarafından belirlenecektir³³⁹. Bütün önlemlerin alınmadığı durumlarda ise ABAD, aktarımın sonlandırılması veya askıya alınması gerektiğine karar vermiştir³⁴⁰.

ABAD, standart sözleşme hükümlerinin Komisyon tarafından onaylanmasının, ulusal denetim makamlarının GDPR m.58/f.2 kapsamındaki yetkilerinin Komisyon tarafından sınırlandırılması anlamına gelmeyeceğinin de altının çizmiştir³⁴¹. Şöyle ki CFR m.8 ve GDPR m.51/f.1 ve m.57/f.1/a uyarınca, yetkili denetim makamları kişisel verilerin işlenmesi bağlamında gerçek kişilerin haklarının korunmasına ilişkin kurallara uyum sağlanıp sağlanmadığını denetlemekle yükümlüdür³⁴². Denetim sonucunda veri aktarılan üçüncü ülkede herhangi bir sebeple standart veri koruma hükümlerine uyulmadığı veya uyulamadığı tespit

³³⁵ Sertçe, s. 57.

³³⁶ ABAD C-311/18, par. 134.

³³⁷ ABAD C-311/18, par. 133.

³³⁸ European Data Protection Board, Recommendations 01/2020 on Measures That Supplement Transfer Tools to Ensure Compliance with the EU Level of Protection of Personal Data, 10.11.2020, par. 47, s. 15, (çevrimiçi), https://edpb.europa.eu/our-work-tools/documents/public-consultations/2020/recommendations-012020-measures-supplement_en, 11.01.2021.

³³⁹ EDPB, Guidelines on articles 46/2a and 46/3b, par. 49, s. 16.

³⁴⁰ ABAD C-311/18, par. 135.

³⁴¹ Sertçe, s. 57.

³⁴² ABAD C-311/18, par. 107, 108.

edilirse denetim makamının, GDPR m.58/f.2/f ve m.58/f.2/j uyarınca veri aktarımını askıya alması veya yasaklaması gerekir³⁴³.

Yeterlilik kararlarında olduğu gibi Komisyon tarafından onaylanan standart sözleşme hükümlerinin de düzenli olarak gözden geçirilmesi gerekmektedir (GDPR Giriş bölümü par. 106). GDPR m.46/f.5 uyarınca, 95/46/EC sayılı DPD m.26/f.4 kapsamında Komisyon'un standart sözleşme hükümlerine ilişkin kabul ettiği kararlar, yine Komisyon kararı ile değiştirilene, yenilenene veya yürürlükten kaldırılana kadar geçerli olacaktır. Nitekim 95/46/EC sayılı DPD yürürlükte olduğu zaman kabul edilen standart sözleşme hükümlerine ilişkin Komisyon kararları³⁴⁴, 4 Haziran 2021 tarihinde Komisyon tarafından bu kararların yerini alacak yeni standart sözleşme hükümlerinin³⁴⁵ kabul edilmesine dek yürürlükte kalmıştır³⁴⁶.

95/46/EC sayılı DPD döneminde onaylanmış olan standart sözleşme hükümlerinin, GDPR'da öngörülen birçok korumadan yoksun kalması ve ABAD'ın "Schrems II" kararında ifade ettiği standart sözleşme hükümlerine ilişkin endişeler, standart sözleşme hükümlerinin güncellenmesi ihtiyacını ortaya çıkarmıştır³⁴⁷. Eski standart sözleşme hükümlerinde yer alan birçok temel husus (örneğin; yeterli korumayı sağlamak adına GDPR'a uyumun taahhüt edilmesi, standart maddelerin sözleşme taraflarınca değiştirilememesi, standart maddelerle çelişmediği müddetçe sözleşmeye ilave maddelerin eklenebilmesi vs.) yeni standart sözleşme hükümlerinde

³⁴³ ABAD C-311/18, par. 113, 114, 121.

³⁴⁴ 95/46/EC sayılı DPD döneminde Komisyon'un standart sözleşme hükümlerine ilişkin üç kararı mevcut olmuştur. Söz konusu kararların ikisi (15.06.2001 tarihli ve 2001/497/EC sayılı; 27.12.2004 tarihli ve 2004/915/EC sayılı kararlar) veri sorumlusundan veri sorumlusuna yapılan aktarımlar zamanı kullanılacak standart hükümler içermekteydi ve birbirine alternatif olarak kullanılmaktaydı. 27.12.2001 tarihli ve 2002/16/EC sayılı kararın yerine geçen 05.02.2010 tarihli ve 2010/87/EU sayılı karar ise veri sorumlusundan veri işleyene yapılan aktarımlar zamanı kullanılacak standart hükümler içermekteydi.

³⁴⁵ Commission Implementing Decision (EU) 2021/914 of 4 June 2021 on standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council C/2021/3972, (çevrimiçi), https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/standard-contractual-clauses-scc/standard-contractual-clauses-international-transfers_en, 14.06.2021.

³⁴⁶ Sertçe, s. 53.

³⁴⁷ Phillip Lee, "The Updated Standard Contractual Clauses: A New Hope?", 07.06.2021, (çevrimiçi), <https://iapp.org/news/a/the-updated-standard-contractual-clauses-a-new-hope/>, 14.06.2021.

aynen devam ettirilse de, yeni standart sözleşme hükümleri eskiye nazaran önemli yenilikler içermektedir³⁴⁸.

Yapılan değişikliklerden en önemlisi, standart sözleşme hükümlerinin modüler yapısıyla ilgilidir. Şöyle ki, yalnızca veri sorumlusundan veri sorumlusuna ve veri sorumlusundan veri işleyene aktarım imkânı sağlayan eski standart sözleşme hükümlerinin aksine, yeni kararda “veri sorumlusundan veri sorumlusuna”, “veri sorumlusundan veri işleyene”, “veri işleyenden veri işleyene” ve “veri işleyenden veri sorumlusuna” olmak üzere dört farklı veri aktarım modülü kabul edilmiştir³⁴⁹. Aynı zamanda Komisyon, yeni kararıyla standart sözleşme hükümlerinin coğrafi açıdan uygulanabilirliğini daha da genişletmiştir. Şöyle ki, eski standart sözleşme hükümlerinde sadece AB’de yerleşik olan veri sorumluları sözleşmeye taraf olabilecek iken, artık AB dışında bulunan veri aktaranların da sözleşmeye taraf olma imkânı kabul edilmiştir. Görüldüğü üzere, yeni sistem ile veri işleme rolü (veri sorumlusu veya veri işleyen) ve konumu farketmeksizin veri aktaran ile veri alıcısı arasındaki veri aktarımı imkânları esneklik kazanmıştır³⁵⁰.

Yeni standart sözleşme hükümleri ile birden fazla veri aktaran tarafın çok taraflı sözleşmeler yapması ve “yerleştirme maddesi” (*docking clause*) uyarınca, zamanla sözleşmeye yeni tarafların eklenmesi mümkün olmuştur. İsteğe bağlı olan bu maddeye göre, üçüncü taraflar yeni sözleşme yapmadan aktarımın ayrıntılarını içeren ekleri imzalayarak mevcut sözleşmeye katılabilirler³⁵¹.

Yeniliklerin önemli bir kısmı ABAD’ın “Schrems II” kararında ifade ettiği standart sözleşme hükümlerine yönelik endişelerinin giderilmesi amacına hizmet etmektedir. Şöyle ki, yeni standart sözleşme hükümlerine göre veri aktaran, verilerin aktarıldığı üçüncü ülkenin ulusal düzenlemelerinin sözleşme maddeleri ile çelişip çelişmediğine ve ek güvenlik önlemlerinin alınmasına gerek olup olmadığına dair veri koruma etki değerlendirmesi (*data protection impact assessment*) yapmalı ve bu

³⁴⁸ Sertçe, s. 59.

³⁴⁹ Compagnucci/ Aboy/ Minssen, s. 8; Sertçe, s. 60.

³⁵⁰ Compagnucci/ Aboy/ Minssen, s. 8; Lee, **Updated Standard Contractual Clauses**.

³⁵¹ Bkz. Commission Implementing Decision (EU) 2021/914 of 4 June 2021, Annex, Clause 7; Compagnucci/ Aboy/ Minssen, s. 9; Sertçe, s. 61-62.

değerlendirmeyi belgeleyerek talep hâlinde yetkili denetim makamına sunmalıdır³⁵². Ayrıca, yeni standart sözleşme hükümlerinde yeterli korumanın sağlanabilmesi için gerekli teknik ve organizasyonel önlemlere de ayrıntılı bir şekilde yer verilmiştir³⁵³.

Sözleşme hükümlerine dayalı aktarımların bir diğer türü ise, özel (veya *ad hoc*)³⁵⁴ sözleşme hükümlerine dayalı aktarımlardır. Standart veri koruma hükümlerinin varlığı, veri sorumluları tarafından belirli bir amaca özgü, bireysel sözleşmesel hükümlerin düzenlenmesini engellemez. Bu noktada aranan tek şart, söz konusu özel sözleşme hükümlerinin, her bir aktarım özelinde yetkili denetim makamı tarafından onaylanmış olmasıdır (GDPR m.46/f.3/a)³⁵⁵. Şimdiye kadar herhangi bir AB veri koruma otoritesi tarafından özel sözleşme hükümleri onaylanmamıştır³⁵⁶.

Veri koruma hükümlerinin belirlenmesinde taraflara daha fazla esneklik sağlaması ve dolayısıyla da yükümlülüklerin daha az ihlal edilmesine sebep olması açısından özel sözleşme hükümleri daha avantajlıdır³⁵⁷. Kanaatimizce, özel sözleşme hükümleri sadece tek bir üye devletten veri aktarımı söz konusu olduğunda daha verimli olacaktır. Çünkü eğer birkaç üye devletlerden veri aktarımı söz konusu ise bu durumlarda veri alıcısı her ülke ile farklı bir sözleşme yapmak zorunda kalacaktır³⁵⁸. Bu gibi durumlarda model hükümlerin tercih edilmesi daha çevik bir aktarım imkânı sağlayacaktır.

Veri sorumlusu/ işleyen ve üçüncü ülkede bulunan veri alıcısı arasında sözleşme yapılması (m.46/f.3/a) ve standart sözleşme hükümlerinin yetkili denetim makamı tarafından kabul edildiği durumlarda (m.46/f.2/d) yetkili denetim makamı tarafından GDPR m.63 uyarınca “tutarlılık mekanizması” (*consistency mechanism*)³⁵⁹ uygulanır (m.46/f.4). Buna göre, yetkili denetim makamı taslak kararını görüş bildirmesi için Kurul’a iletir. Kurul’un görüşü üyelerin salt

³⁵² Compagnucci/ Aboy/ Minssen, a.y.; Sertçe, s. 62-63.

³⁵³ Bkz. Commission Implementing Decision (EU) 2021/914 of 4 June 2021, Annex II; Sertçe, s. 63.

³⁵⁴ Kaya, **Transfer of Personal Data**, s. 42.

³⁵⁵ Giakoumopoulos/ Buttarelli/ O’Flaherty, **Handbook**, s. 260; Sertçe, s. 76.

³⁵⁶ Bilgi Information Technology Law Institute, s. 82; Toparlak, s. 41; Pelen, s. 1725; Sertçe, a.y.

³⁵⁷ Ustaran, s. 116.

³⁵⁸ Barcelo, s. 997.

³⁵⁹ Tutarlılık mekanizması – Tüzük’ün Birlik içerisinde tutarlı bir şekilde uygulanmasına katkıda bulunulması amacıyla yetkili denetim makamlarının birbiriyle ve uygun olduğu hâllerde Komisyon ile işbirliği yapması (GDPR m.63).

çoğunluğuyla sekiz hafta içerisinde kabul edilir. Bu süre, altı hafta daha uzatılabilir (m.64/f.3). Yetkili denetim makamı, Kurul'un görüşünü göz önünde bulundurarak karar taslağını aynı şekilde tutacağını veya değiştireceğini ve varsa değiştirilmiş taslağı, görüşün alınmasından itibaren iki hafta içerisinde Kurul başkanına iletir (m.64/f.7).

3. Bağlayıcı Şirket Kuralları

Bir önceki bölümde de bahsedildiği üzere, yeterli veri koruma düzeyinin bulunmadığı üçüncü ülkelere veya uluslararası kuruluşlara yönelik kişisel veri aktarımını meşrulaştırmak için en çok başvuru hukuki araç sözleşme hükümleridir. Fakat bazı durumlarda veri aktaran ve veri alıcısı arasında bu gibi bir sözleşmenin yapılması isabetli olmayabilir. Şöyle ki, bazı çokuluslu şirketlerin, birçok yabancı ülkelerde bağlı kuruluşları bulunmaktadır. Birbirine bağlı şirketler arasındaki veri aktarımı, şirketler topluluğunun verimli çalışması için vazgeçilmezdir³⁶⁰. Bu gibi durumlarda, her aktarım için sözleşme yapılması veya standart hükümlerin kullanılması pratik olmadığı gibi, lüzumsuz bir sözleşme kalabalığına da sebep olacaktır³⁶¹. Ayrıca, standart veri koruma maddeleri, aktarılan verilerin niteliğine göre düzenlenmesine rağmen bağlayıcı şirket kuralları (*binding corporate rules*), aktarılan verilerin türü farketmeksizin oluşturulmaktadır ve olası tüm veri aktarım faaliyetlerine ex post biçimde uygulanabilecek şekilde tasarlanmaktadır³⁶².

Bağlayıcı şirket kuralları, çok uluslu şirketlerin ihtiyari olarak hazırladığı ve takip ettiği Avrupa gizlilik standartlarına dayanan kurallar dizisidir³⁶³. Bu kurallar, çokuluslu şirketlere, üçüncü ülkelerde bulunan bağlı şirketlerine veri aktarımını gerçekleştirme imkânı sağlamaktadır³⁶⁴. Standart sözleşme hükümlerinden farklı olarak bağlayıcı şirket kuralları, veri aktaran ve veri alıcısı arasında veri koruma

³⁶⁰ Room, s. 161; Lloyd, s. 201.

³⁶¹ Lloyd, s. 203; Toparlak, s. 42-43.

³⁶² Toparlak, s. 43; Sertçe, s. 48.

³⁶³ Ustaran, s. 117; Lingjie Kong, "Data Protection and Transborder Data Flow in the European and Global Context", *The European Journal of International Law*, C. 21, S. 2, 2010, s. 454; Kaya, *Transfer of Personal Data*, s. 45; W. Kuan Hon/ Christian Millard, "Data Export in Cloud Computing – How Can Personal Data Be Transferred Outside The EEA?", s. 20, (çevrimiçi), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2034286, 23.10.2021; Moerel, s. 22-23.

³⁶⁴ Moerel, s. 27.

yükümlülüklerinin belirlenmesine dair bir anlaşma değil, çokuluslu şirketlerin tek taraflı eylemidir³⁶⁵.

95/46/EC sayılı DPD’de açık bir şekilde öngörülmesi de, Yönerge’nin amaçları doğrultusunda güvenli önlemler oluşturmak için bağlayıcı şirket kurallarının kullanılması düşüncesi, ilk olarak Madde 29 Çalışma Grubu tarafından 95/46/EC sayılı DPD’nin m.26/f.2’nin kapsamlı yorumu üzerine geliştirilmiştir³⁶⁶. Söz konusu kurallar, gruba dâhil olan şirketlerin kuruluş yeri veya verileri işlenen veri sahiplerinin uyruğu veya herhangi diğer değerlendirmelerden bağımsız olarak şirketler grubunun geneline uygulanır³⁶⁷.

Bağlayıcı şirket kurallarının, kişisel verilerin üçüncü ülkelere aktarılması için bir mekanizma olarak GDPR’a dâhil edilmesi, kişisel verilerin korunması hukuku açısından önemli bir gelişme olmuştur³⁶⁸. GDPR m.4/f.20 uyarınca, *“bağlayıcı şirket kuralları ortak bir ekonomik faaliyetle iştigal eden bir teşebbüsler grubu veya bir işletmeler grubu içerisinde bir veya daha fazla sayıda üçüncü ülkedeki bir veri sorumlusu veya veri işleyene kişisel veri aktarımları veya aktarım dizisiyle ilgili olarak Üye Devletler’den birinin sınırlarında kurulmuş olan bir veri sorumlusu veya veri işleyen tarafından uyulması gereken veri koruma politikalarıdır”*. Örneğin, Google şirketinin; Chrome, Gmail, Maps ve diğer tüm hizmetlerinin kişisel verileri işlemesi, ortak ekonomik faaliyet olarak nitelendirildiği için kendi aralarında tüm kişisel veri aktarımlarını bağlayıcı şirket kuralları çerçevesinde gerçekleştirebilirler³⁶⁹.

Bağlayıcı şirket kurallarının bağlayıcılığı, gruba dâhil olan şirketlerle sınırlıdır³⁷⁰. Başka bir deyişle, bağlayıcı şirket kuralları sadece grup şirketin bünyesinde bulunan kuruluşların gerçekleştirdiği aktarımın, Tüzükle uyumlu

³⁶⁵ Kong, s. 453.

³⁶⁶ Article 29 Data Protection Working Party, Working Document: Transfers of personal data to third countries: Applying Article 26 (2) of the EU Data Protection Directive to Binding Corporate Rules for International Data Transfers, 03.06.2003, s. 5-6, (çevrimiçi), https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2003/wp74_en.pdf, 25.01.2021.

³⁶⁷ Article 29 Working Party, **BCR for Data Transfers**, s. 8.

³⁶⁸ Ustaran, s. 117.

³⁶⁹ Sharma/ Menon, s. 172.

³⁷⁰ Dülger/ Kahraman, **GDPR ve KVKK Ekseninde**, s. 5.

olduğunu göstermektedir ve dolayısıyla sadece bu kuruluşlar arasında serbest veri akışını temin eder³⁷¹. Bağlayıcı şirket kuralları, gruba dâhil olmayan kuruluşlara yapılan veri aktarımı için hukuki dayanak teşkil etmeyeceği için, madde 46’da öngörülen diğer uygun güvenlik önlemleri tercih edilmelidir³⁷².

Bağlayıcı şirket kurallarına dayalı akatırımlar açısından açıklık getirilmesi gereken diğer husus da ileri aktarımlardır. Bu noktada belirtmek gerekir ki bağlayıcı şirket kuralları açısından ileri aktarımlar, birinci aktarımı müteakiben yapılan bütün aktarımları değil, yalnızca grup dışına yapılan aktarımları kapsamaktadır. Başka bir deyişle, aynı veriler bir şirketler veya teşebbüsler grubu dâhilinde kaç kez el değiştirirse değiştirsin aktarım, aynı yasal dayanağa yani bağlayıcı şirket kurallarına tabi olarak gerçekleştirilmiş olacaktır. Fakat şirketler grubuna dâhil olsa da AB sınırları dışında bulunan bir şirketin, kişisel verileri yeterli koruma sağlamayan üçüncü ülkede bulunan başka bir bağımsız şirkete aktarabilmesi için Komisyon tarafından hazırlanan sözleşmelerden birinin (veri sorumlusundan veri sorumlusuna veya veri sorumlusundan veri işleyene) mevcut olması şartı aranmaktadır³⁷³. Ayrıca bu, Madde 29 Çalışma Grubu’nun veri aktarımları için öngördüğü ilkelerden biridir. Bu nedenle bağlayıcı şirket kuralları hazırlanırken sonraki aktarımlar için kullanılacak olan sözleşme modellerine de yer vermelidir. Ayrıca, veri koruma otoritelerinin ve veri sahibinin talebi üzerine bu sözleşme örneklerini temin etmelidir³⁷⁴.

Bağlayıcı şirket kuralları, çok sayıda kişisel verinin düzenli aktarımı için tasarlanmıştır. Bu davranış kurallarını uygulayarak, şirketler daha fazla idari prosedürden kaçınabilir ve başka herhangi bir şart aranmaksızın veri aktarımları gerçekleştirilebilir. Şunu da belirtmek gerekir ki bu kurallar vasıtasıyla veri aktarımı, veri sorumlusu şirketin kendi tasarrufundadır. Başka bir deyişle, bağlayıcı şirket

³⁷¹ Toparlak, s. 42; Moerel, s. 20.

³⁷² Kuner v.d., **Commentary**, s. 820; Sharma/ Menon, s. 172; Toparlak, a.y.

³⁷³ Article 29 Working Party, **BCR for Data Transfers**, s. 9.

³⁷⁴ Article 29 Working Party, **BCR for Data Transfers**, s. 10.

kuralları yerine GDPR m.46’da öngörülen alternatif uygun güvenlik önlemleri de tercih edilebilir³⁷⁵.

Bağlayıcı şirket kuralları, şirketlerce belirlendikten sonra yetkili denetim makamı tarafından, GDPR m.63 (“tutarlılık mekanizması”) uyarınca onaylanmalıdır³⁷⁶. Burada açıklanması gereken önemli bir husus, şirketler grubunun, kuralları onaylatmak için hangi veri koruma otoritesine başvurması gerektiğiyle ilgilidir. Şöyle ki, Madde 29 Çalışma Grubu’na göre, eğer grubun genel merkezi veya ana şirketi, bir AB üyesi olan ülkede yerleşikse bu ülkenin yetkili denetim makamına başvuru yapılmalıdır³⁷⁷. Eğer genel merkezin veya ana şirketin nerede yerleştiği açık değilse veya AB dışında bir ülkede ise o zaman aşağıdaki kriterlere göre en uygun veri koruma otoritesine başvuru yapılmalıdır³⁷⁸. Yetkili veri koruma kurumuna başvuru yapıldığı zaman, başvurunun neden bu kuruma yapıldığı kısaca açıklanmalıdır. Uygun denetim makamının belirlenmesi sırasında aşağıdaki kriterlerin dikkate alınması gerekmektedir³⁷⁹:

- AB genel merkezli şirketler grubunun, genel merkezinin konumu,
- şirketler grubunun, AB’de bulunan ve delege olarak yetkilendirilmiş veri koruma sorumluluklarına sahip üyesinin konumu,
- yönetim işlevi, idari yük vs. açıdan grup içinde kuralları uygulamak ve başvurularla ilgilenebilmek için en uygun olan şirketin bulunduğu yer,
- işlemin amaçları ve araçları açısından çoğu kararın alındığı yer,
- AB dışındaki ülkelere en çok aktarımın gerçekleşeceği AB’ye üye devlet.

³⁷⁵ Sharma/ Menon, s. 172.

³⁷⁶ Tutarlılık mekanizmasının nasıl uygulandığına dair bkz.: yuk., İkinci Bölüm, “Sözleşme Hükümleri” başlığı.

³⁷⁷ Article 29 Working Party, Working Document Establishing a Model Checklist Application for Approval of Binding Corporate Rules, 14.04.2005, s. 3, (çevrimiçi), ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2005/wp108_en.pdf, 26.02.2021, (Article 29 WP, Approval of BCRs).

³⁷⁸ Bağlayıcı şirket kurallarını onaylatmak için gereken standart başvuru formunun yapısı ve içeriği için bkz. Article 29 Working Party, Recommendation 1/2007 on the Standard Application for Approval of Binding Corporate Rules for the Transfer of Personal Data, 10.01.2007, https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/index_en.htm, 25.02.2021.

³⁷⁹ Article 29 WP, **Approval of BCRs**, s. 3.

Şunu da belirtmek gerekir ki bu kriterler kesin değildir. Başka bir deyişle, başvuru yapılan veri koruma kurumu, gerçekten en uygun veri koruma otoritesinin o olup olmadığına karar verirken takdir yetkisini kullanabilecektir³⁸⁰.

Yetkili denetim makamının, bağlayıcı şirket kurallarını onaylaması için aşağıdaki şartlar aranmaktadır (GDPR 47/1):

- çalışanları da dâhil olmak üzere ortak bir ekonomik faaliyette bulunan bir teşebbüsler grubunun veya bir işletmeler grubunun ilgili her üyesi açısından yasal bağlayıcılığının olması, bu üyelere uygulanması ve bu üyeler tarafından yürütülmesi (GDPR m.47/f.1/a);
- veri sahiplerine kişisel verilerinin işlenmesi ile ilgili olarak uygulanabilir hakları açık bir şekilde vermesi (GDPR m.47/f.1/b);
- m.47/f.2’de yer alan asgari şartların bağlayıcı şirket kurallarının metninde yer alması.

Her bir şirket, kendi kurallarını belirlemekte serbest olsa da mutlaka bağlayıcı şirket kurallarına dâhil edilmesi gereken asgari koşullar da GDPR ile düzenlenmiştir³⁸¹. Söz konusu koşulların içeriği büyük ölçüde Madde 29 Çalışma Grubu’nun Çalışma Belgelerinde³⁸² belirtilen gereksinimlerle benzer niteliktedir.

Şirket gruplarının üyeleri ve uygulamaları zaman zaman değişebileceği için onaylanan bağlayıcı şirket kuralları, her zaman mevcut koşullara uygun olmayabilir. Aşağıdaki koşullar yerine getirildiği takdirde, bağlayıcı şirket kurallarının veri koruma otoriteleri tarafından yeniden onaylanmasına gerek kalmaksızın güncellenmesi mümkündür³⁸³:

³⁸⁰ Article 29 WP, a.y.

³⁸¹ Bağlayıcı şirket kurallarında yer alması gereken asgari unsurlar için bkz.: GDPR m.47/f.2

³⁸² Bkz. Article 29 Working Party, Working Document Setting up a Framework for the Structure of Binding Corporate Rules, 24.06.2008, (çevrimiçi) https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2008/wp154_en.pdf, 29.03.2021, (Article 29 WP, The Structure of BCR); Article 29 Working Party, Working Document setting up a table with the elements and principles to be found in Processor Binding Corporate Rules, 06.02.2018, (çevrimiçi), <https://ec.europa.eu/newsroom/article29/items/614110/en>, 25.03.2021.

³⁸³ Article 29 WP, **BCR for Data Transfers**, s. 15; Article 29 WP, **The Structure of BCR**, s. 9-10; Toparlak, s. 66.

- veri aktaran, yeni bir üyenin kurallara etkili bir şekilde bağlı olduğundan ve uyum sağladığından emin olmadıkça yeni üyeye veri aktarımı gerçekleştirilmemeli,

- önceden belirlenmiş bir kişi veya departman, üyelerin tam olarak güncellenmiş bir listesini oluşturmalı, kurallardaki güncellemeleri takip etmeli ve kaydetmeli ve talep üzerine veri sahiplerine ve veri koruma otoritelerine söz konusu bilgileri sağlamalıdır,

- üye listesindeki değişiklikler veya kurallara yapılacak herhangi güncellemeler, söz konusu güncellemelerin nedenlerinin kısa bir açıklaması ile birlikte, kuralları onaylamış olan veri koruma otoritesine yılda bir kere rapor edilmelidir.

Güncellemeler, iş koşullarının değişmesi ve bu nedenle kuralların mevcut koşullara uyarlanması gerektiğinde söz konusu olacaktır. Fakat değişen koşullar, veri koruma ilkeleri, veri işlemenin amacı, işlenen verilerin kategorileri gibi önemli hususlarla ilgili olduğu zaman, bu değişiklikler için veri koruma otoritesine yeniden başvuruda bulunmak gerekecektir³⁸⁴.

4. Onaylanmış Davranış Kuralları

Davranış kuralları daha önce 95/46/EC sayılı DPD’de de öngörülmüş olsa da (95/46/EC sayılı DPD m.27) yeterli koruma sağlamayan üçüncü ülkelere veya uluslararası kuruluşlara yapılan kişisel veri aktarımlarına hukuki dayanak olarak onaylanmış davranış kurallarının (*approved code of conduct*) (GDPR m.46/f.2/e) ve belgelendirme mekanizmasının (*approved certification mechanism*) (GDPR m.46/f.2/f) kullanılması, GDPR’ın yürürlüğe girmesiyle karşımıza çıkmaktadır³⁸⁵.

Davranış kuralları öncelikle, GDPR’ın düzgün bir şekilde uygulanmasına katkıda bulunmak amacıyla hazırlanmış araçlardır. Söz konusu kurallar; üye devletler, denetim makamları, EDPB ve Komisyon tarafından çeşitli işleme sektörlerinin spesifik özellikleri ve mikro, küçük ve orta büyüklükteki işletmelerin spesifik ihtiyaçları dikkate alınarak hazırlanır (GDPR m.40/f.1). Davranış kuralları

³⁸⁴ Article 29 WP, **BCR for Data Transfers**, s. 15.

³⁸⁵ Sertçe, s. 69.

GDPR'daki soyut yükümlülükler pratik yorum kazandırmaya hizmet eder. Başka bir deyişle, davranış kuralları oluşturan şirketler, belirli bir işleme faaliyeti veya sektörün özelliklerini dikkate alarak GDPR'a uyum gereksinimlerinin nasıl yerine getirileceğini kendileri belirleyebilirler³⁸⁶. Belli bir sektörün özellikleri dikkate alınarak hazırlandığından davranış kuralları GDPR'ın uygulanmasına yönelik daha pratik, şeffaf ve daha uygun maliyetli bir dizi kurallar oluşturma fırsatı sağlar³⁸⁷.

GDPR m.40/f.2/j uyarınca, birlikler ve veri sorumlusu veya işleyici kategorilerini temsil eden diğer organlar, üçüncü ülkelere veya uluslararası kuruluşlara kişisel veri aktarımını gerçekleştirmek için davranış kuralları hazırlayabilir, bu kuralları değiştirebilir ya da bunların kapsamını genişletebilir. Bu birlik ve organlara örnek olarak; meslek birlikleri, akademik kuruluşlar, sektörel kuruluşlar, çıkar grupları vs. gösterilebilir³⁸⁸. Bağlayıcı şirket kurallarından farklı olarak onaylanmış davranış kurallarına dayalı aktarım gerçekleştiren işletmelerin, aynı şirketler grubuna dâhil olması şartı aranmamaktadır³⁸⁹.

Davranış kurallarının, üçüncü ülkelere veya uluslararası kuruluşlara yapılan aktarımlara hukuki dayanak oluşturmaları için bu kuralların onaylanmış olması ve üçüncü ülkedeki veri sorumlusu veya işleyici tarafından, veri sahibinin hakları ile ilgili olanlar da dâhil olmak üzere uygun güvenceleri uygulamak üzere bağlayıcı ve uygulanabilir taahhütlerde bulunulması şartı aranmaktadır³⁹⁰. Taahhütte bulunma şartı, taraflar arasındaki hizmet sözleşmesine gerekli hükümlerin eklenmesi veya tarafların ayrı bir sözleşmesi akdetmesi yoluyla da sağlanabilir³⁹¹. Bu amaç doğrultusunda, davranış kurallarında yetkili denetim makamı tarafından akredite edilen bir organ tarafından, davranış kurallarını uygulamayı taahhüt eden veri

³⁸⁶ Voigt/ Bussche, s. 71-72; Toparlak, s. 46.

³⁸⁷ European Data Protection Board, Guidelines 1/2019 on Codes of Conduct and Monitoring Bodies under Regulation 2016/679, 04.06.2019, par. 11, s. 8, (çevrimiçi), https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-12019-codes-conduct-and-monitoring-bodies-0_en, 22.02.2021.

³⁸⁸ Kuner v.d., **Commentary**, s. 721; European Data Protection Board, Guidelines 04/2021 on Codes of Conduct as Tools for Transfers, 14.07.2021, par. 6, s. 4, (çevrimiçi), https://edpb.europa.eu/our-work-tools/documents/public-consultations/2021/guidelines-042021-codes-conduct-tools-transfers_en, 09.10.2021.

³⁸⁹ EDPB, **Codes of Conduct**, par. 6, s. 4.

³⁹⁰ EDPB, **Code of Conducts**, s. 5-6.

³⁹¹ EDPB, **Code of Conducts**, s. 11.

sorumluları veya veri işleyenlerin söz konusu hükümlere uyumluluğunun izlemesini sağlayan mekanizmalara yer verilir (GDPR m.40/f.4).

GDPR’da kişisel verilerin aktarılmasına ilişkin davranış kurallarının onaylanması için diğer davranış kurallarından farklı bir süreç öngörülmüştür. Şöyle ki, çeşitli üye ülkelerdeki işleme faaliyeti ile ilgili olmayan davranış kuralları taslağı, yetkili denetim makamı tarafından değerlendirilip onaylanırken (GDPR m.40/f.5), yetkili denetim makamı üçüncü ülkelere veya uluslararası kuruluşlara veri aktarımı ile ilgili davranış kurallarının taslağını onaylamadan önce, uygun güvencelerin sağlanıp sağlanmadığına dair görüşünü bildirmesi için tutarlılık mekanizması (GDPR m.63) uyarınca EDPB’ya ibraz eder (GDPR m.40/f.7). EDPB, davranış kurallarının uygun güvenceleri sağladığına kanaat getirdiği takdirde, bununla ilgili görüşünü Komisyon’a sunar (GDPR m.40/f.8) ve Komisyon uygulayıcı işlem yoluyla onaylı davranış kurallarının AB sınırlarında genel geçerliliğe sahip olduğuna karar verebilir (GDPR m.40/f.9). Böylelikle, davranış kuralları hem onaylanmış hem de AB kapsamında genel geçerliliğe sahip olmuş olacaktır³⁹². Böyle bir karar alındığı durumlarda, Komisyon onaylanmış davranış kurallarının ilan edilmesini sağlar (GDPR m.40/f.10) ve tüm davranış kurallarını bir sicilde toplayarak uygun yollarla kamuoyuna açıklar (GDPR m.40/f.11).

Davranış kurallarına uyumluluğun takibi için yetkin denetim makamı tarafından özel bir organ, izleme organı akredite edilmektedir (GDPR m.41/f.1). İzleme organının; bağımsız olması, kuralların konusu hakkında uzmanlığını kanıtlamış olması ve kuralların ihlaline ilişkin şikayetleri ele alabilmek için gerekli yapıya sahip olması gibi şartlar aranmaktadır³⁹³. Bu organ, veri sorumlusu ve veri işleyenin davranış kuralları ile uyumluluğunu izleyerek, bu kuralların ihlali durumunda, veri sorumlusu veya veri işleyenin kurallardan askıya alınması veya çıkarılması da dâhil olmak üzere, uygun işlemleri gerçekleştirecek ve bu gibi işlemler, işlemlerin gerçekleştirilme sebepleri hakkında yetkili denetim makamını bilgilendirecektir (GDPR m.41/f.4). Akredite edilmiş organın, AEA içerisinde veya

³⁹² Çelik, s. 144.

³⁹³ EDPB, **Monitoring Bodies**, s. 21-25.

AEA'da bir kuruluşu bulunması kaydıyla AEA dışında yerleşik olması mümkündür³⁹⁴.

5. Onaylanmış Belgelendirme Mekanizmaları

Belgelendirme mekanizmaları genel olarak, GDPR'a uyum çerçevesinde belirli bir sektör veya işleme faaliyetine özel gereksinimler belirlemek yerine, veri işleme faaliyetinin GDPR'la uyum içinde olduğunu kanıtlamaya hizmet eder³⁹⁵. Başka bir deyişle, belgelendirme bir uyumluluk beyanıdır³⁹⁶. Belgelendirme prosedürünün başarıyla sonuçlandığını belirtmek için mühür veya işaretler kullanılabilir³⁹⁷. GDPR m.42/f.2 kapsamında ise belgelendirme mekanizmalarına, GDPR'a tabi olmayan veri sorumlusu veya veri işleyen GDPR m.46 uyarınca uygun güvenlik önlemlerini sağladığını göstermek için dayanılmaktadır³⁹⁸. Ancak GDPR m.46/f.2/f uyarınca, üçüncü ülkelere veya uluslararası kuruluşlara veri aktarımı için sadece belgelendirme mekanizmalarına dayanılması yeterli olmayıp, üçüncü ülkedeki veri sorumlusu veya veri işleyen sözleşme veya hukuken bağlayıcı diğer bir belge ile uygun güvenlik önlemlerini sağlayacağını taahhüt etmesi gerekmektedir³⁹⁹.

Belgelendirme gönüllülük esasına dayanır ve şeffaf bir süreçle sağlanır (GDPR m.42/f.3). Bu nedenle aktarma faaliyetini belgelendirmek isteyen üçüncü ülkede yerleşik veri sorumlusu veya veri işleyen, belgelendirme usulünün gerçekleştirilmesi için gereken tüm bilgileri ve işleme faaliyetlerine erişimi yetkili denetim makamı veya veri koruma ile ilgili uygun bir uzmanlık seviyesine sahip olan belgelendirme organlarına sağlamalıdır (GDPR m.42/f.6). Belgelendirme sürecini başarıyla tamamlayan üçüncü ülkede yerleşik şirkete veya uluslararası kuruluş,

³⁹⁴ EDPB, **Code of Conducts**, s. 9.

³⁹⁵ Voigt/ Bussche, s. 71; Develioğlu, s. 77; Çelik, s. 146.

³⁹⁶ European Data Protection Board, Guidelines 1/2018 on Certification and Identifying Certification Criteria in Accordance with Articles 42 and 43 of the General Data Protection Regulation (2016/679), 04.06.2019, par. 18, s. 8, (çevrimiçi), https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-42018-accreditation-certification-bodies-under_en, 09.10.2021.

³⁹⁷ EDPB, **Certification**, a.y.

³⁹⁸ Çelik, s. 146.

³⁹⁹ Irene Kamara/ Ronald Leenes/ Eric Lachaud/ Kees Stuurman/ Marc van Lieshout/ Gabriela Bodea, Data Protection Certification Mechanisms: Study on Articles 42 and 43 of the Regulation (EU) 2016/679, Final Report, Brussels, Justice and Consumers, s. 196, (çevrimiçi), https://ec.europa.eu/info/sites/default/files/data_protection_certification_mechanisms_study_final.pdf, 25.04.2021.

ilgili işleme faaliyetinin belgelendirme mekanizmasının onaylı kriterleriyle uyumlu olduğunu kanıtlayan sertifika verilmektedir⁴⁰⁰. Belgelendirme, veri sorumlusu veya veri işleyenin GDPR’a uyumunu azaltmayacağı gibi yetkili denetim makamının görev ve yetkilerine de hâlel getirmeyecektir (GDPR m.42/f.4).

Sertifikalar, veri sorumlusu veya veri işleyene azami üç yıllık bir süre için verilmektedir. Daha sonra gerekliliklerin yerine getirilmesi hâlinde yenilenebilir. Gerekliliklerin yerine getirilmediği veya artık yerine getirilmediği durumlarda ise belgelendirme organları veya yetkili denetim makamı tarafından belgelendirme geri çekilebilir (GDPR m.42/f.7). Sertifikaların verilmesi, GDPR m.43 kapsamında belirtilen belgelendirme kurumlarının, yetkili denetim makamının veya ve EDPB’nin belirlediği kriterlere dayalı olarak gerçekleştirilir. EDPB tarafından onaylanan kriterlere göre verilen sertifikalarla, ortak bir belgelendirme olan Avrupa Veri Koruma Mührü (*European Data Protection Seal*) elde edilmektedir (GDPR m.42/f.5). EDPB, tüm belgelendirme mekanizmaları ve veri koruma mühürleri ile işaretlerini bir sicilde toplayarak kamuoyuna açıklar (GDPR m.42/f.8).

Hem onaylanmış davranış kuralları hem de belgelendirme mekanizması, GDPR’da öngörülen uygun güvenlik önlemleri arasında hünez yeni ve kullanılmamış bir yöntemdir⁴⁰¹. Fakat ABAD’ın Schrems II kararı ile “Gizlilik Kalkanı” Anlaşmasını iptal etmesi ve standart sözleşme hükümleri açısından daha sıkı koşullar belirlemesi, özellikle küçük ve orta büyüklükteki işletmelerin gerçekleştirdiği veri aktarımlarında davranış kuralları ve belgelendirme mekanizmasını tercih etmelerinin önünü açabilir⁴⁰².

D. Belirli Durumlar İçin İstisnalar

Yeterlilik kararının bulunmadığı ve uygun güvenlik önlemlerinin veri sorumlusu veya veri işleyen tarafından sağlanmadığı durumlarda kişisel verilerin Birlik sınırlarının dışına aktarılmasına imkân sağlayan belirli durumlar için istisnalar GDPR m.49 ile düzenlenmektedir. Maddede yer verilen bazı istisnaların (GDPR m.

⁴⁰⁰ Kamara v.d., s.175; Çelik, s. 146.

⁴⁰¹ Pelen, s. 1727.

⁴⁰² Sertçe, s. 75.

49/f.1/b, c ve e bentleri) kapsamını daraltmak amacıyla GDPR giriş bölümü par. 111’de sadece ara sıra yapılan ve tekrarlanmayan aktarımlarla sınırlı kalmak kaydıyla bu istisnalara dayanılabileceği belirtilmiştir. EDPB ise, doğası gereği diğer istisnai hâller için de ara sıra yapılan ve tekrarlanmayan aktarım olma şartının aranması gerektiğini ifade etmiştir⁴⁰³. Nitekim doktrinde baskın olan görüşe göre, söz konusu istisnaların devamlı tekrarlanarak kural hâline gelmesinin önüne geçmek için dar yorumlanması gerekmektedir⁴⁰⁴. Ayrıca, istisnaların kural hâline getirilemeyeceğine ABAD’ın tarafından birkaç kararında yer verilmiştir⁴⁰⁵.

1. Açık Rıza

GDPR m.4/f.11 uyarınca, *“rıza, veri sahibinin bir beyan veya olumlu eylemiyle kendisine ait kişisel verilerin işlenmesine özgürce, belirli bir faaliyete özgü olarak, bilgilendirmeye dayalı ve tereddüte mahal veremeyecek şekilde onay verdiğini gösteren her türlü göstergedir”*. GDPR m.49/f.1/a bağlamında geçerli bir rızadan bahsedebilmek için rızanın genel şartlarının (özgürce verilmiş, spesifik, bilgilendirmeye dayalı ve tereddüte yer bırakmayacak olması) yanı sıra, rızanın *“açık”* olması ve *“yeterlilik kararı ve uygun güvencelerin olmaması nedeniyle böyle aktarımların olası risklerine dair veri sahibinin bilgilendirilmesi”* gibi ilave gereksinimler öngörülmüştür. Şunu da belirtmek gerekir ki açık rızaya dayalı aktarımlarla ilgili hükümler, kamu yetkilerinin kullanımı hususunda kamu kuruluşlarının faaliyetine uygulanmaz (m.49/f.3).

95/46/EC sayılı DPD’de veri sahibinin rızasına dayalı gerçekleşen aktarımlar için veri sahibinin *“muğlak olmayan”* rızası yeterli bulunsa da, GDPR ile bu gereksinim açık rıza olarak değiştirilmiştir. Rızaya dair yaklaşımın sıkılaştırılmasının sebebi, verilerin yeterlilik kararı bulunmayan veya uygun güvencelerin temin edilmediği üçüncü ülkelere aktarılmasının, veri korumaya dair muhtemel riskler oluşturabileceğidir⁴⁰⁶. Yine bu nedenden dolayı rızanın genel şartları içerisinde

⁴⁰³ European Data Protection Board, Guidelines 2/2018 on Derogations of Article 49 under Regulation 2016/679, 25.05.2018, s. 5, (çevrimiçi) https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-22018-derogations-article-49-under-regulation_en, 10.04.2021.

⁴⁰⁴ Kuner v.d., **Commentary**, s. 846; Küzeci, s. 195; Theodorakis, s. 42; Pelen, s. 1719; Sertçe, s. 79.

⁴⁰⁵ Aşıkoğlu/ Uzun, dn. 102, s. 952.

⁴⁰⁶ EDPB, **Derogations**, s. 6.

“bilgilendirmeye dayalı olması” yer almış olmasına rağmen, aktarımın olası risklerine dair veri sahibinin bilgilendirilmesine özellikle vurgu yapılmıştır.

Rızanın özgürce verilmiş olması, veri sahibi için gerçek bir seçim imkânı ifade eder. Eğer veri sahibinin rıza verdiği an böyle bir seçeneği olmamışsa, rıza vermeye mecbur bırakılmışsa veya verdiği rızanın olumsuz sonuçlarına katlanmak zorundaysa rıza, özgürce verilmiş olarak kabul edilmeyecektir⁴⁰⁷. GDPR’ın giriş bölümünde (madde 42) rızanın özgürce verilmiş olarak kabul edilmesi için ilgili kişinin onay vermeyi reddetme veya vermiş olduğu onayı geri alma hakkına sahip olması gerektiği belirtilmiştir. Ayrıca reddetme, ilgili kişi açısından olumsuz sonuçlara sebep olmamalıdır⁴⁰⁸.

Rızanın spesifik olması, rızanın belirli bir işleme amacı için alındığını ifade eder. Bu madde bağlamında, veri sahibinin verdiği rıza belirli bir veri aktarımı için alınmış olmalıdır⁴⁰⁹. Bu nedenle bütün veri işleme amaçları için alınmış genel nitelikli bir rıza, üçüncü ülkelere veya uluslararası kuruluşlara veri aktarımları için geçerli bir dayanak kabul edilmeyecektir. Rızanın spesifik olması, veri sahibinin veriler üzerinde kontrolünü ve şeffaflığı sağlamayı amaçlamaktadır⁴¹⁰.

Alınan rızanın spesifik olması şartı, “bilgilendirilmiş olma” unsuru ile doğrudan bağlantılıdır⁴¹¹. Şöyle ki, rıza alınmadan önce veri sahibi en azından; veri sorumlusunun kimliği, aktarılacak verilerin kategorileri, veri aktarımının amacı, verilen rızanın geri alınabilmesi hakkı vs. hususlarda bilgilendirilmelidir⁴¹². Bu gibi genel bilgilerin dışında, madde 49’dan da açıkça anlaşıldığı üzere, veri sahibi, yalnızca aktarımın kendisine yönelik risklerine dair bilgilendirildikten sonra, kişisel verilerinin aktarılmasına rıza gösterecektir. Bu gibi uyarılar, örneğin üçüncü ülkede

⁴⁰⁷ European Data Protection Board, Guidelines 05/2020 on Consent under Regulation 2016/679, 04.05.2020, par. 13, s. 7,

edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_202005_consent_en.pdf, 08.08.2021.

⁴⁰⁸ Şehriban İpek Aşıkoğlu/ Fatih Burak Uzun, “Kişisel Verilerin Yurtdışına Aktarımının Açık Rızaya Dayandırılmasının Yarattığı Sorunlar ve Çözüm Önerileri”, **Prof. Dr. Türkan Rado’nun Anısına Armağan**, Yayına Hazırlayan: Abuzer Kendigelen, İstanbul, On İki Levha, 2020, s. 943; EDPB, **Consent**, s. 13.

⁴⁰⁹ EDPB, **Derogations**, s. 7.

⁴¹⁰ EDPB, **Derogations**, a.y.

⁴¹¹ EDPB, **Derogations**, a.y.

⁴¹² EDPB, **Consent**, s. 15.

yetkili bir denetim makamının bulunmayabileceği, veri işleme ilkelerinin veya veri sahibi haklarının üçüncü ülkede sağlanmayabileceği bilgisini içermelidir⁴¹³. Her bir aktarım veya aktarım dizisi için ayrıca bilgilendirme yapılacağı için, alınan rıza da sadece o aktarıma özel ve onunla sınırlı olacaktır.

Rızanın “tereddüte yer vermeyecek açıklıkta olması” gerekmektedir. Tereddüte yer bırakmayacak açıklıkta rıza, veri sahibinin verilerinin aktarılmasına dair niyeti olduğunu ifade etmelidir⁴¹⁴. “Tereddüte yer vermeyecek şekilde aktif hareket” şartı rıza kavramını açık rızayla yaklaştırmıştır⁴¹⁵. EDPB’ye göre, rızanın açıkça verilmiş olması, onun ilgili veri sahibi tarafından verilme biçimini ifade eder. Rızanın tereddüte yer bırakmayacak açıklıkta olması, ilgili kişinin rızasını aktif davranışla açıklamasını gerektirir. Bu bakımdan örtülü irade beyanı olan susma (eylemsizlik), kabul niteliğinde bir irade beyanı olarak kabul edilmeyecektir⁴¹⁶. Bu, veri sahibinin açık bir kabul beyanı vermesi gerektiği anlamına gelir⁴¹⁷. EDPB’ye göre, rızanın açık bir şekilde verilmiş olmasından emin olmanın en risksiz yolu, yazılı bir beyan şeklinde verilmesidir. Fakat açık rızanın verilmesi için yazılı ve imzalı bir beyan tek yol değildir. Bunun yanı sıra çevrimiçi yollarla ilgili kişinin form doldurması, e-posta ile imza içeren taranmış belgenin iletilmesi veya e-imza ile verilecek olan rızanın açık rıza koşullarını karşılayabileceği belirtilmiştir⁴¹⁸.

Açık rızaya ilişkin düzenlemeler hem Türk hem AB mevzuatında yer alsa da AB’de istisna olarak uygulanan açık rızanın, Türk hukukunda kişisel veri aktarımlarının merkezinde bulunması nedeniyle, konuyla ilgili detaylı açıklama çalışmanın bir sonraki bölümüne bırakılmıştır⁴¹⁹.

2. Sözleşmenin Yürütülmesi

GDPR m.49/f.1/b uyarınca, ilgili kişi ile veri sorumlusu arasındaki bir sözleşmenin yürütülmesi veya ilgili kişinin talebiyle sözleşme öncesi alınan tedbirlerin uygulanması açısından gerekli olduğu takdirde, kişisel veriler üçüncü

⁴¹³ EDPB, **Derogations**, s. 7

⁴¹⁴ EDPB, **Derogations**, s. 11.

⁴¹⁵ Aşıkoğlu/ Uzun, s. 950.

⁴¹⁶ Giakoumopoulos/ Buttarelli/ O’Flaherty, **Handbook**, s. 149.

⁴¹⁷ EDPB, **Consent**, par. 93, s. 20.

⁴¹⁸ EDPB, **Consent**, par. 94, s. 21.

⁴¹⁹ Bkz.: aş., Üçüncü Bölüm “Açık Rızaya Dayalı Aktarımlar” başlığı.

ülkelere veya uluslararası kuruluşlara aktarılabilecektir. “Sözleşmenin yürütülmesi” yeterince geniş bir kavram olduğu için, üçüncü ülkelere veya uluslararası kuruluşlara yapılacak aktarımların kapsamını daraltmak amacıyla GDPR Giriş bölümü 111. maddesinde, söz konusu aktarımların “ara sıra yapılan” (*occasional*) olması ve sözleşmenin yürütülmesi için “gerekli” (*necessary*) olması şartı getirilmiştir.

Gereklilik testinde (*necessity test*), veri sahibi ile sözleşme arasında yakın ve gerçek bir bağ bulunması şarttır⁴²⁰. Örneğin, turizm acenteleri tarafından müşterilerine ait kişisel verilerin, yurt dışında konaklayacağı otellere aktarılması, bu çerçevede değerlendirilebilir. Çünkü veri aktarımı ve sözleşmenin amacı (müşterinin seyahatini organize etmek) arasında yakın bir bağ bulunmaktadır⁴²¹. Sözleşmenin amacının, üçüncü ülkelere veya uluslararası kuruluşlara veri aktarımı yapılmadan yerine getirilebilmesi durumunda, bu tür bir aktarım gereksizdir ve bu nedenle istisna kapsamında değerlendirilemez⁴²². Madde 29 Çalışma Grubu’na göre şirketler grubunun, örneğin grubun ödeme ve insan kaynakları yönetimi işlevlerini bir merkezde toplamak amacıyla, bağlı şirketlerden ana şirkete insan kaynakları verilerini aktarması için yasal dayanak oluşturamaz. Zira sözleşmenin yerine getirilmesi ile aktarım arasında doğrudan ve objektif bir bağlantı olmadığından, bu tür bir aktarım bir iş sözleşmesinin ifası için gerekli nitelikte olamaz⁴²³.

Diğer önemli husus ise aktarımın ara sıra yapılan olmasıdır. Bu durum, her somut olay açısından ayrıca değerlendirilmelidir⁴²⁴. Burada kast edilen, aktarımın bir kereye mahsus gerçekleşmesi değil, düzenli bir şekilde tekrarlanmamasıdır. Başka bir deyişle aktarım birkaç kez gerçekleşecek olsa dahi, bunun rastlantı olması ve önceden planlanmış bir şekilde gerçekleşmemesi gerekir⁴²⁵. Örneğin, müşterinin ödeme yapma talebini yerine getirmek için AB’deki bir banka, müşterinin kişisel verilerini üçüncü bir ülkedeki bankaya aktarıyorsa bu aktarım, iki banka arasında istikrarlı bir işbirliği çerçevesinde gerçekleşmediği sürece, müşteri talebine bağlı

⁴²⁰ Kuner v.d., **Commentary**, s. 848.

⁴²¹ EDPB, **Derogations**, s. 9.

⁴²² Voigt/ Bussche, s. 130.

⁴²³ Article 29 Working Party, Working Document on a Common Interpretation of Article 26(1) of Directive 95/46/EC of 24 October 1995, 25.11.2005, s. 13, (çevrimiçi), ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2005/wp114_en.pdf, 20.06.2021.

⁴²⁴ EDPB, **Derogations**, s. 9.

⁴²⁵ Bilgi Information Technology Law Institute, s. 22.

olarak birkaç kez gerçekleşse bile ara sıra yapılan aktarım olarak değerlendirilebilir⁴²⁶. Bunun aksine, çok uluslu bir şirketin üçüncü bir ülkedeki bir eğitim merkezinde eğitimler düzenlediği ve bu eğitim kursuna katılan çalışanların kişisel verilerini düzenli olarak aktardığı durumlarda aktarımlar “ara sıra yapılan” olarak nitelendirilmez. İstikrarlı bir ilişki içinde düzenli olarak gerçekleşen veri aktarımları, sistematik ve tekrarlayan olarak kabul edilir ve bu nedenle ara sıra yapılma niteliğini aşar⁴²⁷.

Hükümde aktarıma konu olan verilerin kime ait olması gerektiği yönünde bir açıklama bulunmasa da, hem sözleşmesel ilişkinin doğası gereği hem de istisnanın kapsamını genişletmemek adına sadece sözleşme taraflarına ait kişisel verilerin bu kapsamda değerlendirilmesi gerektiğine dair görüşe katılıyoruz⁴²⁸.

GDPR m.49/f.3’te söz konusu istisnanın kapsamını daraltan bir diğer düzenlemeye daha yer verilmiştir. Buna göre, bu istisna kapsamındaki hükümler, kamu yetkilerinin kullanımı hususunda kamu kuruluşlarının faaliyetine uygulanmayacaktır.

3. İlgili Kişi Yararına Sözleşmenin İmzalanması veya Yürütülmesi

GDPR m.49/f.1/c uyarınca, ilgili kişi yararına veri sorumlusu ile başka bir gerçek veya tüzel kişi arasında yapılan bir sözleşmenin imzalanması veya yürütülmesi için aktarımın gerekli olması durumunda kişisel veriler üçüncü ülkeye aktarılabilecektir. GDPR m.49/f.1/b’den farklı olarak, bu istisna kapsamındaki sözleşme, ilgili kişi yararına düzenlense de, ilgili kişi söz konusu sözleşmenin tarafı değildir⁴²⁹. İlgili kişinin taraf olmadığı bir sözleşme kapsamında kişisel verilerinin üçüncü ülkelere veya uluslararası kuruluşlara aktarılmasını hukuka uygun hâle getiren husus, sözleşmenin ilgili kişi menfaatine yapılacak olmasıdır⁴³⁰. Yapılacak aktarım ile sözleşmenin amacı arasında yakın ve önemli bir ilişki bulunmalıdır⁴³¹. Yukarıdaki örnekte olduğu gibi, bir turizm şirketinin rezervasyon yapmak amacıyla

⁴²⁶ EDPB, **Derogations**, s. 9.

⁴²⁷ EDPB, **Derogations**, s. 9

⁴²⁸ Çelik, s. 180.

⁴²⁹ Sertçe, s. 89; Çelik, s. 181.

⁴³⁰ Çelik, a.y.

⁴³¹ EDPB, **Derogations**, s. 9-10.

müşterisine ait kişisel verileri üçüncü ülkede bulunan bir otele aktarması m.49/f.1/b kapsamında değerlendirilirken, üçüncü ülkede bulunan ülkeye müşterinin aile bireylerine ait kişisel verilerin aktarılması ise m.49/f.1/c kapsamında değerlendirilecektir.

Bir önceki istisna kapsamında, aktarımın “gerekli” ve “ara sıra yapılan” olması ile ilgili belirtilenler bu istisna için de geçerlidir. Ayrıca GDPR m.49/f.3 uyarınca, bu istisna kamu yetkilerinin kullanımı hususunda kamu kuruluşları tarafından gerçekleştirilen faaliyetler kapsamında uygulanmamaktadır.

4. Kamu Yararı

GDPR m.49/f.1/d uyarınca, aktarımın kamu yararına ilişkin önemli sebeplerden dolayı gerekli olduğu durumlarda kişisel veriler üçüncü ülkelere veya uluslararası kuruluşlara aktarılabilir. GDPR’ın giriş bölümünde bu duruma örnek olarak vergi, gümrük veya mali denetim kurumları arasında veya kamu sağlığı veya sosyal güvenlikle ilgili konularda yetkili birimler arasında uluslararası veri aktarımları gösterilmiştir (GDPR Giriş par. 112).

Burada “kamu yararı” ölçütünün dar çerçevede yorumlanması gerekir. Zira aksi takdirde istisnanın sınırları maddenin amacı ile örtüşmeyecek şekilde genişleyebilir⁴³². İstisnanın kapsamını daraltmak için m.49/f.4’te kamu yararının, yalnızca Birlik hukuku veya veri sorumlusunun tabi olduğu ülke mevzuatında tanındığı durumlarda geçerli olacağı belirtilmiştir. Fakat söz konusu “kamu yararı”nın AB veya veri sorumlusunun tabi olduğu üye devlette genel olarak, soyut anlamda mevcut olması, böyle bir aktarım için yeterli değildir⁴³³. Örneğin, üçüncü bir ülkenin yetkili makamı, terörizmle mücadeleyle yönelik soruşturma kapsamında kişisel veri aktarımı talebinde bulunmuşsa, AB veya veri sorumlusunun tabi olduğu üye devlette sadece terörizme karşı mevzuatın varlığı, henüz aktarımın gerçekleşmesi için önemli sebep olarak kabul edilemez. EDPB’ye göre, bu istisna sadece, AB veya üye devletin yasalarında, uluslararası işbirliği için karşılıklılık da dâhil olmak üzere

⁴³² Küzeci, s. 195-196; Arslan, s. 470; Sertçe, s. 91.

⁴³³ Kuner v.d., **Commentary**, s. 850; Sertçe, s. 89.

önemli kamu yararı amaçları için bu tür aktarımlara izin verildiği sonucuna varıldığında uygulanabilir⁴³⁴.

Kamu yararına dayalı kişisel veri aktarımları, esasen kamu kuruluşları tarafından kullanılmak üzere düşünülse de, özel kuruluşların da bu düzenleme kapsamında veri aktarımı gerçekleştirmesi için bir engel yoktur. Başka bir deyişle, bu istisnanın uygulanabilmesi için önemli olan veriyi aktaran veya kabul eden kuruluşun niteliği değil, önemli kamu yararının bulunmasıdır⁴³⁵.

5. Hukuki İddialarda Bulunulması, Bu İddiaların Uygulanması veya Savunulması

GDPR m.49/f.1/e uyarınca, kişisel verilerin üçüncü ülkelere veya uluslararası kuruluşlara aktarılabilmesi belirli durumlardan biri de hukuki iddialarda bulunulması, bu iddiaların uygulanması veya savunulması bakımından aktarımın gerekli olmasıdır.

Hukuki iddialarda bulunma, bu iddiaların uygulanması ve savunulması kendi başına çok geniş kavram olmasının yanı sıra, GDPR giriş bölümü 111. paragrafta, bu istisnanın, düzenleyici kurumlar önündeki prosedürler de dâhil olmak üzere, adli veya idari ya da mahkeme dışı herhangi bir prosedürde olup olmadığına bakılmaksızın her türlü hukuki iddialar için geçerli olduğu belirtilmiştir. Bu açıklamayla istisnanın kapsamı, düzenlemenin amacıyla örtüşmeyecek şekilde genişleyerek istisnadan ziyade bir kural niteliği kazanacaktır. Bunun önüne geçmek için açıklamanın devamında, aktarımların sadece “ara sıra yapılan” ve “gerekli” olduğu durumlarda bu istisnanın uygulanabileceği vurgulanmıştır⁴³⁶. Örneğin, üçüncü bir ülkedeki cezai veya idari soruşturma bağlamında, kişinin kendini savunmak veya herhangi bir cezadan indirim veya feragat elde etmek amacıyla kişisel verilerin aktarılması talep ediliyorsa, bu istisnaya dayanarak aktarım gerçekleştirilebilir. Çünkü aktarım, yasal hakkın kullanımı için gereklidir ve somut olayla sınırlıdır.

⁴³⁴ EDPB, **Derogations**, s. 10.

⁴³⁵ EDPB, **Derogations**, s. 11.

⁴³⁶ EDPB, **Derogations**, a.y.

Bu istisna, gelecekte hukuki işlemlerin veya prosedürlerin başlatılabileceği ihtimaline dayalı olarak kişisel verilerin aktarımını gerekçelendirmek için kullanılamaz. Bu bakımdan ortada somut bir sürecin bulunması ve bu süreç ile aktarım arasında önemli ve yakın bir ilişki bulunması gerekmektedir⁴³⁷. Bu istisnanın uygulanamayacağı bir diğer husus ise ulusal mevzuatta kişisel verilerin, yabancı ülkelerin mahkeme veya diğer resmî kurumlarına aktarılmasını yasaklayan veya kısıtlayan düzenlemelerin bulunmasıdır⁴³⁸.

6. Hayati Menfaatlerinin Korunması

GDPR m.49/f.1/f uyarınca, kişisel verilerin üçüncü ülkelere veya uluslararası kuruluşlara aktarılabileceği diğer bir istisna ise, ilgili kişinin fiziksel veya hukuki engeller sebebiyle rıza vermesinin mümkün olmadığı ve aktarımın ilgili kişinin veya diğer kişilerin hayati menfaatinin korunması açısından gerekli olduğu durumlardır. İlgili kişinin sağlığına ilişkin acil bir durumda, tıbbi yardım gösterilebilmesi için verilerin aktarılması gerekli ise, bu istisna kapsamında gerçekleştirilmesi söz konusu olacaktır⁴³⁹. Bu tür durumlarda ilgili kişinin hayatına karşı ciddi risklerin, veri korumaya karşı risklerden daha ağır bastığı düşünülmektedir⁴⁴⁰. Hükümden açıkça anlaşıldığı üzere, herhangi bir aktarımın bu istisna çerçevesinde değerlendirilebilmesi için aynı anda iki şartın mevcut olması gerekmektedir:

1. Aktarımın, hayati çıkarlarla ilgili olması

Sağlıkla ilgili acil tıbbi müdahale gereken durumlarda, söz konusu olan tıbbi müdahalenin gerçekleştirilmesi, kişisel verilerin aktarılmasıyla doğrudan bağlantılı olmalıdır. Bu yüzden aktarımın amacı, hayatı çıkarları söz konusu olan ilgili kişiye tıbbi yardım göstermek değil de örneğin, genel tıbbi araştırmayı yürütmekse aktarıma hukuki nitelik kazandırmak adına bu istisna kullanılmayacaktır⁴⁴¹.

2. Fiziksel veya hukuki olarak rıza verememe durumu

⁴³⁷ EDPB, **Derogations**, s. 12.

⁴³⁸ EDPB, **Derogations**, a.y.

⁴³⁹ Küzeci, s. 195.

⁴⁴⁰ EDPB, **Derogations**, s. 13

⁴⁴¹ EDPB, **Derogations**, a.y.

Madde metninde sadece fiziksel olarak rıza gösterememekten bahsedilse de EDPB, ilgili kişinin rıza verememesinin fiziksel, zihinsel veya hukuki yetersizlikle ilgili olabileceği sonucuna varmıştır⁴⁴².

Hukuken yetersizlik durumlarına örnek olarak, reşit olmayan bir kişinin rızasının alınması gereken durumlar gösterilebilir. Hukuki ve zihinsel yetersizlik, duruma bağlı olarak, ilgili kişinin hukuki durumunu teyit eden resmî bir belge veya ilgili kişinin zihinsel yetersizliğini gösteren tıbbi rapor ile kanıtlanmalıdır⁴⁴³.

Hayati menfaatlerin söz konusu olduğu bazı durumlarda ise ilgili kişilerin rıza veremeyecek durumda olması yalnızca ihtimal edilebilir. Bu gibi durumlara örnek olarak, doğal afetlerin meydana gelmesinden sonra, arama kurtarma çalışmaları kapsamında kişisel verilerin ilgili kurum veya kişilere (örneğin, acil servis çalışanları veya afet kurbanlarının yakınları vs.) aktarılması gösterilebilir. Böyle durumlarda verileri aktarılan kişilerin, fiziksel olarak rıza veremeyecek durumda olması kuvvetle muhtemeldir⁴⁴⁴.

Bu istisnanın, aktarımın hukuki dayanağını teşkil edebilmesi için yukarıda bahsi geçen her iki şartın aynı anda bulunması gerekmektedir. Örneğin, ilgili kişinin hayati çıkarları söz konusu olsa bile, kendi rızasını ifade edebilecek durumda ise aktarım bu istisnanın dışında kalacaktır. Böyle durumlarda ilgili kişi, rızasını ifade edebilecek durumda olduğundan açık rızaya dayalı aktarım gerçekleştirilebilir.

7. Aktarımın Kamuoyuna Açık Bir Sicilden Yapılması

GDPR m.49/f.1/g uyarınca, aktarımın Birlik veya üye devlet hukukuna göre kamuoyuna bilgi sağlanmasının amaçlandığı ve genel olarak kamuoyu veya meşru bir menfaati gösterebilen herhangi bir kişi tarafından istişareye açık olan bir sicilden yapılması hâlinde kişisel veriler üçüncü ülkelere veya uluslararası kuruluşlara aktarılabilecektir.

Sicilin herkese açık olması, bu istisnanın mantıksal temelini oluşturmaktadır. Şöyle ki, ilgili ülkede meşru menfaati olan herkes bu bilgilere ulaşabiliyorsa, üçüncü

⁴⁴² EDPB, **Derogations**, a.y.

⁴⁴³ EDPB, **Derogations**, a.y.

⁴⁴⁴ EDPB, **Derogations**, s. 13.

ülkelerde bulunan kişilerin de onlara ulaşmasında bir engel bulunmamalıdır⁴⁴⁵. Söz konusu siciller, Birlik veya üye devlet yasalarına göre, kamuya bilgi sağlama amacını taşımalıdır. Bu nedenle, özel kuruluşların sorumluluğunda olan siciller, bu istisnanın kapsamı dışındadır⁴⁴⁶.

Sicilin kamuya bilgi sağlama amacının yanı sıra, genel olarak kamuoyu veya meşru menfaatinin gösterebilen herhangi bir kişi tarafından istişareye açık olması gerekmektedir. Ayrıca maddede öngörülen bu gibi koşulların yanı sıra, bu kayıtlardan aktarımlar yalnızca, Birlik veya üye devlet kanunları ile belirlenen koşullar, ilgili durumda yerine getirildiği ölçüde gerçekleştirilebilir⁴⁴⁷.

Bu çerçevede gerçekleştirilen aktarımların istisnai niteliğini korumak için sadece sicile yönelik değil, aynı zamanda sicilde bulunan kişisel verilere de yönelik sınırlama öngörülmüştür. Şöyle ki aktarım, sicilde bulunan bütün kişisel verileri veya tüm kişisel veri kategorilerini içermez. Sicilin, meşru bir menfaati bulunan kişilerin incelemesine yönelik hâllerde, yalnızca bu kişilerin talebi üzerine veya bu kişilerin alıcı olması hâlinde, aktarım yapılır (GDPR m.49/f.2). Aksi takdirde, bu istisnanın, sicillerin içeriğini boşaltmak amacıyla kullanılması, maddenin doğasına uygun olmayacaktır. Ayrıca böyle durumlarda, kamuya hizmet etmek amacı bulunan sicillerden aktarılan verilerin, üçüncü ülkede bulunan kuruluşlar tarafından toplandıkları amaç dışında kullanılması riski de mevcuttur⁴⁴⁸.

Bu istisnaya örnek olarak, AB ülkesinde doğmuş ancak üçüncü bir ülkede ikamet eden bir kişi tarafından, daimi ikametgâh almak için doğum yerinden kişi hâllerine ilişkin belgelerinin ekstrelerini elde etmek amacıyla, ulusal yasalara uyumlu şekilde kullanıldığı durumlar gösterilebilir⁴⁴⁹.

8. Veri Sorumlusunun Zorlayıcı Meşru Menfaati

Daha önce 95/46/EC sayılı DPD’de yer almayan düzenlemeye göre, yeterlilik kararı veya uygun güvenlik önlemlerinin olmadığı, hatta yukarıda bahsi geçen

⁴⁴⁵ Küzeci, s. 195; Article 29 WP, **Common Interpretation of Article 26(1)**, s. 16.

⁴⁴⁶ EDPB, **Derogations**, a.y.

⁴⁴⁷ Bilgi Information Technology Law Institute, s. 90.

⁴⁴⁸ Başalp, **Kişisel Veriler**, s. 72-73; Arslan, s. 471; Article 29 WP, **Common Interpretation of Article 26(1)**, s. 16.

⁴⁴⁹ Article 29 WP, **Common Interpretation of Article 26(1)**, a.y.

istisnalardan herhangi birinin bulunmadığı durumlarda bile, GDPR’da kesin olarak belirtilen bazı koşullar altında ve veri sorumlusunun zorlayıcı meşru menfaatlerinin (*compelling legitimate interests*) gerektirdiği durumlarda kişisel verilerin üçüncü ülkelere veya uluslararası kuruluşlara aktarımı gerçekleştirilebilir (m.49 par. 2). Madde metninden de anlaşıldığı üzere, bu düzenleme GDPR kapsamında kişisel verilerin aktarılması için uygulanabilecek son çare (*a last resort*) olarak öngörülmüştür⁴⁵⁰. Bu doğrultuda, öncelikle aktarımı gerçekleştirmek için hiçbir hukuki dayanağın (yeterlilik kararı, uygun güvenlik önlemleri, istisnalar) bulunmadığı veri aktaran tarafından kanıtlanmalı, daha sonra ise aktarımın aşağıdaki spesifik özelliklere sahip olup olmadığı belirlenmelidir:

1. Aktarımın tekrarlamayan (*not repetitive*) olması - aktarımın sadece bir kere yapılmış olmasın; değil, bir kereden fazla tekrarlanırsa bile bunun devamlı olarak, düzenli bir şekilde gerçekleşmemesini ifade etmektedir (örneğin; rastgele, önceden kesin belli olmayan koşullar altında vs.)⁴⁵¹.

2. Sınırlı sayıda veri sahibiyle ilgili olması - EDPB, bu hususla ilgili mutlak bir sınır çizilmesinin imkânsızlığını dikkate alarak “sınırlı sayıda” kavramının kaç veri sahibini kapsayacağını belirlemek için, somut aktarımın özelliklerinin dikkate alınması gerektiğine kanaat getirmiştir⁴⁵².

3. Veri sahibinin haklarının baskın olmadığı durumlarda, veri sorumlusu tarafından gözetilen zorlayıcı meşru menfaatler doğrultusunda gerekli olması - İstisnanın kapsamına sadece veri aktaran veri sorumlularının meşru menfaatleri dâhildir. Başka bir deyişle, veri alıcıları ve veri aktaran veri işleyenlerin meşru menfaatleri bu istisna kapsamında değerlendirilmeyecektir⁴⁵³. İstisnanın kapsamını biraz daha daraltan ise m.6/f.1/f’de bahsi geçen, veri sorumlusunun bütün meşru menfaatlerinin değil sadece “zorlayıcı” olanların dikkate alınmasıdır. Örneğin, bir veri sorumlusu, şirketini ani bir zarardan veya işi ciddi şekilde etkileyecek bir cezadan korumak için kişisel verileri aktarmak zorunda kalıyorsa bu durum söz

⁴⁵⁰ EDPB, **Derogations**, s. 14.

⁴⁵¹ EDPB, **Derogations**, s. 4.

⁴⁵² EDPB, **Derogations**, s. 15.

⁴⁵³ Hon, s. 215.

konusu olabilir. Böyle durumlarda veri sorumlusu, veri sahibini m.13 ve m.14'deki bilgilere ek olarak, gözetilen meşru menfaatleri konusunda da bilgilendirmelidir. Ayrıca, veri sorumlusunun meşru menfaatleri ve veri sahibinin hakları, özgürlükleri veya meşru menfaatleri arasında yapılan denge testi sonucunda, kişisel verilerin aktarılmasının, veri sahibinin hakları için tehlike arz ettiği ortaya çıkarsa, veri sahibinin hakları daha ağır bastığı için aktarım bu istisnaya dayanamayacaktır⁴⁵⁴.

4. Veri aktarımı ile ilgili tüm durumların veri sorumlusu tarafından değerlendirmiş olması ve bu değerlendirmeye dayalı olarak kişisel verilerin korunması ile ilgili uygun güvenceleri sağlamış olması - Değerlendirme zamanı özellikle, veri sahibinin hakları, aktarımın bu haklara olumsuz etkisi, fiziksel, maddi veya maddi olmayan her türlü zarar vs. dikkate alınmalıdır. Bu riskleri değerlendirirken ve belirli koşullar altında neyin veri sahibinin hakları ve özgürlükleri için “uygun güvence” olarak kabul edilebileceği belirlenirken, veri aktaran veri sorumlusu, verilerin doğasını, işleme amacını ve süresini, menşe ülkede ve nihai varış ülkesindeki durumu dikkate almalıdır (GDPR Giriş bölümü 113). Bütün durumlar için geçerli olan uygun güvencelerin belirlenmesi imkânsız olduğundan, söz konusu aktarımın spesifik özellikleri göz önünde bulundurularak karar verilmelidir. Veri sorumlusu, veri sahibini uygun güvenceler ve bunların bir nüshasının elde edilme yolları hakkında bilgilendirmelidir (GDPR m.13/f.1/f, m.14/f.1/f). Veri sahibinin yanı sıra, yetkili denetim makamının da aktarımla ilgili bilgilendirilmesi gerekmektedir. Fakat bu bilgilendirme, denetim makamının aktarımı onaylaması gerektiği anlamına gelmemelidir⁴⁵⁵.

E. Uluslararası Anlaşmalara Dayalı Aktarımlar

1. Genel Olarak

Her ne kadar GDPR'ın 5. bölümünde yer verilmesi de kişisel verilerin, AB'den üçüncü ülkelere aktarılmasının bir diğer yolu da uluslararası anlaşmalardır.

⁴⁵⁴ EDPB, **Derogations**, s. 15.

⁴⁵⁵ EDPB, **Derogations**, a.y.

Avrupa Birliği'nin İşleyişi hakkında Anlaşma'nın⁴⁵⁶ (TFEU) 216. maddesi uyarınca, yasal bağlayıcılığı olan bir AB düzenlemesinde öngörüldüğü durumlarda, Birlik, bir veya daha fazla üçüncü ülke veya uluslararası kuruluşla anlaşma akdedebilecektir.

Bu anlamda kişisel verilerin üçüncü ülkelere transferi için uluslararası anlaşma akdedilebileceğini öngören tek AB düzenlemesi, GDPR'ın giriş bölümünün 102. maddesidir⁴⁵⁷. Şöyle ki burada GDPR'ın, AB ile üçüncü ülkeler arasında akdedilen ve kişisel verilerin aktarımını düzenleyen uluslararası anlaşmalara hâlel getirmeyeceği hükme bağlanmıştır. Bu tür anlaşmalar veri sahipleri için uygun korumaları içermelidir. Aynı zamanda bu tür anlaşmalar GDPR ve AB hukukunun diğer hükümlerini etkilemediği müddetçe, üye devletler de üçüncü ülkelerle veya uluslararası kuruluşlarla veri sahiplerinin temel haklarına uygun düzeyde koruma sağlayan uluslararası anlaşmalar akdedebilirler. AB ve üçüncü ülkeler arasında belirli amaçlarla kişisel veri aktarımlarını düzenleyen uluslararası anlaşmalara Yolcu İsim Kayıtları (PNR) anlaşmaları, Dünya Bankalararası Finansal İletişim Birliği (SWIFT) anlaşması örnek olarak gösterilebilir. Adı geçen sözleşmeler, GDPR kabul edilene kadar imzalanmış olsalar da yürürlükte kalmaya devam etmektedirler. Zira GDPR m.96 uyarınca, *“kişisel verilerin üçüncü ülkelere veya uluslararası kuruluşlara aktarılması hususunda üye devletler tarafından 24 Mayıs 2016 tarihinden önce imzalanan ve bu tarihten önce geçerli Birlik hukukuna uyumlu olan uluslararası anlaşmalar değiştirilene, yenilenene veya yürürlükten kaldırılana kadar yürürlükte kalır”*.

a. PNR Anlaşmaları

PNR verileri, hava taşıyıcıları tarafından uçuş rezervasyon sürecinde toplanan yolcuların isimleri, adresleri, kredi kartı bilgileri ve koltuk numaraları gibi bilgileri içerir⁴⁵⁸. Terör saldırılarının veya ciddi uluslararası suçların önlenmesi, tespiti, soruşturulması ya da yargılanmasının sağlanması için AB belirli üçüncü ülkelerle

⁴⁵⁶ The Treaty on the Functioning of the European Union, 25.03.1957, (çevrimiçi), https://eur-lex.europa.eu/resource.html?uri=cellar:9e8d52e1-2c70-11e6-b497-01aa75ed71a1.0006.01/DOC_3&format=PDF, 31.01.2021.

⁴⁵⁷ Kuner v.d., **Commentary**, s. 760; Christopher Kuner, “Data Protection, Data Transfers, and International Agreements: the CJEU’s Opinion 1/15”, (çevrimiçi), <https://verfassungsblog.de/data-protection-data-transfers-and-international-agreements-the-cjeus-opinion-115/>, 22.10.2021; Sertçe, s. 101.

⁴⁵⁸ Giakoumopoulos/ Buttarelli/ O’Flaherty, **Handbook**, s. 266.

(ABD, Kanada ve Avustralya) PNR verilerinin aktarımı hususunda anlaşmalar yapmıştır. Hâlihazırda AB ve Japonya arasında PNR verilerinin aktarımı doğrultusunda müzakereler devam etmektedir.

Bu anlaşmaların akdedilme ihtiyacı, 11 Eylül 2001 tarihinde gerçekleşen terör saldırısından sonra ülkelerin terörle mücadele kapsamında daha sıkı önlemler alma kaygısından kaynaklanmıştır⁴⁵⁹. Bu tedbirler çerçevesinde ABD’li güvenlik güçlerinin PNR bilgilerini paylaşmayı reddeden havayolu şirketlerine yaptırım uygulaması (örneğin; para cezası, inişe izin vermeme vs.) sonucu, birçok havayolu şirketleri bu verileri paylaşmak zorunda kalmıştır. Kişisel verilerin transferi hususunda her ülkede yeterli hukuki düzenleme bulunmadığı ve özellikle ABD düzenlemeleri AB standartlarıyla uyumlu olmadığı için bu denli geniş ve ayrıntılı aktarım AB otoriteleri tarafından eleştirilmiştir⁴⁶⁰. 2003 yılında Avrupa Komisyonu, PNR uygulamalarının 95/46/EC sayılı DPD’ye aykırı olduğu konusundaki endişelerini ifade etmiştir⁴⁶¹.

Bunun üzerine yapılan müzakereler sonucunda, 2004 yılında PNR bilgilerinin ABD’ye yasal bir biçimde aktarımını düzenleyen ilk anlaşma akdedilmiştir. Fakat Avrupa Parlamentosu, anlaşmayı imzalarken Komisyon’un yetkilerini aştığını ve kendisinin görüşünün alınmadığını ileri sürerek iptal edilmesi için ABAD nezdinde dava açmıştır⁴⁶². ABAD, aktarılabilecek verilerin ihtiyaç duyulandan fazla olması, verilerin sağlanma amacının net bir biçimde ifade edilmemesi, ABD tarafından gereğinden fazla bir sürede tutulabileceği vs. gibi gerekçelerle bu anlaşmayı iptal etmiştir⁴⁶³. Bahsedilen sorunları ortadan kaldırmak için 2006, 2007 ve 2011

⁴⁵⁹ Salih Benli, “Yolcu İsim Kayıtları”, **Terazi Hukuk Dergisi**, C. 10, S. 103, 2015, s. 41; Gizem Gültekin Varkonyi, “Yolcu İsim Kayıtlarının Terörle Mücadele Kapsamında Yurt Dışına Yasal Aktarımı: Avrupa Birliği Uygulamaları ve Türkiye”, **Türkiye Barolar Birliği Dergisi**, C. 30, S. 132, 2017, s. 341; Küzeci, s. 207.

⁴⁶⁰ Gültekin Varkonyi, s. 342.

⁴⁶¹ Gültekin Varkonyi, s. 357.

⁴⁶² Küzeci, s. 207; Kaya, **Transfer of Personal Data**, s. 31; Mehmet Özcan/ Fatma Yılmaz, “Pendulum Swings in between Civil Rights and Security: EU Policies against Terrorism in the Light of the PNR Case”, **Uluslararası Hukuk ve Politika Dergisi**, C. 3, S. 12, 2007, s. 59.

⁴⁶³ ABAD, Joined Cases C-317/04 and C-318/04, 30.05.2006, (çevrimiçi), <https://eur-lex.europa.eu/legal-content/en/txt/pdf/?uri=celex:62004cj0317&from=en>, 31.01.2021.

yıllarında yeni anlaşmalar imzalanmıştır. 26 Nisan 2012 tarihli Konsey kararı⁴⁶⁴ ile yürürlüğe giren anlaşma hâlen AB ve ABD arasında PNR verilerinin aktarımını düzenlemektedir⁴⁶⁵.

Bu tür anlaşmaların AB hukukunun diğer hükümlerini etkilememesi gerektiğinden, kişisel verilerin bu anlaşmalara dayalı olarak geniş bir şekilde ABD'ye aktarılması, Avrupa İnsan Hakları Sözleşmesi⁴⁶⁶ m.7, m.8 ve TFEU m.16'da yer alan temel haklar bağlamında AB kamuoyunda tartışmalara neden olmuştur⁴⁶⁷. Örneğin, eleştiri alan hususlardan biri bilginin toplanma amacı ve kullanımına ilişkin olmuştur. Şöyle ki, PNR anlaşmalarında verilerin kullanılacağı kesin amaç gösterilmemiştir. İlk başlarda bu verilerin sadece terör suçlarını önlemek amacıyla kullanılması düşünülse de, yıllar içinde PNR anlaşmaları bu verilerin başkaca amaçlarla kullanımını da mümkün kılmıştır⁴⁶⁸. 2004, 2007 ve 2011 anlaşmaları karşılaştırıldığında yürürlükte olan anlaşmanın, verilerin kullanım amacını genişlettiği açıkça görülmektedir⁴⁶⁹.

Diğer eleştiri konusu ise verileri saklama süresinin orantılılık ilkesine uygun olmamasıyla ilgilidir. Şöyle ki, veri saklama süresi 2004 anlaşmasında 3.5 yıl, 2007 anlaşmasında aktif veritabanında 7 yıl, aktif olmayan veritabanında ise bu süreye ek olarak 8 yıl iken, 2011 anlaşmasının 8'inci maddesi uyarınca veriler, aktif veritabanında 5 yıl, bu süre dolduktan sonra ise aktif olmayan veritabanında 10 yıla kadar tutulabilecektir.

AB ve Kanada arasında 2006 yılında imzalan PNR anlaşmasının süresi bittikten sonra, yeni anlaşma için müzakereler başlamış ve 2014 yılında tamamlanmıştır. Fakat bu anlaşmanın da AB hukukunun diğer hükümlerine uyumluluğu tartışılmıştır. Bunun üzerine 25 Kasım 2014 tarihinde Avrupa

⁴⁶⁴ European Commission, 26.04.2012 tarihli ve 2012/472/EU sayılı karar, (çevrimiçi), <https://eur-lex.europa.eu/legal-content/en/all/?uri=celex:32012d0472>, 31.01.2021.

⁴⁶⁵ Gültekin Varkonyi, s. 343; Kaya, **Transfer of Personal Data**, s. 32.

⁴⁶⁶ Council of Europe, European Convention on Human Rights, 04.11.1950, (çevrimiçi) https://www.echr.coe.int/documents/convention_eng.pdf, 31.01.2021.

⁴⁶⁷ Benli, s. 42.

⁴⁶⁸ Benli, a.y.

⁴⁶⁹ PNR verilerinin kullanım amaçları için bkz.: ABD ile AB arasında PNR anlaşması m.4.

Parlamentosu anlaşmanın CFR m.7 ve 8 açısından ABAD'ın görüşünü talep eden karar kabul etmiş ve 10 Nisan 2015 tarihinde mahkemeye başvuruda bulunmuştur⁴⁷⁰.

ABAD konuyla ilgili, anlaşmanın AB Temel Haklar Şartı'nda öngörülen haklarla uyumsuz olduğuna ve bu nedenle akdedilemeyeceğine dair görüş sunmuştur. ABAD'a göre, anlaşma bir bütün olarak ele alındığında PNR verileri, kişiler arasındaki ilişkileri, seyahat alışkanlıklarını, finansal durumlarına dair bilgileri, beslenme alışkanlıkları ve sağlık durumlarını ortaya çıkaracak şekilde analiz edilerek kişilerin özel hayatını etkileyebilir. Bu nedenle Şart'ın 7. maddesinde öngörülen özel hayatın gizliliğine saygı hakkına bir kısıtlama getirmektedir. Aynı zamanda kişisel verilerin işlenmesi söz konusu olduğu için 8. maddeyle korunan kişisel verilerin korunması hakkına da müdahale teşkil etmektedir⁴⁷¹.

Temel haklara bu tür müdahale kamu güvenliği ve terörizme karşı mücadele yoluyla kamu yararına dayanmaktaydı. Fakat kamu yararının geçerli olması için temel haklara müdahalenin sadece ulaşılmak istenen amacın elde edilmesi için kesin surette gerekli olanlarla sınırlı olması gerekmektedir. ABAD anlaşmanın kesin surette gerekli olma kriterini karşılamadığı sonucuna varmıştır⁴⁷².

b. SWIFT Anlaşması

Kişisel verilerin aktarımlarını düzenleyen uluslararası anlaşmalara bir diğer örnek de "Terörist Finansmanı Takip Programı amacıyla finansal mesajlaşma verilerini AB'den ABD'ye aktarılması ve işlenmesi" anlaşmasıdır⁴⁷³. Bu anlaşmanın akdedilmesi ihtiyacı, ABD Hazine Bakanlığı'nın, Terörist Finansmanı Takip Programı kapsamında terörizm soruşturmaları amacıyla, Avrupa bankalarından yapılan küresel para transferlerinin çoğu için veri işleyen Belçika merkezli Dünya Bankalararası Finansal İletişim Birliği'nden (SWIFT) bazı verileri açıklamasını talep etmesi üzerine meydana gelmiştir⁴⁷⁴. AB vatandaşları hakkında olan verilerin, sadece

⁴⁷⁰ Giakoumopoulos/ Buttarelli/ O'Flaherty, **Handbook**, s. 266; Kuner, **CJEU Opinion**.

⁴⁷¹ Giakoumopoulos/ Buttarelli/ O'Flaherty, **Handbook**, s. 267; Kuner, **CJEU Opinion**.

⁴⁷² Giakoumopoulos/ Buttarelli/ O'Flaherty, **Handbook**, a.y.

⁴⁷³ Agreement between the European Union and the United States of America on the processing and transfer of Financial Messaging Data from the European Union to the United States for purposes of the Terrorist Finance Tracking Program (çevrimiçi), [https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:22010A0113\(01\)](https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:22010A0113(01)), 25.04.2021.

⁴⁷⁴ Giakoumopoulos/ Buttarelli/ O'Flaherty, **Handbook**, s. 268; Arslan, s. 478-479.

SWIFT'in veri işleme merkezlerinden birinin ABD'de bulunması gerekçesine dayanarak ABD'ye açıklanması edilmesi için AB hukuku açısından yeterli hukuki dayanak bulunmamaktaydı. Bu yüzden hem yeterli korumanın sağlanması hem de hukuki dayanağın oluşturulması maksadıyla 28 Haziran 2010 tarihinde AB ve ABD arasında SWIFT Anlaşması akdedilmiş ve 13 Temmuz 2010 tarihli Konsey kararı ile yürürlüğe girmiştir⁴⁷⁵.

Anlaşmanın 4.2. maddesine göre, aşağıdaki durumlarda SWIFT tarafından muhafaza edilen finansal verilerin terörizm ya da terörizm finansmanının engellenmesi, soruşturulması, tespiti ya da yargılaması amaçlarıyla ABD Hazine Bakanlığı'na sağlanmasına izin verilecektir:

- talep edilen verilerin mümkün olduğunca net bir şekilde ifade edilmesi,
- verilerin gerekliliğinin kanıtlanması,
- talep edilen verilerin mümkün olduğunca minimize edilmesi için tasarlanmış olması,
- Single Euro Payments Area (SEPA)'ya dâhil verileri içermemesi.

Anlaşmanın 4.3 ve 4.4. maddeleri uyarınca, ABD Hazine Bakanlığının, finansal veri aktarımına dair her bir talebinin SWIFT anlaşmasının prensiplerine uygun olup olmadığı Avrupa Polis Teşkilatı (Europol) tarafından onaylanmalıdır. Bu nedenle ABD Hazine Bakanlığı her talebin bir kopyasını Europol'a temin etmelidir.

Aktarılan veriler yalnızca terörizmin veya finansmanın önlenmesi, soruşturulması, tespiti veya kovuşturulması için işlenecektir. Herhangi yetkisiz erişim veya işleme biçimini önlemek için, aktarılan finansal veriler sadece terörizm ya da finansmanını soruşturan analistlerin erişebileceği güvenli fiziksel ortamlarda tutulmalı, finansal veriler başka bir veri tabanı ile bağlantılı olmamalı, herhangi değişiklik veya ekleme yapılmamalı ve kopyalanmamalıdır (Anlaşmanın 5. maddesi).

⁴⁷⁵ Avrupa Birliği Konseyi, 13.07.2010 tarihli ve 2010/412/EU sayılı karar, (çevrimiçi), <https://eur-lex.europa.eu/legal-content/en/txt/html/?uri=celex:32010d0412&from=cs>, 05.02.2021.

Anlaşmada ileri aktarımlar için de kurallar belirlenmiştir. Şöyle ki, finansal verilerin ileri aktarımı, bir AB'ye üye devletin vatandaşı ya da ikamet eden kişiyi kapsadığı takdirde, verilerin üçüncü bir ülkenin otoriteleri ile paylaşımı kamu güvenliğine yönelik ani ve ciddi bir tehdidin önlenmesi için gerekli olması durumları istisna olmakla, ilgili üye devletin yetkili otoritelerinin önceden rızasının alınmasına bağlıdır. Bu tür veriler üçüncü ülkeye terörizmin veya finansmanının soruşturulması, tespiti, önlenmesi veya kovuşturulması amaçları için aktarılabilir ve aktarılma amacı için gerekli olmadığı durumda ABD Hazine Bakanlığı verilerin silinmesini talep edebilecektir (Anlaşmanın 7. maddesi).

2. Birlik Hukuku Çerçevesinde Yetkilendirilmeyen Aktarımlar

Kanaatimizce, uluslararası anlaşmalara dayalı aktarımlardan bahsederken GDPR'ın 48. maddesinde öngörülen Birlik hukuku çerçevesinde yetkilendirilmeyen aktarımların da bu başlık altında ele alınması isabetli olacaktır. Zira düzenlemenin metninde de bu tür aktarımların gerçekleştirilebilmesi için uluslararası anlaşmanın bulunması şartı aranmaktadır⁴⁷⁶. Şöyle ki, bu düzenlemeye göre, bir veri sorumlusu veya veri işleyen kişisel verileri aktarmasını gerektiren mahkeme, hakem heyeti veya idari makam kararları, diğer aktarım gerekçelerine hâle gelmeksizin, ancak talepte bulunan üçüncü ülke ve AB ya da bir üye devlet arasında yürürlükte olan karşılıklı hukuki yardım anlaşması gibi bir uluslararası anlaşmaya dayanması hâlinde, herhangi bir şekilde tanınabilir veya tenfiz edilebilir (GDPR m.48). Söz konusu düzenlemenin gerekçesi olarak, GDPR'ın giriş bölümünün 115. paragrafında uluslararası anlaşmaların bulunmadığı durumlarda, bu tür taleplerin üçüncü ülke hukukunun ülke dışında uygulanmasına yol açacağı, bu durumun ise GDPR'ın amaçladığı gerçek kişilerin korunmasına engel olabileceği belirtilmiştir⁴⁷⁷.

Bu madde, AB vatandaşlarının kişisel verilerinin üçüncü ülkelere aktarımını ve açıklanmasını sınırlandırmak için uygulamaya konulmuş yeni bir düzenlenmedir. Bu düzenlemenin, “Snowden olayları”na tepki olarak ortaya çıkmış olduğu

⁴⁷⁶ Develioğlu, s. 78.

⁴⁷⁷ Sharma/ Menon, s. 179; Sertçe, s. 98.

düşünülmektedir⁴⁷⁸. Şöyle ki, bir mahkeme veya idari makamın kararına dayanarak kişisel verilerin aktarılmasını talep eden üçüncü ülke ile uluslararası anlaşmanın varlığının aranması şartının hükme dâhil edilmesindeki amaç, üçüncü ülke mahkemesinin veya idari makamının yetkilerinin sınırları dışında kullanılması iddiasını kısıtlamak ve üçüncü ülkelerin kendi yasal gerekliliklerine dayanarak AB hukukunu atlatmasına engel olmaktan ibarettir⁴⁷⁹.

Karşılıklı hukuki yardım, bilgi toplama ve alışverişi amacıyla farklı ülkeler arasında bir işbirliği şeklidir. Bir ülkedeki yetkililer, başka bir ülkedeki cezai soruşturmalara veya yargılamalara yardımcı olmak için bir ülkede bulunan kanıtları isteyebilir ve sağlayabilir⁴⁸⁰. Karşılıklı hukuki yardım anlaşması gibi uluslararası bir anlaşmanın bulunduğu durumlarda, AB şirketleri genellikle doğrudan talepleri reddetmeli ve talepte bulunan üçüncü ülke yetkilisini mevcut karşılıklı hukuki yardım anlaşmasına yönlendirmelidir⁴⁸¹. Buna örnek olarak, AB ile ABD ve Japonya⁴⁸² arasında akdedilen karşılıklı hukuki yardım anlaşmaları gösterilebilir⁴⁸³. Her ne kadar AB ile İzlanda ve Norveç⁴⁸⁴ arasında da böyle bir anlaşma mevcut olsa da adı geçen ülkeler AEA'ya dâhil olduğu için, zaten üçüncü ülke olarak kabul edilmemektedirler ve kişisel verilerin serbest dolaşımına dair kurallar bu ülkeler için de geçerlidir.

⁴⁷⁸ Theodore Christakis, “Transfer of EU Personal Data to U.S. Law Enforcement Authorities After the CLOUD Act: Is There a Conflict with the GDPR?”, Ed.: Randal Milch, Sebastian Benthall, **Cybersecurity and Privacy in a Globalized World - Building Common Approaches**, New York University School of Law, 2019, s. 5-6; David J. Kessler/ Jamie Nowak/ Sumera Khan, “The Potential Impact of Article 48 of the General Data Protection Regulation on Cross Border Discovery From the United States”, **The Sedona Conference Journal**, C. 17, S. 2, 2016, s. 582.

⁴⁷⁹ Sertçe, s. 99.

⁴⁸⁰ European Commission, Mutual Legal Assistance and Extradition, (çevrimiçi), https://ec.europa.eu/info/law/cross-border-cases/judicial-cooperation/types-judicial-cooperation/mutual-legal-assistance-and-extradition_en, 28.03.2021.

⁴⁸¹ EDPB, **Derogations**, s. 5.

⁴⁸² Agreement on Mutual Legal Assistance between the European Union and the United States of America, (çevrimiçi), [https://eur-lex.europa.eu/legal-content/en/txt/pdf/?uri=celex:22003a0719\(02\)&from=en](https://eur-lex.europa.eu/legal-content/en/txt/pdf/?uri=celex:22003a0719(02)&from=en), 25.10.2021; Agreement between the European Union and Japan on Mutual Legal Assistance in Criminal Matters, (çevrimiçi), [https://eur-lex.europa.eu/legal-content/en/txt/pdf/?uri=celex:22010a0212\(01\)&from=en](https://eur-lex.europa.eu/legal-content/en/txt/pdf/?uri=celex:22010a0212(01)&from=en), 27.10.2021.

⁴⁸³ European Commission, **Mutual Legal Assistance and Extradition**.

⁴⁸⁴ Agreement between the European Union and the Republic of Iceland and the Kingdom of Norway on the Application of Certain Provisions of the Convention of 29 May 2000 on Mutual Assistance in Criminal Matters (çevrimiçi), <https://eur-lex.europa.eu/legal-content/en/all/?uri=celex%3a22004a0129%2801%29>, 25.10.2021.

Şunu da belirtmek gerekir ki bu maddede bahsi geçen uluslararası anlaşmaların kapsamı sadece karşılıklı hukuki yardım anlaşmaları ile sınırlı değildir. İfade edilme şeklinden de anlaşıldığı üzere, örnek olarak bahsedilen karşılıklı hukuki yardım anlaşmalarının yanı sıra, bir ülkenin mahkemelerinin veya kamu kurumlarının diğer ülkelerden resmî olarak yardım talep etmesine ilişkin hükümler içeren herhangi uluslararası anlaşmalar, bu düzenleme kapsamında değerlendirilebilecektir⁴⁸⁵. “Hukuki ve Ticari Konularda Yabancı Ülkelerde Delil Sağlanması Hakkında” Lahey Sözleşmesi⁴⁸⁶, Avrupa Konseyi Siber Suç Sözleşmesi⁴⁸⁷, AB ve ABD arasında “Şemsiye Sözleşme”⁴⁸⁸ bu tür anlaşmalara örnek gösterilebilir⁴⁸⁹.

Bu tür aktarımları gerçekleştirmek için aranan diğer şart, GDPR’ın diğer hükümlerine halel gelmemesidir. Aslında ilk başta maddenin taslak metni hazırlanırken bu ifadeye yer verilmemiş, onun yerine “veri sahibinin bilgilendirilmesi”, “denetim makamından izin alınması” gibi daha sert ve geniş kapsamlı sınırlamalara yer verilmiştir⁴⁹⁰. Bu sıkı düzenlemeye Konsey tarafından itiraz edilmiş ve Parlamento ile bugünkü metin üzerinde mutabakata varılmıştır. Sonuç olarak, denetim makamının onayını gerektiren bütün hükümler çıkarılmış, onun yerine “*diğer hükümlere halel gelmeksizin*” ifadesi eklenmiştir⁴⁹¹. GDPR’ın giriş bölümünün 115. paragrafında da üçüncü ülke mahkemelerinin veya idari makamlarının kararının tek başına bir kişisel veri aktarımı için meşru gerekçe oluşturmadığı belirtilmiştir. Bu nedenle, üçüncü ülke yetkilileri tarafından talep edilen kişisel veri aktarımları, sadece GDPR’ın 5. bölümünde öngörülen şartlara uygun olduğu takdirde yasal olarak kabul edilecektir.

⁴⁸⁵ Kessler/ Nowak/ Khan, s. 588.

⁴⁸⁶ Convention of 18 March 1970 on the Taking of Evidence Abroad in Civil or Commercial Matters, 18.03.1970, (çevrimiçi), <https://www.hcch.net/en/instruments/conventions/full-text/?cid=82>, 25.10.2021.

⁴⁸⁷ Council of Europe, “Convention on Cybercrime”, №185, (çevrimiçi), <https://www.coe.int/en/web/conventions/full-list?module=treaty-detail&treatynum=185>, 25.10.2021.

⁴⁸⁸ Agreement between the United States of America and the European Union on the protection of personal information relating to the prevention, investigation, detection, and prosecution of criminal offences, 10.12.2016, (çevrimiçi), [https://eur-lex.europa.eu/legal-content/en/txt/pdf/?uri=celex:22016a1210\(01\)&rid=3](https://eur-lex.europa.eu/legal-content/en/txt/pdf/?uri=celex:22016a1210(01)&rid=3), 25.10.2021.

⁴⁸⁹ Kuner v.d., **Commentary**, s. 829; Sertçe, s. 98.

⁴⁹⁰ Detaylı bilgi için bkz. Christakis, s. 6; Kessler/ Nowak/ Khan, s. 583-584.

⁴⁹¹ Christakis, s. 6.

ÜÇÜNCÜ BÖLÜM

TÜRK HUKUKUNDA KİŞİSEL VERİLERİN AKTARILMASI

I. Genel Olarak

AB hukukunda olduğu gibi Türk hukukunda da kişisel verilerin aktarılması, kişisel verilerin işlenmesi kavramının bir alt bileşeni olarak ele alınmıştır. Şöyle ki KVKK m.3 uyarınca, *“kişisel verilerin işlenmesi: kişisel verilerin ... elde edilmesi, kaydedilmesi, depolanması, muhafaza edilmesi, değiştirilmesi, yeniden düzenlenmesi, açıklanması, aktarılması, devralınması, elde edilebilir hâle getirilmesi, sınıflandırılması ya da kullanılmasının engellenmesi gibi verileri üzerinde gerçekleştirilen her türlü işlemi”* ifade etmektedir.

Tanımdan da anlaşıldığı üzere kişisel verilerin işlenmesi, verilerin oluşturulduğu ilk günden silindiği veya imha edildiği güne kadar devam eden “yaşam döngüsü” boyunca veriler üzerinde gerçekleştirilecek her türlü hareketi kapsayan geniş bir kavramdır. Aktarılma ise kişisel verilerin işlenmesi kavramı içerisinde yer alan bir kavram, veri işlemenin bir aşamasıdır. Buna rağmen diğer işleme türlerinden farklı olarak sadece aktarılma şartları Kanun’da iki ayrı başlık altında ele alınmıştır. Bunun da temel nedeni, verilerin aktarılması söz konusu olduğunda veriler üzerinde üçüncü kişilerin hâkimiyetinin söz konusu olacağı ve daha fazla koruma ihtiyacı ortaya çıkacağı gerçeğinden kaynaklanmaktadır⁴⁹².

Kişisel verilerin aktarılması bir işleme türü olduğu için kişisel verilerin işlenmesi ile ilgili Kanun’da yer alan hükümler, aktarılma açısından genel hüküm niteliğindedir. Bu nedenle kişisel verilerin aktarılması zamanı sadece Kanun’un 8’inci ve 9’uncu maddelerinde yer alan şartların aranması yeterli olmayıp, aynı zamanda kişisel verilerin işlenmesi için öngörülen temel ilkelere de (KVKK m.4) uyulması gerekmektedir⁴⁹³.

⁴⁹² Çelik, s. 35.

⁴⁹³ Kişisel Verileri Koruma Kurumu, Kişisel Verilerin Yurtdışına Aktarılması Rehberi, s. 2, (çevrimiçi) <https://kvkk.gov.tr/yayinlar/k%c4%b0%c5%9e%c4%b0sel%20ver%c4%b0ler%c4%b0n%20yurtdi%c5%9eina%20aktarilmasi.pdf>, 25.11.2021; Erarslan, **Verilerin Aktarılması**, s. 89; Özcan, s. 112; Tepe, s. 70.

II. Kişisel Verilerin Aktarılmasına Dair Temel İlkeler

A. Veri Aktarımının Hukuka ve Dürüstlük Kurallarına Uygun Olması

Kanun m.4/f.2 hükmüyle kişisel verilerin hukuka ve dürüstlük kurallarına uygun aktarılması gerektiği düzenlenmiştir. Hukuka ve dürüstlük kurallarına uygun olma ilkesi, kişisel verilerin korunması hukukunun temel ilkesi olarak nitelendirilmektedir. Çünkü bu ilke, kişisel verilerin korunmasına yönelik diğer ilkeleri de kapsar ve onların kaynağını oluşturur⁴⁹⁴.

Veri aktarımının hukuka uygun olması gerekliliği kendi kendini açıklar niteliktedir. Kolayca anlaşılabilmesi üzere, hukuka uygun veri aktarımı, bu aktarımın kanunlardan veya diğer hukuki düzenlemelerden kaynaklanan ilke ve yükümlülüklerle uygun olmasını ifade eder⁴⁹⁵. Kurul'un, Amazon Turkey Perakende Hizmetleri Limited Şirketi (Amazon Turkey) hakkında yapılan başvuru ile ilgili verdiği kararı, bu ilkeye örnek olarak gösterilebilir. Sözü geçen kararda Kurul, veri sorumlusu olan Amazon Turkey şirketinin gerçekleştirdiği aktarımın yurt dışına veri aktarımı ile ilgili kanun hükümlerine uygun olmadığına, yani ilgili kişilerin açık rızalarını almadan ve ilgilinin açık rızası olmaksızın yurt dışına veri aktarımı için aranan şartlara uymadan kişisel verilerini aktardığına ve bu nedenle cezalandırılmasına karar vermiştir⁴⁹⁶.

Aktarımın dürüstlük kurallarına uygun olması ise veri sorumlusunun, veri aktarımındaki hedeflerine ulaşmaya çalışırken, ilgili kişilerin menfaatlerini ve makul beklentilerini dikkate alması⁴⁹⁷, ilgili kişinin güveninin kötüye kullanılmaması, ilgili

⁴⁹⁴ Bygrave, **Data Protection**, s. 58; Küzeci, s. 228; Sinem Göçmen Uyarer, **Kişisel Verilerin Korunması: KVKK ve TCK Kapsamında**, Ankara, Seçkin, 2020, s. 123; Özkan, s. 85.

⁴⁹⁵ Küzeci, s. 228; Ayözger Öngün, s. 134; Dülger, **Kişisel Veriler**, s. 263; Develioğlu, s. 45; Çekin, **Kişisel Verilerin Korunması**, s. 45; Room, s. 21; Lloyd, s. 96; Hayrunnisa Özdemir, **Elektronik Haberleşme Alanında Kişisel Verilerin Özel Hukuk Hükümlerine Göre Korunması**, Ankara, Seçkin, 2009, s. 166; Taştan, s. 46; Göçmen Uyarer, s. 123; Erarslan, **Özel Nitelikli Kişisel Veriler**, s. 92; Erarslan, **Verilerin Aktarılması**, s. 90; Voigt/ Bussche, s. 88; İmançlı, s. 109.

⁴⁹⁶ Kişisel Verileri Koruma Kurulu 27/02/2020 tarihli ve 2020/173 karar, (çevrimiçi), <https://www.kvkk.gov.tr/Icerik/6739/2020-173>, 06.07.2021.

⁴⁹⁷ Bygrave, **Data Protection**, s. 58; Baran Kızılırmak, "Kişisel Verilerin İşlenmesinde Adli ve Önleyici Amaçla Öngörülen İstisnaların Ulusal ve Uluslararası Hukuka göre Değerlendirilmesi", **Kadir Has Üniversitesi Hukuk Fakültesi Dergisi**, C. 7, S. 2, 2019, s. 230; İmançlı, s. 112.

kişinin yanlıgısından yararlanılmaması gerektiğini ifade etmektedir⁴⁹⁸. Örneğin, veri aktarımının hukuki sebebi olarak açık rıza gösterilmesine rağmen, gerçekte veri aktarımının hukuki sebebi farklıysa ve ilgili kişi bu hususta bilgilendirilmemişse, ilgili kişi her zaman rızasını geri alabileceği ve verisi üzerinde denetime sahip olduğu yanlıgısına düşürüldüğü için aktarım dürüstlük kuralına aykırı olacaktır⁴⁹⁹.

B. Aktarılan Verinin Doğru ve Güncel Olması

Kanun m.4/f.2/b uyarınca, işlenen kişisel veriler doğru ve gerektiğinde güncel olmalıdır. Verilerin doğru olması, onların gerçeğe uygun olmasını, herhangi konuda yanlış veya aldatıcı olmaması gerektiğini, güncel olması ise verilerin doğru olup olmadığının kontrol edilmesi gerektiğini, artık doğru olmaması durumunda ise o verilerin güncellenmesi gerektiğini ifade eder⁵⁰⁰. Bu bağlamda söz konusu ilke, KVKK m.11’de yer alan eksik veya yanlış işlenmiş kişisel verilerin düzeltilmesini isteme hakkına paraleldir⁵⁰¹. Aktarılan kişisel verilerin doğru ve gerektiğinde güncel olması hususunda yükümlülük veri sorumlusundadır⁵⁰². Kişisel verilerin doğru olması bireyin temel hak ve özgürlüklerinin, ekonomik menfaatinin ve manevi bütünlüğünün korunmasını sağlar⁵⁰³. Verilerin doğru olması sadece veriler ilk kez aktarıldığında değil, bütün süreç boyunca sağlanmalıdır. Bu nedenle ilgili kişi, aktarılan bilgilerin gerçekte uyumlu olup olmadığını düzenli olarak kontrol edebilir. Gerçekle bağdaşmayan, yalan veya güncel olmayan kişisel verilerin düzeltilmesi veya kaldırılması gerekmektedir⁵⁰⁴.

Bu ilkenin uygulanması hem veri sorumlusunun hem de ilgili kişinin menfaatine hizmet etmektedir. Zira doğru ve güncel olmayan verilerin aktarılması

⁴⁹⁸ Nafiye Yücedağ, “Kişisel Verilerin Korunması Kanunu Kapsamında Genel İlkeler”, **Kişisel Verileri Koruma Dergisi**, C. 1, S. 1, 2019, s. 50.

⁴⁹⁹ Yücedağ, **Genel İlkeler**, s. 50; Bu hususun da yer aldığı Kurul kararı özeti için bkz.: (çevrimiçi), <https://www.kvkk.gov.tr/Icerik/5412/Acik-Rizain-Hizmet-Sartina-Baglanmasi>, 02.03.2021.

⁵⁰⁰ Bygrave, **Data Protection**, s. 60; Ayözger Öngün, s. 145; Küzeci, s. 213; Dülger, **Kişisel Veriler**, s. 294; Şimşek, s. 100; Erarslan, **Özel Nitelikli Kişisel Veriler**, s. 108; Özdemir, **Elektronik Haberleşme**, s. 139; Erarslan, **Verilerin Aktarılması**, s. 92; Özcan, s. 95.

⁵⁰¹ Göçmen Uyarer, s. 125.

⁵⁰² Kişisel Verileri Koruma Kurumu, **Doğru Bilinen Yanlıklar**, s. 23.

⁵⁰³ Küzeci, s. 343; Akgül, s. 312.

⁵⁰⁴ Özdemir, **Elektronik Haberleşme**, s. 138; Özkan, s. 88.

sonucunda, veri sahibinin hakları ihlal edildiği gibi, veri aktarımının amacına da ulaşamayacaktır⁵⁰⁵.

C. Veri Aktarımının Belirli, Açık ve Meşru Amaçlar İçin Yapılması

Kanun m.4/f.2/c uyarınca, kişisel veriler belirli, açık ve meşru amaçlar dâhilinde işlenmelidir. Veri işleme faaliyetinin amaçları aslında işleme faaliyetinin varlık sebebini oluşturmaktadırlar⁵⁰⁶. Amacın belirli ve açık olması, hem şeffaflığın sağlanmasına hem de ilgili kişinin haklarının güvence altına alınmasına hizmet etmektedir⁵⁰⁷. Maddenin gerekçesine göre, bu ilke “*veri sorumlusunun, veri işleme amacını açık ve kesin olarak belirlemesini ve bu amacın meşru olmasını zorunlu kılmaktadır.*”⁵⁰⁸

Amacın belirli olması, henüz aktarılma faaliyeti gerçekleşmeden önce verilerin aktarılma amacının belirlenmiş olmasını ifade etmektedir⁵⁰⁹. Bu kural aynı zamanda veri sorumlusunun aydınlatma yükümlülüğünden kaynaklanan bir zorunluluktur. Zira aydınlatma yükümlülüğü çerçevesinde veri sorumlusunun, ilgili kişiyi amaç da dâhil olmak üzere aktarım hakkında bilgilendirmesi gerekmektedir. Daha önce de belirtildiği üzere, aydınlatma yükümlülüğü en geç aktarım gerçekleşene dek yerine getirilmeli olduğu için dolayısıyla, aktarım amacının da o ana kadar belirlenmiş olması gerekmektedir⁵¹⁰. Bu anlamda amaç belirlenirken “gelecekte yapılacak araştırmalar için”, “kullanıcı deneyimini geliştirmek için”, “pazarlama faaliyetleri için” gibi belirsiz veya muğlak ifadelerin kullanılması isabetli değildir⁵¹¹. Amacın açık olması ise, ilgili kişinin aktarımın amacı hakkında açık ve anlaşılır bir biçimde bilgilendirilmesini ifade eder. Bu nedenle veri sorumlusunun,

⁵⁰⁵ Küzeci, s. 344; Kızılırmak, **Kişisel Verilerin İşlenmesinde**, s. 230.

⁵⁰⁶ Yücedağ, **Genel İlkeler**, s. 52.

⁵⁰⁷ Yücedağ, **Genel İlkeler**, s.52.

⁵⁰⁸ Bkz.: KVKK m.4 gerekçesi.

⁵⁰⁹ Küzeci, s. 203; Ayözger Öngün, s. 138; Dülger, **Kişisel Veriler**, s. 273; Çekin, **Kişisel Verilerin Korunması**, s. 73-74; Erarslan, **Özel Nitelikli Kişisel Veriler**, s. 109-110; Göçmen Uyarer, s. 126; İmançlı, s. 118.

⁵¹⁰ Ayözger Öngün, a.y; Yücedağ, **Genel İlkeler**, s. 52.

⁵¹¹ Küzeci, s. 203; Ayözger Öngün, s. 138; Dülger, **Kişisel Veriler**, s. 224; Çekin, **Kişisel Verilerin Korunması**, s. 74-75; Erarslan, **Özel Nitelikli Kişisel Veriler**, s. 112; İmançlı, s. 118.

aktarımın amacıyla ilgili bilgilendirme metinlerinde makul bir kişi tarafından anlaşılabilir dil ve format kullanması gerekmektedir⁵¹².

Amacın meşru olması aktarılan verilerin, veri sorumlusunun yapmış olduğu iş veya sunmuş olduğu hizmetle bağlantılı, bunlar için gerekli olması ve kanuni temellere dayanması anlamına gelmektedir⁵¹³. Örneğin, bir sosyal medya kuruluşu, kullanıcılarının kişisel bilgilerini bir siyasi partiye seçim kampanyasında kullanmak üzere aktarırsa bu aktarma faaliyeti, üye olmak ve siteyi kullanmak şeklinde belirlenen meşru amaç kapsamında değerlendirilemeyecektir⁵¹⁴.

D. Veri Aktarımının Amaca Bağlı, Sınırlı ve Ölçülü Olması

Kanun m.4/f.2/ç uyarınca, veri işleme faaliyeti; işlendiği amaçla bağlantılı, sınırlı ve ölçülü olmalıdır. Buna göre, aktarılan veriler, belirlenen amaçların gerçekleştirilebilmesi açısından elverişli olmalı ve amacın gerçekleştirilmesiyle ilgili olmayan veya ihtiyaç duyulmayan kişisel verilerin aktarılmasından kaçınılması gerekmektedir⁵¹⁵.

Amaca bağlı kalma ilkesi, diğer bir veri işleme ilkesi olan belirli amaçlarla işleme ilkesine hizmet etmektedir ve verinin aktarıldığı amaç haricinde başka bir amaçla aktarılmasını yasaklar⁵¹⁶. Eğer veri aktarımı için başta öngörülen amaç sonradan değişirse yeni amaç için de hukuka uygunluk koşulları aynen aranacaktır⁵¹⁷. Amaçla ölçülü olma, temel hak ve özgürlüklere en az müdahalenin olduğu yöntemin tercih edilmesini ifade eder⁵¹⁸. Amaçla sınırlı olma ise veri sorumlusunun, aktarım amacına ulaşmak için en az sayıda veri kullanımı anlamına gelir⁵¹⁹. “Veri minimizasyonu” olarak da adlandırılan bu ilkeye göre aktarılan kişisel verilerin

⁵¹² Ayözger Öngün, s. 139; Dülger, **Kişisel Veriler**, s. 277-278; Göçmen Uyarer, s. 126; Erarşlan, **Verilerin Aktarılması**, s. 93; İmançlı, s. 118.

⁵¹³ Ayözger Öngün, s. 139; Dülger, **Kişisel Veriler**, s. 276-277; İmançlı, s. 118; Hakalmaz, s. 64.

⁵¹⁴ Erarşlan, **Özel Nitelikli Kişisel Veriler**, s. 112.

⁵¹⁵ Ayözger Öngün, s. 141; Çekin, **Kişisel Verilerin Korunması**, s. 10; Develioğlu, s. 47; Göçmen Uyarer, s. 126-127; Yücedağ, **Genel İlkeler**, s. 59; Erarşlan, **Özel Nitelikli Kişisel Veriler**, s. 98, 100; Özkan, s. 90.

⁵¹⁶ Bygrave, **Data Protection**, s. 62; Bygrave, **Data Privacy**, s. 153; Küzeci, s. 231; Ayözger Öngün, s. 141; Akgül, s. 133.

⁵¹⁷ Voigt/ Bussche, s. 89; Ayözger, s. 123.

⁵¹⁸ Bygrave, **Data Protection**, s. 59; Bygrave, **Data Privacy**, s. 147; Çekin, **Kişisel Verilerin Korunması**, s. 53.

⁵¹⁹ Bygrave, **Data Privacy**, s. 151; Küzeci, s. 236.

miktarı, verilerin toplanması ve devamında aktarılması amaçlarına ulaşmak için zorunlu olan miktarla sınırlı kalmalıdır⁵²⁰. Örneğin, bir çalışanın sadece SGK işe giriş beyannamesi ve maaş bordrosunun aktarılması yeterli iken, tüm özlük dosyasının aktarıldığı takdirde veri minimizasyonu ilkesi ihlal edilmiş kabul edilecektir⁵²¹. Nitekim bir Kurul kararına konu olan olayda, davacı ve veri sorumlusu arasındaki uyuşmazlığa bakan mahkeme, veri sorumlusundan davacı hakkında bazı bilgilerin mahkemeye sunulmasını talep etmiş, veri sorumlusu ise talep edilenden daha fazla veriyi mahkemeye sunmuştur. Davacının şikâyeti üzerine Kurul, bu ilkenin ihlal edildiğine kanaat getirmiş ve veri sorumlusu hakkında idari yaptırım uygulanmasına karar vermiştir⁵²².

E. Aktarılan Verilerin Sınırlı Süre ile Muhafazası

KVKK m.4/f.2/d uyarınca, kişisel veriler, ilgili mevzuatta öngörülen veya aktarıldıkları amaç için gerekli olan süre kadar muhafaza edilecektir. Maddeden de anlaşıldığı üzere, verilerin aktarıldıktan sonra muhafaza edilme süresi, kanunla veya diğer yasal düzenlemelerle belirlenen sürelerle sınırlıdır. Sınırlı sürede muhafaza edilme ilkesi, kişisel verilerin güncelliğini korumakla da bağlantılıdır. Nitekim aktarım amacına ulaşmışsa veriler güncelliğini kaybetmiştir⁵²³. Eğer böyle bir süre öngörülmemişse, verinin aktarılma amacıyla orantılı bir muhafaza süresi belirlenecektir. Nitekim verilerin azami muhafaza sürelerinin belirlenmesi “Veri Sorumluları Sicili Hakkında Yönetmelik”⁵²⁴ gereğince, veri sorumluları için bir

⁵²⁰ Erarslan, **Verilerin Aktarılması**, s. 93; İmançlı, s. 122.

⁵²¹ Altındağ, s. 120.

⁵²² Bkz.: Kişisel Verileri Koruma Kurulu, “İşlenme Amacının Gerektirdiğinden Fazla Kişisel Veri İşlenmesi/ Aktarılması (Veri Minimizasyonu İlkesine Aykırılık)” Kararı, (çevrimiçi) <https://www.kvkk.gov.tr/icerik/5413/islenme-amacinin-gerektirdiginden-fazla-kisisel-veri-islenmesi-aktarilmasi-veri-minimizasyonu-ilkesine-aykirlilik->, 22.11.2021; Aynı yönde karar için bkz.: Kişisel Verileri Koruma Kurulu, 03.03.2020 tarihli ve 2020/196 sayılı “İlgili kişiye ait kişisel verinin denetim faaliyeti kapsamında bir kamu kurumuna aktarılmasına ilişkin şikâyet hakkında” kararı, (çevrimiçi) <https://www.kvkk.gov.tr/icerik/6759/2020-196>, 22.11.2021.

⁵²³ Ozan Selek, “Genel Veri Koruma Tüzüğü Işığında Kişisel Verilerin İşlenmesinde Rıza Açıklaması”, **Dokuz Eylül Üniversitesi Hukuk Fakültesi Dergisi**, C. 21, S. 2, 2019, s. 84; Özkan, s. 93.

⁵²⁴ RG. T. 30.12. 2017, S. 30286.

zorunluluktur. Bu süre sona erdiğinde aktarılan veriler; silinecek, yokedilecek veya anonim hâle getirilecektir⁵²⁵.

III. Kişisel Verilerin Yurt İçinde Aktarılması

A. Genel Olarak

95/46/EC sayılı DPD ve GDPR'da olduğu gibi KVKK'da da işisel verilerin ülke sınırları içerisinde aktarılmasına, veri işleme türlerinden biri olarak yer verilmiştir (KVKK m.3). Gerek 95/46/EC sayılı DPD'de gerek GDPR'da verilerin Birlik içerisinde aktarımının şartları ayrıca düzenlenmemiş, veri işlemeye ilişkin genel kurallar çerçevesinde değerlendirilmiştir⁵²⁶. Fakat KVKK'da bu hususta farklı bir yol izlenmiş ve kişisel verilerin aktarılması, madde 8 ile ayrıca düzenlenmiştir.

Konunun önemi göz önünde bulundurularak ayrı bir madde ile düzenlenmesine rağmen Kanun'da kişisel verilerin yurt içinde aktarımı kavramının tanımına yer verilmemiştir. Birinci bölümde yapılan açıklamalar⁵²⁷ ışığında kişisel verilerin yurt içinde aktarılmasını, yurt içinde bulunan üçüncü kişilere yönelik her türlü veri paylaşımı şeklinde ifade etmek mümkündür. Nitekim maddenin gerekçesinde de üçüncü kişilere yapılan aktarımlar ifadesine yer verilmiştir⁵²⁸. Bu noktadan hareketle, üçüncü kişi niteliğine sahip olmayan kişilere yönelik veri paylaşımları, 8. madde hükümlerinden muaf tutulacaktır. Örneğin, tüzel kişiliğe sahip olan veri sorumlusunun kendi bünyesinde gerçekleştirdiği ikincil işleme faaliyetleri, veri aktarımı değildir⁵²⁹. Buna karşılık, bir şirketler topluluğu bünyesinde bulunan ve her biri veri sorumlusu niteliği taşıyan birkaç şirket arasındaki veri paylaşımları ise veri aktarımını teşkil etmektedir⁵³⁰. Nitekim Kurul tarafından verilen bir kararda *“bir şirketler topluluğu bünyesinde yer alan birden çok veri sorumlusu şirketler arasında veri aktarımı gerçekleştirilmesinin, üçüncü kişiye veri aktarımı*

⁵²⁵ Bygrave, **Data Protection**, s. 60; Başalp, **Kişisel Veriler**, s. 39.

⁵²⁶ Dülger, **Kişisel Veriler**, s. 431.

⁵²⁷ Bkz.: yuk., Birinci Bölüm, “Kişisel Verilerin Aktarılması/ Tanımı” başlığı.

⁵²⁸ Bkz.: KVKK m.8 gerekçesi.

⁵²⁹ Dülger, **Kişisel Veriler**, s. 432; Altındağ, s. 117; İmançlı, s. 164; Hakalmaz, s. 41.

⁵³⁰ Dülger, **Kişisel Veriler**, s. 435-436; Ünsal Özden/ Uz/ Karamustafaoğlu, s. 22; Altındağ, s. 118-119; İmançlı, s. 164; Kişisel Verileri Koruma Kurumu, **Sıkça Sorulan Sorular**, s. 78. Bir şirketler topluluğuna bağlı her bir şirket ayrıca veri sorumlusu sayılması gerektiğine dair bkz.: Kişisel Verileri Koruma Kurumu, **Doğru Bilinen Yanlılar**, s. 20.

olarak değerlendirildiği, bu itibarla aynı şirketler topluluğu bünyesinde yer alan veri sorumluları arasında gerçekleşecek veri aktarımında da 6698 sayılı Kişisel Verilerin Korunması Kanununun 8'inci maddesi hükümlerinin esas alınması gerektiği” belirtilmiş ve “iş başvurusunda bulunan bir adayın açık rızası olmadan kişisel verilerinin bir şirketler topluluğu altında yer alan veri sorumluları arasında aynı veri tabanını kullanmak suretiyle paylaşılması”nın veri ihlali teşkil ettiği belirtilmiştir⁵³¹.

Dikkat edilmesi gereken diğer husus ise, aktarımın gerçekleştiği bütün süre boyunca veri alıcısının Türkiye sınırlarında bulunması gerekmesidir. Diğer durumlarda gerçekleşen aktarım, yurt dışına yapılan aktarım olarak kabul edilecektir⁵³².

Bu kapsamda değinilmesi gereken önemli hususlardan biri de verilerin üçüncü kişilerin erişimine sunularak paylaşılmasıdır. Zira günümüzde internetin temel iletişim aracına dönüşmesi sonucu, kişisel verilerin üçüncü kişiler için erişilebilir duruma getirilmesi oldukça kolay ve yaygın bir hâl almıştır. Bu gibi durumlarda kişisel veriler fiziksel olarak el değiştirmese bile onlar üzerinde üçüncü kişilerin hâkimiyeti, dolayısıyla da korunması ihtiyacı ortaya çıkmaktadır. Bu noktadan hareketle, kanaatimizce kişisel verilerin üçüncü kişilerin erişimine sunulması da kişisel veri aktarımı olarak değerlendirilmelidir.

Kişisel verilerin yurt içinde aktarılması şartları, Kanun’un 8. maddesi ile düzenlenmiştir. Buna göre; “*kişisel veriler ilgilinin açık rızası olmaksızın aktarılamaz*”. Sadece “...5'inci maddenin ikinci fıkrasında ve yeterli önlemler alınmak kaydıyla, 6'ncı maddenin üçüncü fıkrasında belirtilen şartlardan birinin bulunması hâlinde...”, açık rıza alınmadan kişisel veriler aktarılabilir. Ayrıca aktarımla ilgili diğer kanunlarda yer alan hükümler de saklıdır.

Kişisel verilerin aktarılması, hukuki niteliği itibarıyla bir veri işleme türü olduğu için, yapılan aktarımların her zaman yasal dayanağının bulunması

⁵³¹ Bkz.: Kişisel Verileri Koruma Kurulu, “İş Başvurusu Sürecinde İşlenen Kişisel Verilerin Hukuka Aykırı Şekilde Paylaşılması” hakkında kararı, (çevrimiçi), <https://www.kvkk.gov.tr/Icerik/5410/Is-Basvurusu-Surecinde-Islenen-Kisisel-Verilerin-Hukuka-Aykiri-Sekilde-Paylasilmasi>, 01.10.2021.

⁵³² Dülger, **Kişisel Veriler**, s. 433.

gerekmektedir⁵³³. Maddeden anlaşıldığı üzere, kişisel verilerin yurt içinde aktarılabilmesi için aşağıdaki hukuki dayanaklardan birinin bulunması gerekmektedir:

1. İlgili kişinin açık rızasının bulunması
2. Kişisel verilerin işlenmesi için 5'inci ve 6'ncı maddelerde öngörülen hukuka uygunluk sebeplerinden birinin mevcut olması
3. Aktarımla ilgili diğer kanunlarda yer alan hükümler

Görüldüğü üzere, kişisel verilerin aktarılması için aynen genel veri işleme faaliyetinde aranan şartların varlığı aranmaktadır. Sadece kanun koyucu tarafından özel nitelikli kişisel verilerin hassas içeriği göz önünde bulundurularak bu tür verilerin aktarılması için aynı zamanda yeterli önlemlerin alınmış olması zorunluluğu getirilmiştir. Diğer veri işleme türlerinden farklı düzenlemeye tabi tutulmamasına rağmen, kişisel verilerin yurt içinde aktarılmasının ayrı bir madde hâlinde kaleme alınmış olması, Kanun'un sistematüğinde karışıklığa sebep olduğu gerekçesiyle doktrinde eleştiri konusu olmuş ve gereksiz bir düzenleme olarak nitelendirilmiştir⁵³⁴.

B. Açık Rızaya Dayalı Aktarımlar

1. Açık Rızanın Tanımı

Rıza kavramına Türk hukukunun çeşitli hukuki düzenlemelerinde rastlansa da, kişisel verilerin korunmasına yönelik düzenlemelerde daha spesifik bir kavram - "açık rıza" kavramına yer verilmiştir. Çünkü aşağıda daha detaylı açıklanacağı üzere, kişisel verilerin korunması hukukunda zımni rızanın genel olarak geçerliliği yoktur⁵³⁵. Örneğin, 1982 Anayasası'nın 20. maddesine 2010 yılında yapılan Anayasa Değişikliği ile eklenen düzenlemede "*kişisel veriler, ancak kanunda öngörülen hâllerde veya kişinin açık rızasıyla işlenebilir*" ifadesine yer verilmiştir. Aynı

⁵³³ Arslan, s. 464.

⁵³⁴ Tepe, s. 70-71.

⁵³⁵ Başalp, **Kişisel Veriler**, s. 44; Küzeci, s. 251; Taştan, s. 161-162; Erarslan, **Verilerin Aktarılması**, s. 99; Kurul, "Amazon Turkey" kararında "*zımni irade beyanı ile onay alınmasının mevzuata uygun kabul edilmeyeceği*"ni belirtmiştir. Bkz.: Kişisel Verileri Koruma Kurulu, 27.02.2020 tarihli ve 2020/173 sayılı karar, (çevrimiçi), <https://www.kvkk.gov.tr/Icerik/6739/2020-173>, 28.11.2021.

zamanda KVKK'da da kişisel verilerin aktarılması (m.5), özel nitelikli kişisel verilerin aktarılması (m.6), kişisel verilerin yurt içinde (m.8) ve yurt dışına aktarılması (m.9) için hukuka uygunluk sebeplerinden biri olarak herhangi rıza değil, açık rızanın varlığı aranmaktadır.

Açık rıza, işleme sürecine kişinin aktif müdahalesini sağlayarak bireyin kişisel verilerinin geleceğini tayin etme hakkına hizmet etmektedir⁵³⁶. KVKK'nın tanımlara ilişkin 3. maddesinde açık rıza kavramı *“belirli bir konuya ilişkin, bilgilendirilmeye dayanan ve özgür iradeyle açıklanan rıza”* olarak tanımlanmıştır. Anlaşıldığı üzere kanun koyucu “açık rıza” kavramını “rıza” kavramı üzerinden tanımlamıştır. Kanaatimizce, bir kavramın kendisiyle tanımlanması isabetli bir yaklaşım değildir⁵³⁷. Bu bağlamda, maddenin gerekçesinde kullanılan tanım daha isabetli olmuştur. Şöyle ki gerekçede, açık rızaya ilişkin *“ilgili kişinin kendisiyle ilgili veri işlenmesine, özgürce, konuyla ilgili yeterli bilgi sahibi olarak, tereddüde yer bırakmayacak açıklıkta ve sadece o işlemle sınırlı olarak verdiği onay beyanı”* ibaresine yer verilmiştir⁵³⁸. Rızaya ilişkin benzer tanım, GDPR'da da yer almaktadır⁵³⁹. Nitekim gerekçede de bu tanımın 95/46/EC sayılı DPD'nin hükümleri dikkate alınarak kullanıldığı belirtilmiştir.

Tanımda yer alan unsurlar, verilerin aktarılması açısından değerlendirildiğinde aktarılma için geçerli açık rızanın; *kişisel verilerin aktarılmasına ilişkin olma, aktarılma hakkında bilgilendirmeye dayalı olma ve özgür iradeyle alınmış olma* gibi unsurları içermesi gerekmektedir. Bu unsurlar, aynı zamanda açık rızanın geçerlilik şartları olarak da nitelendirilebilir. Zira açık rızaya dayalı veri aktarımından bahsedebilmek için, bu unsurların hepsinin aynı anda mevcut olması gerekmektedir. Ayrıca, açık rızanın en geç aktarma faaliyetinin

⁵³⁶ Küzeci, s. 220.

⁵³⁷ Aynı yönde görüş için bkz. Çekin, **Kişisel Verilerin Korunması**, s. 74.

⁵³⁸ Bkz.: KVKK m.3 gerekçesi.

⁵³⁹ GDPR m.4/f.11: *veri sahibinin “rızası” veri sahibinin 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 göstergedir.*

gerçekleştiği sırada alınması gerekmektedir. Aksi takdirde alınan açık rıza, aktarma faaliyeti açısından hukuki dayanak teşkil etmeyecektir⁵⁴⁰.

2. Belirli Bir Konuya İlişkin Olma

Hukuka uygun bir veri aktarma eyleminden bahsedebilmek için aranan açık rıza, belirli bir konuya ilişkin alınmış olmalıdır. Rızanın belirli bir konuya ilişkin olması, ilgili kişinin kendi verileri üzerinde kontrolü ve şeffaflığı sağlayabilmesine hizmet etmektedir⁵⁴¹. Bu unsur, kişisel verilerin aktarılması açısından gözden geçirildiğinde açık rızanın aktarılmaya ilişkin olması gerektiğini ifade etmektedir. Bu gereklilik ile “belirli ve açık amaçlar için işleme” ilkesi arasında yadsınamaz bir bağlantı mevcuttur⁵⁴². Şöyle ki geçerli bir rızadan bahsedebilmek için verilen rızanın sebebi (kişisel verileri aktarılması) belli olmalıdır⁵⁴³. Bir başka anlatımla, ilgili kişinin rızası, genel nitelikli yani kişisel verilerinin herhangi işleme türü için olmamalı, sırf aktarım işlemi için verilmiş olmalıdır. Rızanın spesifik olarak aktarım faaliyetine ilişkin verildiği açıkça anlaşılmalıdır. Örneğin, elektronik sağlık kayıtları için toplanan tedavi bilgilerinin, hem toplanması hem de tedavide rol alacak olan sağlık çalışanlarına ileride gerçekleştirilebilecek aktarımlar için genel bir rıza beyanı geçerli olmayacaktır⁵⁴⁴.

Rızanın belirli bir aktarılma faaliyetine özgü olmasının yanı sıra, ilgili kişinin aktarılacak her bir verisi için ayrıca rızasının alınması gerekmektedir. Verilerin işlenmesi için genel bir muvafakat geçerli sayılmayacaktır. Başka bir deyişle, rıza beyanı sadece somut aktarımın sınırları çerçevesinde geçerli olacaktır⁵⁴⁵. Hangi

⁵⁴⁰ Ayözger Öngün, s. 137; Dülger, **Kişisel Veriler**, s. 224; Çekin, **Kişisel Verilerin Korunması**, s. 88; Mehmet Bedii Kaya, **Elektronik Ticaret Hukuku: Ticari Elektronik İletiler**, 2. bs., İstanbul, On İki Levha, 2020, s. 150; Göçmen Uyarer, s. 116; Erarslan, **Özel Nitelikli Kişisel Veriler**, s. 123; Taştan, s. 164-165; Erarslan, **Verilerin Aktarılması**, s. 98.

⁵⁴¹ Nevzat Ali Anı, “Kişisel Verilerin İşlenmesi ve Açık Rıza”, Yüksek Lisans Tezi, İstanbul Üniversitesi, 2018, s. 131.

⁵⁴² Erarslan, **Özel Nitelikli Kişisel Veriler**, s. 149.

⁵⁴³ 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**, C. 74, S. 2, 2016, s. 637.

⁵⁴⁴ Article 29 Data Protection Working Party, Opinion 15/2011 on the Definition of Consent, 13.07.2011, (çevrimiçi), https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2011/wp187_en.pdf, 26.07.2021, s. 18; Aşıkoğlu, **Kişisel Veriler**, s. 183.

⁵⁴⁵ Başalp, **Kişisel Veriler**, s. 39; Küzeci, s. 234; Develioğlu, s. 53; Abdülhamid Zor, **Veri Sorumlusunun Yükümlülükleri ve Bu Yükümlülüklerin İhlalinden Doğan Özel Hukuk Sorumluluğu**, İstanbul, On İki Levha, 2020, s. 138.

konuları kapsadığı bilinmeyen, genel nitelikli ve sınırları muğlak bir konuda gösterilen rıza beyanının, aktarma faaliyeti açısından geçerliliği olmayacaktır⁵⁴⁶. Kurul bu hususla ilgili “Amazon Turkey” kararında belirli bir konu ile sınırlandırılmayan genel nitelikli açık rızanın “battaniye rıza” niteliğinde olduğunu ve hukuken geçersiz sayıldığını ifade etmiştir⁵⁴⁷.

Belirli bir duruma ilişkin olma unsuru ile bağlantılı olan bir diğer ilke ise amaca bağlılık ilkesidir. Aktarılma faaliyeti boyunca başta belirtilen amaca bağlı kalınması, verilen rızanın, daha sonra genişletilmesi ve belirsizleştirilmesinin önüne geçmeye hizmet etmektedir. Örneğin, kablolu yayın hizmeti veren bir şirketin, müşterilerin ilgisini çekebilecek filmler sunabilmesi için onarın film izleme alışkanlıklarını takip etmelerine ilişkin alınan rıza, söz konusu verilerin hedefli reklam (*targeted advertising*) amacıyla üçüncü bir şirkete aktarılması için geçerli sayılmayacaktır⁵⁴⁸. Zira müşterinin başta rıza verdiği amaçla bağdaşmamaktadır. Bu yüzden de, ilgili kişinin verilerinin aktarılması açısından veri sorumlusunun birkaç amacı mevcut ise ve bu amaçlar birbirinden kesin bir ayrılık içerisindeyse, ilgili kişiden her bir amaç için ayrı açık rıza alınması gerekmektedir⁵⁴⁹.

3. Bilgilendirmeye Dayalı Olma

Açık rızanın bir diğer koşulu alınan rızanın, ilgili kişinin bilgilendirilmiş olmasına dayanmasıdır. İlgili kişinin bilgilendirilmesi şartı, ilgili kişilere hukuki koruma sağlamanın en etkili yoludur. Çünkü bu sayede ilgili kişiler veri işleme sürecinden haberdar olabilmekte ve başvurabilecekleri hukuki korumalar hakkında karar verebilmektedirler⁵⁵⁰. Aynı zamanda bu gereklilik, ilgili kişilerin rıza gösterdikleri konuyu anlamalarına ve bu yönde bilinçli karar almalarına hizmet etmektedir⁵⁵¹. Bu anlamda veri sorumlusu tarafından ilgili kişiye aktarılan verinin

⁵⁴⁶ Taştan, s. 153; Özdemir, **Elektronik Haberleşme**, s. 168; Kemal Atasoy, “Kişilik Hakkı Kapsamında Sosyal Medyada Kişisel Verilerin Korunması ve Veri Sahibinin Rızası”, **Marmara Üniversitesi Hukuk Fakültesi Hukuk Araştırmaları Dergisi**, C. 22, S. 3, 2016, s. 290.

⁵⁴⁷ Dülger, **Kişisel Veriler**, s. 224; Kaya, **Elektronik Ticaret**, s. 151. Alışveriş sırasında “kişisel verilerimin işlenmesini ve paylaşılmasını kabul ediyorum” şeklinde rıza alınarak kişisel verilerin işlenmesinin kanun hükümlerine aykırı olduğuna dair bkz.: Kişisel Verileri Koruma Kurumu, **Doğru Bilinen Yanlışlar**, s. 27.

⁵⁴⁸ Anı, s. 131.

⁵⁴⁹ Dülger, **Kişisel Veriler**, s. 225; Erarslan, **Özel Nitelikli Kişisel Veriler**, s. 148.

⁵⁵⁰ Ayözger, s. 139; Şimşek, s. 90; Küzeci, s. 224; Akgül, s. 141.

⁵⁵¹ Çekin, **Big Data ve İrade Serbestisi**, s. 637.

niteliği, aktarmanın amaçları, aktarımın alıcıları, ilgili kişinin hakları, rızanın alınmasının sonuçları ve veri aktarımı ile ilgili tüm konulara ilişkin net ve anlaşılır bir şekilde, doğru ve tam bilgi verilmelidir⁵⁵². Örneğin, 22.07.2020 tarihli ve 2020/559 sayılı Kurul kararına konu olan incelemede, veri sorumlusu müşterilere reklam, promosyon amaçlı iletiler göndermek için onların bilgilerinin, hizmet aldığı üçüncü kişilerle paylaşılacağına dair bilgilendirme yaparak açık rızalarını almış olsa da, bilgilendirmede bu üçüncü kişilerin yurt dışında bulunabileceği ve dolayısıyla müşterilerin verilerinin yurt dışına aktarılabilmesi hususu açık ve anlaşılır bir biçimde beyan edilmediği için bu aktarım, Kurul tarafından hukuka aykırı olarak kabul edilmiştir⁵⁵³.

Kişisel verilerin aktarılmasına ilişkin verilecek açık rızanın geçerli sayılması için veri sorumlusu tarafından yerine getirilmesi gereken bilgilendirme şartının ne şekilde yapılacağı, birçok hukuki düzenlemelerde belirli kural ve yöntemlere tabi tutulmuş ve özellikle açık rızanın geçerlilik şartı olmasının yanı sıra veri sorumlusu için de ayrıca bir yükümlülük olarak düzenlenmiştir. Bu yükümlülük KVKK'nın 10. maddesinde “veri sorumlusunun aydınlatma yükümlülüğü” başlığı altında düzenlenmiştir. Buna göre veri sorumlusu, açık rızasının alınması bakımından ilgili kişiyi, kişisel verilerin hangi amaçla işleneceği, işlenen kişisel verilerin kimlere ve hangi amaçla aktarılabilmesi ve kişisel veri toplamanın yöntemi ve hukuki sebebi hakkında bilgilendirecektir. Şunu da belirtmek gerekir ki Kanun'da sayılan bilgilendirme ölçütleri, asgari ölçütlerdir⁵⁵⁴. Aydınlatma metninin içeriği somut olayın özelliklerine göre, maddede sayılanların dışına çıkmayı gerektirebilir⁵⁵⁵.

Aktarılacak verinin trafik veya konum verisi olması hâlinde elektronik haberleşme mevzuatında ayrıcalıklı bir düzenleme öngörülmüştür. Şöyle ki “Elektronik Haberleşme Sektöründe Kişisel Verilerin İşlenmesi ve Gizliliğin Korunmasına İlişkin Yönetmelik” m.8 uyarınca, trafik ve konum verilerinin üçüncü taraflara aktarımının söz konusu olduğu durumlarda; aktarılacak verinin kapsamı,

⁵⁵² Article 29 Working Party, **Definition of Consent**, s. 19; Küzeci, s. 235; Dülger, **Kişisel Veriler**, s. 225; Taştan, s. 159; Zor, s. 138.

⁵⁵³ Bkz.: Kişisel Verileri Koruma Kurulu, 22/07/2020 tarih ve 2020/559 sayılı Kararı, (çevrimiçi), <https://kvkk.gov.tr/Icerik/6790/2020-559>, 03.09.2021.

⁵⁵⁴ Dülger, **Kişisel Veriler**, s. 526.

⁵⁵⁵ Yücedağ, **Hukuka Uygunluk Sebepleri**, s. 774.

aktarılabak kişinin adı ve açık adresi, aktarma amacı ve süresi, üçüncü tarafın yurt dışında olması durumunda verinin aktarılabacağı ülkenin adı hakkında bilgi verildikten sonra açık rıza alınır. Bu bilgilerde herhangi bir değışiklik olduđu durumda açık rızanın yeniden alınması gerekmektedir. İşletmeciler, bu verilerin sadece açık rıza bilgilendirmesinde belirtilen üçüncü taraflarca ve belirtilen amaçla işlenmesini temin etmekle yükümlüdür.

Aydınlatma yükümlülüğünün yerine getirilmesi esnasında uyulması gereken usul ve esaslar, “Aydınlatma Yükümlülüğünün Yerine Getirilmesinde Uyulacak Usul ve Esaslar Hakkında Tebliğ”⁵⁵⁶ (Aydınlatma Tebliği) m.5’te düzenlenmiştir. Buna göre, kişisel veri işlendiği her durumda aydınlatma yükümlülüğü yerine getirilmeli (m.5/f.1/a), veri işleme amacı değıştiğinde, veri işleme faaliyetinden önce bu amaç için aydınlatma yükümlülüğü ayrıca yerine getirilmeli (m.5/f.1/b), veri sorumlusunun farklı birimlerinde kişisel veriler farklı amaçlarla işleniyorsa, aydınlatma yükümlülüğü her bir birim nezdinde ayrıca yerine getirilmeli (m.5/f.1/c), sicile kayıt yükümlülüğünün bulunması durumunda, aydınlatma yükümlülüğü çerçevesinde ilgili kişiye verilecek bilgiler, sicile açıklanan bilgilerle uyumlu olmalıdır (m.5/f.1/ç).

Bilgilendirme gerçekleştirilirken anlaşılır ve basit bir dil kullanılmasına da dikkat edilmelidir. Kişinin, anlayamayacağı terimlerin ya da okumakta güçlük çekeceği oranda küçük puntolarla yazılmış ve sıkışık ifadelerin yer aldığı bir formu imzaladığında ilgili kişi bilgilendirilmiş sayılmayacaktır⁵⁵⁷. Bilgilendirme yapılırken eksik, yanıltıcı ve yanlış bilgilere yer verilmemelidir.

Belirtmek gerekir ki, aydınlatma yükümlülüğünün yerine getirilmesi, ilgili kişinin talebine bağlı değildir (m.5/f.1/d) ve yükümlülüğünün yerine getirildiğinin ispatı veri sorumlusuna aittir (m.5/f.1/e).

Bu hususta ele alınması gereken diğer önemli husus ise, bilgilendirme zamanının belirlenmesidir. Bununla ilgili, Aydınlatma Tebliği’nin 6. maddesinde, kişisel verilerin aktarılabak olması hâlinde, en geç ilk kez aktarımın yapılacağı

⁵⁵⁶ RG. T. 10.03.2018, S. 30356.

⁵⁵⁷ Küzeci, s. 242; İmançlı, s. 188, Yılmaz, s. 141; Dölger, **Kişisel Veriler**, s. 473; Çekin, **Kişisel Verilerin Korunması**, s. 178.

esnada ilgili kişiyi aydınlatma yükümlülüğünün yerine getirilmesi gerektiği öngörülmüştür. Hangi koşullar altında olursa olsun, açık rızaya dayalı aktarım için bilgilendirme aktarma eyleminden önce gerçekleştirilmelidir⁵⁵⁸.

Son olarak şunu da belirtmek gerekir ki aydınlatma yükümlülüğünün kapsamı daha geniştir, sadece açık rızanın alınmasına ilişkin bilgilendirme ile sınırlı değildir. Kişisel verilerin işlenmesine ilişkin herhangi hukuka uygunluk şartlarının varlığı hâlinde de veri sorumlusu tarafından yerine getirilmesi gerekmektedir⁵⁵⁹.

4. Özgür İradeyle Alınmış Olma

Kişisel verilerin aktarılmasına ilişkin verilen rızanın geçerli sayılması için gereken bir diğer şart ise, bu kişinin rızasını hiçbir baskı ve mecburiyet altında kalmadan, özgür iradesi ile vermiş olmasıdır. Diğer bir anlatımla, rıza ilgili kişinin özgür iradesinin yansıması olarak, serbest ve özgür bir zihinsel etkinliğin ürünü olmalıdır⁵⁶⁰. Rızanın özgür iradeyle verilmiş olması, ilgili kişiye gerçek anlamda bir tercih imkânının sunulmasını ifade etmektedir⁵⁶¹. Bir başka ifadeyle, rıza beyanından doğacak muhtemel sonuçlar, kişinin tercih özgürlüğüne engel teşkil edecek nitelikteyse rızanın özgür iradeyle açıklandığından bahsedilemez. Bu unsur aynı zamanda ilgili kişinin, verilerinin aktarılmasına rıza göstermediği takdirde olumsuz sonuçlara maruz bırakılmamasını sağlamaya hizmet etmektedir.

İlgili kişinin irade beyanı olan rıza, veri sahibinin yaptığı davranışın bilincinde ve kendi kararı olması hâlinde geçerlilik kazanacaktır. Bu nedenle, korkutma, tehdit, cebir, hile, hata, zorlama, aldatma vs. gibi özgür iradeyi sakatlayan her türlü fiil, kişinin vermiş olduğu rızayı geçersiz kılacaktır⁵⁶². Ayrıca, tarafların eşit olmadığı veya bir tarafın diğeri üzerinde sosyal, ekonomik veya kültürel olarak etkin

⁵⁵⁸ Dülger, **Kişisel Veriler**, s. 227; Cihan Avcı Braun, “Kişisel Verilerin İşlenmesinde Rıza”, **Yeditepe Üniversitesi Hukuk Fakültesi Dergisi**, C. 25, S. 1, 2018, s. 15.

⁵⁵⁹ Dülger, **Kişisel Veriler**, s. 527; Erarslan, **Özel Nitelikli Kişisel Veriler**, s. 121; İmançlı, s. 187; Yücedağ, **Hukuka Uygunluk Sebepleri**, s. 773.

⁵⁶⁰ Küzeci, s. 266.

⁵⁶¹ Taştan, s. 155; Çekin, **Kişisel Verilerin Korunması**, s. 80.

⁵⁶² Kişisel Verileri Koruma Kurumu, **Açık Rıza Rehberi**, s. 6; Dülger, **Kişisel Veriler**, s. 227; Çekin, **Kişisel Verilerin Korunması**, s. 91-92; Avcı Braun, s. 21; Göçmen Uyarer, s. 112; Zor, s. 139; Hakalmaz, s. 83.

olduğu durumlarda özgür iradenin özellikle sorgulanması gerekir⁵⁶³. Örneğin, işçinin, kişisel verilerinin üçüncü bir şirkete aktarılmasına rıza göstermeme imkânı veya rıza göstermediği takdirde herhangi olumsuz sonuçlara maruz kalmayacağı, işveren tarafından temin edilmemişse özgür iradeyle verilmiş bir açık rızadan söz edilemez⁵⁶⁴.

Her ne kadar Kanun'da yer verilmese de maddenin gerekçesinde ve AB düzenlemelerinde irade beyanının “*tereddüde yer bırakmayacak açıklıkta olması*” gerektiği belirtilmiştir. Buna göre, ilgili kişinin rızasını aktif bir davranışla açıklaması gerekmektedir. Bu bağlamda, örtülü irade beyanının bir türü olan susma (eylemsizlik) kural olarak, kabul niteliğinde bir irade beyanı olarak nitelendirilemez⁵⁶⁵. Bu nedenle, ilgili kişinin rıza gösterip göstermediğine dair herhangi bir şüphenin bulunmaması için mutlaka kişinin aktif bir davranışta bulunması gerekmektedir⁵⁶⁶. Dolayısıyla irade beyanına ilişkin kuşku mevcutsa veya aktif bir davranış bulunmamaktaysa rıza geçersiz kabul edilmelidir.

Özgür irade ile verilmiş bir rızadan bahsedilebilmesi için açık rızanın, bir mal veya hizmetin sunulmasının ön şartı olarak sunulmaması gerekmektedir⁵⁶⁷. Örneğin, çevrimiçi alış verişi hizmeti sunan bir şirket tarafından, bu hizmetten yararlanmak isteyen müşterilerin kişisel verilerinin, hizmetin sunulmasıyla ilgilisi olmayan başka bir şirkete aktarılması şartını üyelik sözleşmesinin kurulması için zorunlu kılması hâlinde özgür iradeyle verilmiş rıza söz konusu değildir. Nitekim, Kurul'un “Amazon Turkey” kararında⁵⁶⁸, müşterinin açık rızası hizmet sunumuna önkoşul olarak alındığı için, özgür iradenin sakatlandığı sonucuna varılmıştır. GDPR m.7/f.4 uyarınca, rızanın özgür bir iradeyle dayalı olarak veriliş ve verilmemesi denetlenirken, her şeyden önce bir hizmetin sağlanması da dâhil olmak üzere bir sözleşmenin ifasının o sözleşmenin ifası için gerekmeyen kişisel verilerin işlenmesine yönelik bir rızaya bağlanıp bağlanmadığına ayrıca dikkat edilmesi gerektiği belirtilmiştir. Bu

⁵⁶³ Dülger, **Kişisel Veriler**, s. 227-228; Taştan, s. 155; Kişisel Verileri Koruma Kurumu, **Açık Rıza Rehberi**, s. 7; Voigt/ Bussche, s. 95; Hakalmaz, s. 84.

⁵⁶⁴ Kişisel Verileri Koruma Kurumu, **Açık Rıza Rehberi**, s. 7.

⁵⁶⁵ Taştan, s. 157;

⁵⁶⁶ Giakoumopoulos/ Buttarelli/ O’Flaherty, **Handbook**, s. 149.

⁵⁶⁷ Dülger, **Kişisel Veriler**, s. 227, 233-234; Çekin, **Kişisel Verilerin Korunması**, s. 85.

⁵⁶⁸ Bkz.: Kişisel Verileri Koruma Kurulu 27/02/2020 tarihli ve 2020/173 karar, (çevrimiçi), <https://www.kvkk.gov.tr/Icerik/6739/2020-173>, 06.07.2021.

hususla bazı yazarlar tarafından haklı olarak, zorlamaya varmayacak derecede etkilemeye çalışmanın, özgür iradenin sakatlanması anlamına gelmeyeceği, aksi yöndeki yorumun ticaret hayatına ket vuracağı belirtilmiştir⁵⁶⁹. Bu hususta KVKK’da herhangi bir hüküm bulunmasa da Bankaların Bilgi Sistemleri ve Elektronik Bankacılık Hizmetleri Hakkında Yönetmelik m.10 uyarınca, “müşterinin, bilgilerini paylaşmaya dair açık rıza göstermesinin verilecek hizmet için bir ön şart hâline getirilemeyeceği” belirtilmiştir.

Rızanın özgür iradeye dayanması aynı zamanda ilgili kişinin istediği zaman rızasını geri çekebilmesini de ifade etmelidir. Bununla ilgili Türk hukukunda herhangi bir düzenleme bulunmasa da kanunun özünden hareketle, ilgili kişinin istediği zaman rızasını geri çekme imkânı sağlanmalıdır⁵⁷⁰. Ayrıca, bu imkân en az rızanın verildiği kadar kolay bir şekilde gerçekleştirilebilmelidir⁵⁷¹. Rızanın geri alınmasının, geriye dönük bir etkisi bulunmamaktadır. Başka bir deyişle, rıza geri alınmadan önce gerçekleştirilen rızaya dayalı veri aktarımları hukuka uygun olarak kabul edilecektir⁵⁷². Kurum’un Whatsapp hakkındaki 12.01.2021 tarihli kamuoyu duyurusunda da ilgili kişinin açık rızasını geri alma işleminin sadece ileriye yönelik sonuç doğuracağı ve geri alma beyanının veri sorumlusuna ulaştığı andan itibaren açık rızaya dayalı olarak gerçekleştirilen tüm faaliyetlerin durdurulması gerektiği ifade edilmiştir⁵⁷³.

C. Açık Rızanın Aranmadığı Durumlar

Kişisel verilerin aktarılabilmesi için ilgili kişinin rızası olmasa dahi, KVKK’da öngörülen bazı koşullarda kural olarak hukuka aykırı kabul edilen kişisel verilerin aktarılması eylemi, hukuka uygun hâle gelmektedir. Dolayısıyla bu

⁵⁶⁹ Dülger, **Kişisel Veriler**, s. 227; Göçmen Uyarer, s. 113; Hakalmaz, s. 83. Bu yönde Kurulun aldığı karar için bkz.: Kişisel Verileri Koruma Kurulu 25.03.2019 tarihli ve 2019/82 sayılı karar.

⁵⁷⁰ Dülger, **Kişisel Veriler**, s. 227; Göçmen Uyarer, s. 115-116; Çekin, **Kişisel Verilerin Korunması**, s. 97; Erarslan, **Özel Nitelikli Kişisel Veriler**, s. 123; Taştan, s. 165; Hakalmaz, s. 87.

⁵⁷¹ Kişisel Verileri Koruma Kurumu, **Doğru Bilinen Yanlılar 2**, s. 18; Küzeci, s. 237; Dülger, **Kişisel Veriler**, s. 230, 238; Ayözger Öngün, s. 137; İmançlı, s. 138-139.

⁵⁷² Kişisel Verileri Koruma Kurumu, **Doğru Bilinen Yanlılar 2**, s. 17-18; Develioğlu, s. 53; İmançlı, s. 139; Göçmen Uyarer, s. 116; Çekin, **Kişisel Verilerin Korunması**, s. 98; Hakalmaz, s. 87.

⁵⁷³ Kişisel Verileri Koruma Kurumu, Whatsapp Uygulaması Hakkında Kamuoyu Duyurusu, 12.01.2021, (çevrimiçi), <https://www.kvkk.gov.tr/icerik/6856/whatsapp-uygulaması-hakkında-kamuoyu-duyurusu>, 14.03.2021.

hükümler hukuka uygunluk niteliğini haizdir⁵⁷⁴. Kişisel verilerin aktarılması, veri işleme failiyetinin bir türü olduğundan, açık rızanın bulunmadığı durumlarda aranan hukuka uygunluk sebepleri için farklı düzenlemeye gidilmemiştir. Sadece kişisel verilerin, açık rıza bulunmadığı durumlarda işlenmesini düzenleyen maddelere - m.5/f.2 (genel nitelikli kişisel verilerin işlenmesi), m.6/f.3 (özel nitelikli kişisel verilerin işlenmesi) atıfta bulunulmuştur.

Kanun'da öncelikle kişisel verilerin ilgili kişinin açık rızası ile aktarılabileceği, devamında ise açık rızanın bulunmadığı durumlarda kişisel verilerin aktarılmasına imkân tanıyan hukuka uygunluk sebepleri belirtildiği için bu düzenleniş biçimi, açık rızanın diğer hukuka uygunluk sebepleri karşısında bir önceliğe sahip olduğu izlenimini yaratmıştır. Fakat belirtmek gerekir ki her ne kadar açık rıza ve diğer hukuka uygunluk sebepleri ayrı fıkralar hâlinde düzenlenmişse de, bu, açık rıza ve diğer hukuka uygunluk sebepleri arasında bir hiyerarşi bulunduğu anlamına gelmemelidir⁵⁷⁵. Bunun aksine bütün hukuka uygunluk sebepleri eşit değerdedir. Bu yanlışlığı ortadan kaldırmak amacıyla Kurum tarafından yapılan açıklamada da açık rıza, Kanun'daki diğer hukuka uygunluk sebeplerinden biri olarak değerlendirilmiş ve diğer veri işleme şartları karşısında bir üstünlüğü bulunmadığı belirtilmiştir⁵⁷⁶. Kanaatimizce, tereddütte mahal bırakmamak adına maddenin açık rıza ve diğer hukuka uygunluk sebepleri arasında bir hiyerarşi olmadığını gösterir şekilde düzenlenmesi isabetli olacaktır⁵⁷⁷.

KVKK'da öngörülen hukuka uygunluk sebeplerinin varlığına rağmen veri aktarımı için, veri sorumlusunun açık rızaya başvurup başvurmayacağı doktrinde tartışma konusu olmuştur. Şöyle ki, bizim de katıldığımız görüşe göre, öncelikle aktarılma için diğer hukuka uygunluk sebeplerinin bulunup bulunmadığı

⁵⁷⁴ Çekin, **Kişisel Verilerin Korunması**, s. 87.

⁵⁷⁵ Çekin, **Kişisel Verilerin Korunması**, s. 88; Yücedağ, **Hukuka Uygunluk Sebepleri**, s. 773; Şehriban İpek Aşıkoğlu, "Kişisel Verilerin İşlenmesinde Hukuka Uygunluk Sebepleri", **Türk Hukukunun Avrupa Birliği Hukukuna Uymu Özel Hukuk: Acquis Communautaire'in Alınması, Açıklamalar, Değerlendirmeler, Öneriler** içinde, Ed.: Arslan Kaya, Baki İlkay Engin, Ali Paşlı, Şehriban İpek Aşıkoğlu, Elif Oğuz, İstanbul, İstanbul Üniversitesi Yayınevi, 2020, s. 1075; Dülger, **Kişisel Veriler**, s. 236-237, 390; İmançlı, s. 132; Göçmen Uyarer, s. 114; Aşıkoğlu/ Uzun, s. 934, Hakalmaz, s. 74; Çelik, s. 50.

⁵⁷⁶ Kişisel Verileri Koruma Kurumu, **Doğru Bilinen Yanlıklar 2**, s. 15.

⁵⁷⁷ Aşıkoğlu, **Hukuka Uygunluk Sebepleri**, s. 1075.

değerlendirilmeli, bu sebeplerin bulunmadığı takdirde ilgili kişinin açık rızasına başvurulmalıdır⁵⁷⁸. Çünkü Kanun’da öngörülen bir hukuka uygunluk sebebinin varlığına rağmen açık rıza alındığı zaman, ilgili kişi haklı olarak istediği zaman rızasını geri alabileceğini düşünebilir. Hâlbuki başka bir hukuka uygunluk sebebi bulunduğundan ilgili kişinin rızasını geri alması, hiçbir anlam ifade etmeyecektir. Dolayısıyla Kanun’da öngörülen hukuka uygunluk sebebinin varlığına rağmen, ilgili kişiden açık rıza talep edilmesi yanıltıcı bir uygulamadır⁵⁷⁹. Kurum bu hususla ilgili *“diğer kişisel veri işleme şartlarının varlığı durumunda açık rıza alınmasının ilgili kişinin yanıltılması ve yanlış yönlendirilmesi dolayısıyla veri sorumlusunca hakkın kötüye kullanılması anlamına geleceği”* yönünde açıklama yapmıştır⁵⁸⁰. Örneğin, Kurul’un 22.07.2020 tarihli ve 2020/559 sayılı kararına konu olan inceleme kapsamında veri sorumlusunun sunduğu savunma yazısında kişisel verilerin yurt dışına aktarılmasına dair meşru menfaatinin bulunduğu belirtilmiş, devamında ise ilgili kişilere sunmuş olduğu aydınlatma ve rıza metninde *“...Şirketimiz tarafından sunulan ürün ve hizmetlerin sizlerin beğeni, kullanım alışkanlıkları ve ihtiyaçlarınıza göre özelleştirerek sizlere önerilmesi ve tanıtılması, kabulünüz kapsamında paylaşmış olduğunuz iletişim bilgilerinize reklam, promosyon vb. ticari elektronik ileti gönderilmesi, saklanmasını ve ... gönderim sağlanması için hizmet aldığı üçüncü kişilerle paylaşılması amaçlarıyla işbu metni kabul etmeniz hâlinde vermiş olduğunuz açık rızanız kapsamında işlenebilecektir.”* şeklinde bir beyana yer verildiği belirtilmiştir. Kurul ise bu beyanın, kişisel veri işleme faaliyetinin asıl olarak ve yalnızca ilgili kişilerin açık rızalarına dayanılarak gerçekleştirildiği izlenimine neden olduğunu belirtmiştir⁵⁸¹.

Karşı görüşe göre⁵⁸² ise uygulamada çoğu zaman hukuka uygunluk sebeplerinden hangisinin bulunup bulunmadığı belirsizdir. Bu nedenle veri

⁵⁷⁸ Küzeci, s. 342; Dülger, **Kişisel Veriler**, s. 390; Selek, s. 934; İmançlı, s. 132; Tepe, s. 62-64; Hakalmaz, s. 74; Kurul’un bu yönde kararı için bkz.: 22.07.2020 tarihli ve 2020/559 sayılı karar, (çevrimiçi) <https://kvkk.gov.tr/Icerik/6790/2020-559>, 29.07.2021.

⁵⁷⁹ Küzeci, s. 342; Dülger, **Kişisel Veriler**, s. 390-391; İmançlı, s. 133; Yücedağ, **Hukuka Uygunluk Sebepleri**, s. 773, 786; Kişisel Verileri Koruma Kurumu, **Doğru Bilinen Yanlışlar**, s. 25.

⁵⁸⁰ Bkz.: Kişisel Verileri Koruma Kurumu, Hizmetin Açık Rıza Şartına Bağlanması, (çevrimiçi), <https://www.kvkk.gov.tr/Icerik/5412/Acik-Rizadin-Hizmet-Sartina-Baglanmasi>, 22.09.2021; Aynı yönde karar için bkz.: Kişisel Verileri Koruma Kurulu, 22.07.2020 tarihli ve 2020/559 sayılı kararı.

⁵⁸¹ Bkz.: Kişisel Verileri Koruma Kurulu, 22.07.2020 tarihli ve 2020/559 sayılı kararı.

⁵⁸² Çekin, **Kişisel Verilerin Korunması**, s. 89-90.

sorumlusunun, geçersizlik riskine karşı veri aktarımı faaliyetini açık rızaya dayandırması doğal karşılanmalıdır. Bu görüş, diğer hukuka uygunluk sebeplerinin varlığına rağmen açık rızanın tercih edilmesinin, yanıltıcı bir uygulama olduğunu kabul etmekle beraber, açık rıza ve diğer hukuka uygunluk sebepleri arasında hiyerarşik bir ilişki bulunmadığı için veri sorumlusunun, aktarma faaliyetini dilediği hukuki sebebe dayandırabileceğini savunmaktadır. Fakat bu durumda ilgili kişi, açık rızasını geri aldığı takdirde veri sorumlusunun hukuki sebebi değiştirmesi imkânsızdır. Başka bir anlatımla, veri sorumlusunun bu hakkı seçimlidir. Dolayısıyla, bir hukuki sebebin tercih edilmesiyle birlikte diğer hukuka uygunluk sebepleri de tükenmektedir⁵⁸³.

1. Genel Nitelikli Kişisel Veriler Açısından

a. Kanunlarda Açıkça Öngörülme

Genel nitelikli kişisel verilerin, ilgili kişinin açık rızası aranmaksızın aktarılması için aranan sebepler KVKK m.5/f.2’de düzenlenmiştir. Bunlardan birincisi, kanunlarda açıkça öngörülmüş olma şartıdır. Şöyle ki şayet kanunlarda kişisel verilerin aktarılmasına ilişkin açık bir hüküm mevcut ise ilgili kişinin açık rızası aranmaksızın veri aktarımı gerçekleştirilebilecektir. Örneğin, 1774 sayılı Kimlik Bildirme Kanunu⁵⁸⁴ gereğince otel işletmecileri, işletmelerinde konaklayan kişilerin kişisel verilerini genel kolluk kuvvetlerine anlık bildirmek, talep hâlinde Devlet İstatistik Enstitüsü’ne vermek zorundadırlar (madde 2). Bunun için otelde konaklayan ilgili kişinin açık rızasını almaya gerek yoktur.

Yine 5502 sayılı Sosyal Güvenlik Kurumuna İlişkin Bazı Düzenlemeler Hakkında Kanun’un 35’inci maddesi uyarınca SGK’nın, bu Kanun ve diğer mevzuatla verilen görevleri yerine getirmek amacıyla işlediği kişisel veriler ile ticari sır niteliğinde olan verileri, gerçek veya tüzel kişilerle paylaşabilmesi için veri sahibinin noter onaylı muvafakatinin veya e-Devlet uygulaması üzerinden kimlik teyidi ile verilen izninin bulunması gerekmektedir. Fakat maddenin devamında,

⁵⁸³ Çekin, **Kişisel Verilerin Korunması**, s. 90; Tepe, s. 63.

⁵⁸⁴ RG. T. 11.07.1973, S. 14591.

10.12.2003 tarihli ve 5018 sayılı Kamu Mali Yönetimi ve Kontrol Kanununun⁵⁸⁵ eki (I), (II), (III) ve (IV) sayılı cetvellerde yer alan kamu idareleri ile Türkiye Cumhuriyet Merkez Bankasının ilgili mevzuatında belirtilen görevleri yapabilmeleri için ihtiyaç duydukları sağlık verisi dışındaki kişisel veriler ile ticari sır niteliğindeki verilerin paylaşılabileceği ve SGK'nın, kimliği belirli veya belirlenebilir bir gerçek veya tüzel kişiyle ilişkilendirilemeyecek şekilde anonim hâle getirdiği verileri araştırma, planlama ve istatistik gibi amaçlar için kamu idareleri, Türkiye Cumhuriyet Merkez Bankası, bilimsel araştırma yapan kamu personeli, bilimsel dernekler, kamu kurumu niteliğindeki meslek kuruluşları veya üniversiteler ile ücretsiz olarak paylaşabileceği düzenlenmiştir. Anlaşıldığı üzere, bunun için veri sahibinin rızasının alınması şartı aranmamıştır.

Yine 7223 sayılı Ürün Güvenliği ve Teknik Düzenlemeler Kanunu'nda yetkili kuruluşun, kişisel verilere dair edindiği bilgilerin gizliliğini korunmakla yükümlü olduğu belirtilmiştir. Aynı zamanda insan sağlığı ve güvenliğinin gerektirdiği durumlarda, bu bilgilerin açıklanması, bu yükümlülüğün kapsamı dışında tutulmuştur (m.23/f.1). Buradan çıkan sonuca göre, kişisel verilerin açıklanması, insan sağlığı ve güvenliği açısından gerekli olduğunda ilgili kişinin açık rızasının alınmasına gerek kalmayacaktır.

Yine 6102 sayılı Türk Ticaret Kanunu'nun⁵⁸⁶ 780'inci maddesi uyarınca, çek alacaklıları, ellerinde bulunan çek ile çek hesabı sahibine ve bu çeki düzenleyenlere ilişkin verilere karekod aracılığıyla erişim sağlayabilir. Çek alacaklıları bu karekod ile; çek hesabı sahibinin adı, soyadı veya ticaret unvanı, çek hesabı sahibinin tacir olması hâlinde, ticaret siciline tescil edilen yetkililerinin adı, soyadı veya ticaret unvanı, çek hesabı sahibinin, çek hesabı bulunan toplam banka sayısı, çek hesabı sahibine ait bankalara ibraz edilmemiş çek adedi ve tutarı gibi kanunda öngörülen diğer bilgiler, çek sahibi ya da cirantanın rızası aranmaksızın üçüncü kişilerin erişimine sunabilirler. Görüldüğü üzere, TTK ile çek alacaklılarına, karekod aracılığıyla çek hesabı sahibi ve bu çeki düzenleyenlere ilişkin verilere ulaşma ve

⁵⁸⁵ RG. T. 24.12.2003, S. 25326.

⁵⁸⁶ RG. T. 14.02.2011, S. 27846.

kanunda öngörülen durumlarda bu verileri, veri sahibinin rızası olmadan üçüncü kişilere aktarma hakkı tanınmıştır⁵⁸⁷.

Düzenlemede özellikle “açıkça” öngörülmeden bahsedildiği için, bu hükmün dar anlamda yorumlanması gerekmektedir⁵⁸⁸. Bu nedenle kanunlarda kişisel verilerin aktarılmasına ilişkin genel bir yetki verilmesi, bu kapsamda değerlendirilemez⁵⁸⁹. Başka bir deyişle, ilgili kanun hükümleri uyarınca aktarılan verilerin kapsamı, kanunlarda belirtilen veri içeriği veya veri işleme amacı ile sınırlı olmalıdır⁵⁹⁰. Örneğin, 5490 sayılı Nüfus Hizmetleri Kanunu⁵⁹¹ m.43’te “...*Nüfus kayıt örneklerinde, bunları istemeye yetkili olanlar tarafından açıkça ve gerekçeli olarak istenmediği takdirde, kimlik bilgileri dışında kişisel bilgilere yer verilmez. Bu belgeler üzerinde silinti ve kazıntı yapılamaz*” ibaresi yer almaktadır. Bu noktadan hareketle nüfus kaydı örneği vermeye yetkili kamu kuruluşun tarafından, talep edilenden daha fazla kimlik bilgisinin yer aldığı belgenin düzenlenmesi ve paylaşılması hukuka aykırılık teşkil edecektir⁵⁹².

Bu düzenleme esasen Anayasa’da da yer alan “*kişisel verilerin korunmasına ilişkin esas ve usuller kanunla düzenlenir*” hükmünün bir yansıması olarak görülebilir⁵⁹³. Düzenlemede sadece kanunlarda açıkça öngörülme şartı arandığı için yönetmelik, tüzük gibi diğer mevzuatlarda öngörülen kişisel veri aktarımı faaliyetlerinin ne şekilde değerlendirileceğinin açıklığa kavuşturulması gerekmektedir. Şöyle ki Anayasa’da yer alan kişisel verilerin işlenmesine ilişkin hususların ancak kanunlar ile düzenlenebileceğine ilişkin hüküm gereğince, tek başına herhangi bir kanundan yetki almamış bir yönetmelik ile kişisel verilerin aktarımının düzenlenmesi Anayasa’ya aykırılık teşkil edeceğinden, sadece ilgili olduğu kanunlarda açıkça usul ve esaslarının düzenlenmesi öngörülen hususlarda

⁵⁸⁷ Erarslan, **Özel Nitelikli Kişisel Veriler**, s. 232.

⁵⁸⁸ Göçmen Uyarer, s. 131; Aşıkoğlu, **Hukuka Uygunluk Sebepleri**, s. 1070.

⁵⁸⁹ İmançlı, s. 140.

⁵⁹⁰ Murat Altındere, **Kişisel Verilerin Korunması Hukuku ve Uygulaması**, Ankara, Adalet, 2020, s. 43; Dülger, **Kişisel Veriler**, s. 392.

⁵⁹¹ RG. T. 29.04.2006, S. 26153.

⁵⁹² Aşıkoğlu, **Kişisel Veriler**, s. 116.

⁵⁹³ Aşıkoğlu, **Kişisel Veriler**, s. 112.

yönetmelik çerçevesinde düzenlenen kişisel veri aktarım faaliyetini hukuka uygun kabul etmek gerekmektedir⁵⁹⁴.

Kişisel verilerin aktarılmasına ilişkin KVKK'da ve diğer kanunlarda yer alan hükümler arasındaki ilişkinin KVKK'da açıkça düzenlenmemesi ve bu konuda Kurul'un yayınlanmış bir kararının bulunmaması, söz konusu hükümlerin çelişmesi hâlinde hangisinin uygulanacağı hususunda belirsizliğe sebep olmaktadır⁵⁹⁵. Kurum, bu doğrultuda KVKK'nın kişisel verilerin korunması ve işlenmesi açısından çerçeve bir düzenleme niteliği taşıdığını ve kişisel verilerin işlenmesine ilişkin hükümler içeren sektörel düzenlemelerin KVKK ile uyumlu hale getirilmesi gerektiğini belirtmiştir⁵⁹⁶. Doktrindeki bir görüşe⁵⁹⁷ göre yurt dışına kişisel veri aktarımına ilişkin hükümler içeren diğer kanunların öncelikli uygulanması gerekse de, KVKK temel hak ve özgürlükleri düzenleyen bir kanun olduğundan, ilgili kişilerin temel hak ve özgürlüklerini daha kapsamlı himaye ettiği durumlarda Kurul, aktarımın m.9 kapsamında yapılması gerektiğine karar verebilmelidir. Başka bir görüşe⁵⁹⁸ göre ise Kurum'un konuyla ilgili yaklaşımı dikkate alındığında KVKK m.9 hükmü ile yurt dışına aktarıma ilişkin diğer kanun hükümleri arasında genel ve özel nitelikte hüküm şeklinde bir ayrıma gidilmesi, sorunun çözümü için yeterli olmayacağından, diğer kanun hükümlerinin KVKK'ya uygunluğu konusunda ayrıca değerlendirme yapılması gerekmektedir.

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

KVKK m.5/f.2/b uyarınca, fiilî imkânsızlık nedeniyle rızasını açıklayamayacak durumda bulunan veya rızasına hukuki geçerlilik tanınmayan kişinin kendisinin ya da bir başkasının hayatı veya beden bütünlüğünün korunması için zorunlu olması durumunda, açık rıza aranmaksızın veri aktarımı hukuka uygun bulunmaktadır. Görüldüğü üzere, bu hukuka uygunluk sebebinin unsurlarını, ilgili

⁵⁹⁴ Aşıkoğlu, **Kişisel Veriler**, s. 117-118; Aşıkoğlu, **Hukuka Uygunluk Sebepleri**, s. 1077.

⁵⁹⁵ Bilgi Information Technology Law Institute, s. 8; Çelik, s. 52.

⁵⁹⁶ Kişisel Verileri Koruma Kurumu, **Uygulama Rehberi**, s. 122.

⁵⁹⁷ Bilgi Information Technology Law Institute, s. 8.

⁵⁹⁸ Çelik, s. 53.

kişinin rızasını açıklamasının fiilen veya hukuken imkânsız olması ve kendisinin veya üçüncü kişinin hayati menfaatlerinin korunması için gerekli olması teşkil etmektedir⁵⁹⁹. Fiilî imkânsızlık; hastalık, sakatlık veya deprem, sel gibi dış etkenler nedeniyle kişinin fiziksel olarak rızasını açıklayamayacak durumda olmasını ifade ederken, hukuki imkânsızlık ise kişinin; hukuk sistemi karşısında ayırt etme gücüne sahip olma, ergin olma veya sınırlı olmama şartlarını karşılayamadığından dolayı rızasını açıklayamayacak durumda olmasını ifade etmektedir⁶⁰⁰. İlgili kişinin veya üçüncü kişinin hayati menfaati, kişinin sağlığı veya beden bütünlüğü ile doğrudan ilişkili olan bütün menfaatlerini ifade eder⁶⁰¹. Böyle durumlarda, ilgili kişinin farazi iradesi esas alınır. Çünkü zaten ilgili kişi içinde bulunduğu fiilî veya hukuki durum nedeniyle rızasını açıklayabilme imkânına sahip değildir⁶⁰².

Bu hukuka uygunluk sebebinin uygulama alanı bulabilmesi için bir aciliyetin söz konusu olması gerekmektedir. Şayet ilgili kişinin rızasının açıklanmasının beklenebileceği durum mevcut ise bu hukuka uygunluk sebebi geçerli olarak kabul edilmeyebilecektir⁶⁰³. Bu nedenle bu hukuka uygunluk sebebi, somut olayın özellikleri dikkate alınarak ve gereklilik ve ölçülülük ilkeleri ile sınırlandırılarak yorumlanmalıdır⁶⁰⁴. Örneğin, uzun süre haber alınamayan ve hayatından şüphe edilen kişinin, en son bulunduğu yerdeki telefon sinyalinin konum bilgilerinin paylaşılması için ilgili kişinin açık rızasını almaya gerek yoktur⁶⁰⁵.

c. Sözleşmenin Taraflarına Ait Kişisel Verilerin Aktarılmasının Gerekli Olması

KVKK m.5/f.2/c uyarınca, bir sözleşmenin kurulması veya ifasıyla doğrudan doğruya ilgili olması kaydıyla, sözleşmenin taraflarına ait kişisel verilerin işlenmesinin gerekli olması hâlinde açık rıza olmaksızın ilgili kişinin kişisel verilerinin aktarılması mümkündür. Bu hukuka uygunluk sebebinin üç temel unsuru bulunmaktadır; akdedilmesi düşünülen veya akdedilmiş bir sözleşmenin mevcut olması, aktarılacak kişisel verilerin sözleşmenin taraflarına ilişkin olması,

⁵⁹⁹ Aşıkoğlu, **Kişisel Veriler**, s. 119; Dülger, **Kişisel Veriler**, s. 394.

⁶⁰⁰ Erarslan, **Verilerin Aktarılması**, s. 102.

⁶⁰¹ Yücedağ, **Hukuka Uygunluk Sebepleri**, s. 777.

⁶⁰² Özdemir, **Elektronik Haberleşme**, s. 155.

⁶⁰³ Dülger, **Kişisel Veriler**, s. 396; Yücedağ, **Hukuka Uygunluk Sebepleri**, s. 777; Aşıkoğlu, **Kişisel Veriler**, s. 119; Zor, s. 146.

⁶⁰⁴ Aşıkoğlu, **Hukuka Uygunluk Sebepleri**, s. 1066.

⁶⁰⁵ Altındere, s. 44.

sözleşmenin kurulması veya ifası için doğrudan ilgili ve gerekli olması⁶⁰⁶. Bu hukuka uygunluk sebebinin uygulama alanı bulabilmesi için bu şartların aynı anda mevcut olması gerekmektedir. Örneğin, mesafeli satış sözleşmesi ile satın alınan bir ürünün kargo ile teslim edilmesi sırasında adres ve kimlik bilgilerinin taşıyıcı firmaya aktarılması bu kapsamda değerlendirilebilir⁶⁰⁷.

Sözleşmenin kurulabilmesi için zaten tarafların açık rızaları mevcut olduğundan dolayı, ayrıca kişisel verilerinin aktarılması için de rıza alınması, sözleşmenin doğasına aykırı olacaktır. Bu nedenle, tarafların birbirine yöneltmiş olduğu sözleşme kurma yönünde açık veya örtülü beyanın bulunup bulunmadığı değerlendirilmelidir. Şöyle ki ilgili kişinin sözleşme kurma rızası olmadan bir sözleşme taslağı hazırlayıp ve buna dayanarak ilgili kişinin kişisel verilerinin aktarılması hukuka uygun olarak kabul edilmeyecektir⁶⁰⁸.

Düzenlemede “işlenecek kişisel verinin sözleşmenin taraflarından birine ait olması” ibaresi kullanıldığından dolayı, tüzel kişilere dair verilerin KVKK’nın kapsamına dâhil olmadığını göz önünde bulundurarak, bu hukuka uygunluk sebebinin sadece kişisel verileri aktarılacak olan sözleşme tarafının, gerçek kişi olduğu durumlarda uygulanabileceği sonucu çıkarılabilir. Bu durumda, iki tüzel kişi arasında akdedilen sözleşmede, gerçek kişi olan temsilcilerin kişisel verilerinin aktarılması gerektiğinde başka bir hukuka uygunluk sebebinin bulunması gerekmektedir⁶⁰⁹. Bunun aksine, “işlenecek verilerin sözleşmenin taraflarından birine ait olması” şartına rağmen, sözleşmenin ifası için gerekli olduğu durumlarda, sözleşmenin tarafı olan şirketin çalışanlarının verilerinin de bu kapsamda aktarılabilmesi görüşü de mevcuttur⁶¹⁰.

⁶⁰⁶ Çekin, **Kişisel Verilerin Korunması**, s. 93; Küzeci, s. 344; Aşıkoğlu, **Kişisel Veriler**, s. 120; Zor, s. 147.

⁶⁰⁷ Dülger, **Kişisel Veriler**, s. 397.

⁶⁰⁸ Aşıkoğlu, **Kişisel Veriler**, s. 121.

⁶⁰⁹ Yücedağ, **Hukuka Uygunluk Sebepleri**, s. 778

⁶¹⁰ Anı, s. 109.

Veri aktarımı sözleşmenin kurulması veya ifası için gerekli olmalıdır. Şayet veri sorumlusu, ilgili kişinin haklarına daha az veya hiç müdahale etmeyen bir seçeneğe sahipse veri aktarımı gerekli kabul edilemeyecektir⁶¹¹.

d. Veri Sorumlusunun Hukuki Yükümlülüğünü Yerine Getirebilmesi İçin Zorunlu Olması

KVKK m.5/f.2/ç uyarınca, veri sorumlusunun hukuki yükümlülüğünü yerine getirebilmesi için kişisel verileri aktarılmasının zorunlu olduğu durumlarda veri aktarım faaliyeti hukuka uygun olacaktır. Veri sorumlusunun sözleşmesel yükümlülüğünü yerine getirmesi için zorunlu olan hâller bu kapsamda değerlendirilmeyecektir⁶¹². Zira sözleşmesel yükümlülükler için başka bir hukuka uygunluk sebebi zaten öngörülmüştür. Hukuki yükümlülüğün hukuken veri sorumlusuna yüklenmiş olması gerekir. Hukuki yükümlülük hem kanun hem de ikincil mevzuat ile getirilen düzenlemelerde öngörülmüş olabilir⁶¹³. Fakat bir hukuki yükümlülüğün bahs edebilmek için, veri sorumlusunun tercih imkânı bulunmamalı, ilgili düzenlemeye uyulması zorunlu olmalıdır⁶¹⁴.

Örneğin, işverenin 5510 sayılı Sosyal Sigortalar ve Genel Sağlık Sigortası Kanunu⁶¹⁵ uyarınca, çalıştırdığı işçiyi SGK'ya bildirme zorunluluğu bulunmaktadır. Yine aynı Kanun'un hükümleri gereği, bir iş kazasının olması durumunda işveren, iş kazasını o yerdeki yetkili kolluk kuvvetlerine derhal, SGK'ya da en geç kazadan sonraki 3 iş günü içinde "iş kazası ve meslek hastalığı bildirgesi" ile doğrudan ya da taahhütlü posta ile bildirmek zorundadır. İşveren, bu hukuki yükümlülüklerini yerine getirmek amacıyla çalışanın kişisel verilerini SGK'ya veya kolluk kuvvetlerine aktarırken çalışanın açık rızasına almasına gerek kalmayacaktır⁶¹⁶.

Veri sorumlusu hukuki yükümlülüğünü yerine getirirken veri aktarımını gereklilik ve ölçülülük ilkelerine uygun bir şekilde gerçekleştirmelidir⁶¹⁷. Örneğin, mahkeme tarafından talep edilen bir bilgi veya belgenin sunulması, bir hukuki

⁶¹¹ Çekin, **Kişisel Verilerin Korunması**, s. 93; Altındere, s. 44; Özkan, s. 109.

⁶¹² Dülger, **Kişisel Veriler**, s. 405; Taştan, s. 165-166.

⁶¹³ Yücedağ, **Hukuka Uygunluk Sebepleri**, s. 778.

⁶¹⁴ Yücedağ, a.y.

⁶¹⁵ RG. T. 16.06.2006, S. 26200.

⁶¹⁶ Altındere, s. 45.

⁶¹⁷ Aşkoğlu, **Kişisel Veriler**, s. 130.

yükümlülük olsa da talep edilen belge dışında fazla bilgi veya belge sunulması hukuka aykırı olarak nitelendirilecektir. Nitekim Kurum, 23 Şubat 2018 tarihli kararında, mahkemece talep edilmemiş olmasına rağmen davalıya ait kredi kartının altı aylık ekstresinin de banka tarafından mahkemeye sunulmasını hukuka aykırı bulmuş ve idari para cezası yaptırımını uygulamıştır⁶¹⁸.

Hukuki yükümlülük şartı kapsamında veri aktarabilmek için, veri aktarımı aynı zamanda zorunlu olmalıdır. Aktarma faaliyetinin bir hukuki yükümlülükle ilişkilendirilebilir olması, tek başına yeterli değildir, bu yönde bir zorunluluk bulunması şarttır⁶¹⁹. Başka bir deyişle, verilerin aktarılmasına ilişkin takdir yetkisi mevcut ise veri aktarımı bu kapsamda değerlendirilemeyecektir⁶²⁰.

e. Verinin İlgili Kişinin Kendisi Tarafından Alenileştirilmiş Olması

İlgili kişi tarafından alenileştirilen kişisel verilerin, açık rıza olmadan aktarılması KVKK m.5/f.2/d hükmü gereğince, hukuka uygun kabul edilecektir. Kurum tarafından hazırlanmış yayında⁶²¹ alenileştirme kavramı, “...herkes tarafından bilinir kılma” şeklinde tanımlanmıştır. Bununla ilgili maddenin gerekçesinde kişinin kendisi tarafından alenileştirilen, bir başka ifadeyle herhangi bir şekilde kamuoyuna açıklanmış olan verilerin işlenebileceği belirtilmiştir. Gerekçeye göre, herkes tarafından bilinebilecek hâle gelen verilerin işlenmesinde korunması gereken hukuki yarar bulunmamaktadır⁶²².

Gerekçede belirtilenin aksine şunu belirtmek gerekir ki bir verinin alenileştirilmiş olması, bu verilerin her şekilde ve her türlü amaç için aktarılmasını hukuka uygun hâle getirmeyecektir. Her ne kadar Kanun’da bir sınır belirlenmese de bu hükmün, amaca bağlılık ilkesine dayanarak dar yorumlanması gerektiği kanaatindeyiz. Nitekim Kurum tarafından yayınlanan duyuruda da, alenileştirme kavramının, alenileştirme iradesi ve alenileştirme amacı dikkate alınarak dar

⁶¹⁸ Aşkoğlu, a.y.; Karar metni için bkz. (çevrimiçi), <https://kisiselveri.com/wp-content/uploads/KurulKarariKarali-kucuk.jpg>, 12.10.2021.

⁶¹⁹ Dülger, **Kişisel Veriler**, s. 403.

⁶²⁰ Dülger, a.y.

⁶²¹ Bkz.: Kişisel Verileri Koruma Kurumu, 6698 Sayılı Kanun’da Yer Alan Kurumsal Terimler, s. 9, <https://www.kvkk.gov.tr/yayinlar/6698%20sayılı%20kanun%e2%80%99da%20yer%20alan%20kurumsal%20terim%40b0mler.pdf>, 28.09.2021.

⁶²² Bkz.: KVKK m.5 gerekçesi.

yorumlanmalıdır⁶²³. Başka bir deyişle ilgili kişi, verilerini hangi amaçla aleni hâle getirmişse aktarılma bu amaçla sınırlandırılmalıdır⁶²⁴. Örneğin, kiralık ev ilanı için internet sitesinde iletişim bilgilerini yayınlayan bir kişinin verileri, pazarlama amacı dışında aktarılmamalıdır. Çünkü kişi sadece pazarlama amacıyla iletişim bilgilerini alenileştirmiştir⁶²⁵. Nitekim Kurul da bu hususla ilgili bir kararında; kişisel verilerini bir internet sitesinde paylaşan ilgili kişiyi, onun mesleki yetkinliği ile ilgili değil sigortacılık faaliyeti ile ilgili aradığı için, Şirket tarafından şikâyetçinin verilerinin internette bulunma ve alenileştirme amacı dışında kullanıldığına ve sigorta şirketine idari para cezası uygulanmasına karar vermiştir⁶²⁶.

Alenileştirmenin amacı, ilgili kişinin beyanı esas alınarak belirlenecektir. Şayet böyle bir beyan yoksa alenileştirmenin amacı, alenileştirme işleminin doğası ve dürüstlük kuralı çerçevesinde belirlenmelidir⁶²⁷.

Burada dikkat edilmesi gereken diğer husus, verilerin ilgili kişi tarafından iradi olarak alenileştirilmiş olmasıdır⁶²⁸. Bu bakımdan hukuka aykırı olarak üçüncü kişi tarafından kamuya açıklanan kişisel veriler bu kapsamda değerlendirilmeyecektir⁶²⁹.

Kanun'un uygulanmayacağı istisnai hâlleri düzenleyen m.28/f.2/b'de, ilgili kişi tarafından alenileştirilen kişisel verilerin aktarıldığı durumlarda; veri sorumlusunun aydınlatma ve sicile kayıt yükümlülüğü, ilgili kişinin ise tazminat talep etme hakkı dışında m.11'de öngörülen haklarının bulunmadığı belirtilmiştir.

⁶²³ Kişisel Verileri Koruma Kurumu, "Alenileştirme" Hakkında Kamuoyu Duyurusu, (çevrimiçi), <https://www.kvkk.gov.tr/icerik/6843/-alenilestirme-hakkinda-kamuoyu-duyurusu>, 23.11.2021; Kişisel Verileri Koruma Kurumu, **Doğru Bilinen Yanlıklar**, s. 29.

⁶²⁴ Yücedağ, **Hukuka Uygunluk Sebepleri**, s. 780; Göçmen Uyarer, s. 133; Altındere, s. 46; Aşıkoğlu, **Kişisel Veriler**, s. 125; Erarslan, **Özel Nitelikli Kişisel Veriler**, s. 289; Zor, s. 152; Özkan, s. 112.

⁶²⁵ Altındere, a.y.

⁶²⁶ Bkz.: Kişisel Verileri Koruma Kurulu, 07/11/2019 tarihli ve 2019/331 sayılı kararı, (çevrimiçi), <https://www.kvkk.gov.tr/icerik/6623/2019-331>, 28.09.2021; Aynı yönde karar için bkz. Kişisel Verileri Koruma Kurulu, 27.01.2020 tarihli ve 2020/67 sayılı karar, (çevrimiçi), <https://kvkk.gov.tr/icerik/6718/2020-67>, 28.09.2021.

⁶²⁷ Dülger, **Kişisel Veriler**, s. 405.

⁶²⁸ Kaya, **Hassas Veriler**, s. 327.

⁶²⁹ Aşıkoğlu, **Hukuka Uygunluk Sebepleri**, s. 1072; Aşıkoğlu, **Kişisel Veriler**, s. 124; Dülger, **Kişisel Veriler**, s. 405.

f. Bir Hakkın Tesisi, Kullanılması veya Korunması İçin Veri Aktarımının Zorunlu Olması

Kişisel verilerin aktarılmasını hukuka uygun hâle getiren bir diğer durum ise, bir hakkın tesisi, korunması veya kullanılması için veri aktarımının zorunlu olmasıdır (m.5/f.2/e). Hakkın hukuki bir talep olması, sözleşmeden veya kanun hükmünden doğması şartı aranmamaktadır⁶³⁰. Veri sorumlusunun hukuki yükümlülüğü ve kanunlarda açıkça öngörülme hukuka uygunluk sebeplerinden farklı olarak bu durumda tesis edilecek, korunacak veya kullanılacak hakkın, veri sorumlusu veya ilgili kişiye ait olmasına dair bir ayrıma gidilmemiştir⁶³¹. Bu yüzden herhangi bir kişinin hakkının tesisi, korunması veya kullanımı için zorunlu olduğu durumlarda, veri aktarımı gerçekleştirilebilecektir. Örnek olarak, kısıtlı bir kişinin haklarının korunması amacıyla vasiinin veya kayyımın, kısıtlının kişisel verilerini gereken yerlere aktarması gösterilebilir. Şunu da belirtmek gerekir ki bu kapsamda aktarılan verilerin ölçülü olması ve söz konusu işlem için zorunlu olması şarttır.

g. Veri Sorumlusunun Meşru Menfaatleri İçin Veri Aktarımının Zorunlu Olması

Kişisel verilerin aktarılmasına ilişkin son hukuka uygunluk sebebi ise, ilgili kişinin temel hak ve özgürlüklerine zarar vermemek kaydıyla, veri sorumlusunun meşru menfaatleri için zorunlu olması hâlinde kişisel verilerin aktarılmasıdır (m.5/f.2/f). GDPR’da hem veri sorumlusu hem de üçüncü kişilerin meşru menfaatinin kapsayan bu istisnanın kapsamı KVKK ile daraltılmış ve sadece veri sorumlusunun meşru menfaatine yer verilmiştir.

Meşru menfaat, geniş bir kavram olduğu için bu madde açısından dar yorumlanması gerekmektedir⁶³². Nitekim Kanun’da veri sorumlusunun meşru menfaati, ilgili kişinin temel hak ve özgürlükleri ile sınırlandırılmıştır⁶³³. Şöyle ki kişisel verilerin korunması hakkı olan ilgili kişi ve meşru menfaati olan veri sorumlusu arasındaki yarışta, ilgili kişinin temel hak ve özgürlüklerine zarar vermemek kaydıyla veri sorumlusunun meşru menfaatinin dikkate alınması kabul

⁶³⁰ Aşkoğlu, **Kişisel Veriler**, s. 125; Aşkoğlu, **Hukuka Uygunluk Sebepleri**, s. 1073.

⁶³¹ Aşkoğlu, **Kişisel Veriler**, s. 125; Aşkoğlu, **Hukuka Uygunluk Sebepleri**, s. 1073.

⁶³² Küzeci, s. 402; Taştan, s. 174.

⁶³³ Altındere, s. 47.

edilmiştir. Meşru menfaatin soyut amaçlardan ziyade somut bir kullanım veya aktarım amacına yönelik olması gerekmektedir⁶³⁴. Aynı zamanda söz konusu meşru menfaat etkin, belirli ve hâli hazırda mevcut olmalıdır⁶³⁵.

GDPR’da kullanılan “gereklilik” kavramının aksine Kanun’da “zorunluluk” kavramı tercih edilmiştir. Çekin’e göre Kanun’da kullanılan “zorunluluk” kıstası “gereklilik” kıstasından farklı anlaşılmamalıdır. Zira uygulama alanını sadece zorunluluk hâlleriyle sınırlandırmak hükmün amacına hizmet eder nitelikte olmayacaktır⁶³⁶. Dolayısıyla verilerin aktarılması, söz konusu meşru menfaat açısından gerekli olmalıdır. Başka bir deyişle veri aktarımı faaliyeti ile veri sorumlusunun meşru menfaati arasında sıkı bir ilişki mevcut olmalıdır⁶³⁷. Gereklilik ve ölçülülük ilkesi uyarınca da gerçekten veri sorumlusunun meşru menfaatinin gerçekleşmesi için verilerin aktarılmasının gerekli olup olmadığı değerlendirilmelidir⁶³⁸. Örneğin, birleşme ve devralma sırasında işverenin işçi verilerini devralan şirkete aktarmasında meşru menfaat bulunmaktadır. Fakat devralanın, hukuki ve mali açıdan gerekli incelemeyi yapması için bütün işçi verilerinin aktarılmasına gerek yoktur. İşçi verileri, işçinin adı ve soyadı kapatılarak devralana aktarıldığında da devralan, ilgili şirketin işgücü ile ilgili gerekli bilgiye sahip olacaktır. Bu bakımdan işçilerin ad ve soyadlarının devralan şirkete aktarılması, ölçülü bir veri işleme türü olarak kabul edilmeyecektir⁶³⁹.

Veri sorumlusunun meşru menfaatinin bulunması, veri aktarımını tek başına hukuka uygun hâle getirmez. Bunun için veri sorumlusunun meşru menfaati ile ilgili kişinin temel hak ve özgürlükleri arasında bir denge testi yapılması gerekmektedir⁶⁴⁰. Şöyle ki veri sorumlusunun menfaatinin, ilgili kişinin hak ve özgürlüklerinden üstün olduğu durumlarda veri aktarımı hukuka uygun kabul edilecektir.

Bununla ilgili Kurul, otomotiv sektöründe faaliyet gösteren veri sorumlusu tarafından reklam amaçlı gönderilen bir kısa mesaj hakkında ilgili kişinin şikâyeti

⁶³⁴ Çekin, **Kişisel Verilerin Korunması**, s. 96; Altındere, s. 47.

⁶³⁵ Dülger, **Kişisel Veriler**, s. 412; Özkan, s. 114; Develioğlu, s. 66.

⁶³⁶ Çekin, **Kişisel Verilerin Korunması**, s. 97.

⁶³⁷ Çekin, a.y.; Altındere, s. 47.

⁶³⁸ Aşıkoğlu, **Hukuka Uygunluk Sebepleri**, s. 1074.

⁶³⁹ Yücedağ, **Hukuka Uygunluk Sebepleri**, s. 785.

⁶⁴⁰ Yücedağ, **Hukuka Uygunluk Sebepleri**, s. 783; Altındere, s. 47.

üzerine başlattığı inceleme sonucunda, bu istisnaya dayanan veri sorumlusu hakkında, meşru menfaatin ne olduğunu açıklamadığından ve bu menfaat ile kişilerin temel hak ve özgürlükleri arasında bir denge testi uygulanıp uygulanmadığı ile ilgili de herhangi bir açıklama bulunmadığından dolayı kişisel verilerin aktarılması bakımından geçerli bir meşru menfaatin bulunmadığı kanaatine varmıştır⁶⁴¹.

2. Özel Nitelikli Kişisel Veriler Açısından

Yukarıda da belirtildiği üzere, özel nitelikli kişisel veriler, başkaları tarafından ele geçirildiği zaman ilgili kişi açısından daha fazla risk ve tehlike arz ettiği için bu tür verilerin aktarılması, daha sıkı şartlara tabi tutulmuştur⁶⁴².

KVKK m.8/f.2/b uyarınca, özel nitelikli kişisel verilerin açık rıza olmaksızın aktarılabilmesi için hem yeterli önlemlerin alınmış olması hem de KVKK m.6/f.3'te belirtilen şartlardan birinin mevcut olması gerekmektedir. Başka bir deyişle özel nitelikli kişisel verilerin yurt içinde açık rıza aranmaksızın aktarılabilmesi, bu tür verilerin genel olarak işlenmesi için aranan hukuka uygunluk şartlarına tabi kılınmıştır.

Özel nitelikli kişisel verilerin aktarılması açısından m.6/f.3 ile ikili ayrıma gidilmiştir. Şöyle ki, sağlık ve cinsel hayata ilişkin veriler ve bunların dışındaki verilerin açık rıza olmadan aktarılabilmesi için farklı şartlar belirlenmiştir.

Bu doğrultuda, aktarılacak kişisel verilerin hangi kategoriye; sağlık ve cinsel hayata dair veriler veya bunların dışında kalan verilere ait olduğunun tespit edilmesi önem arz etmektedir. Zira aktarılma faaliyetine uygulanacak düzenleme buna göre belirlenecektir. Örneğin, tıbbi teşhis-tedavi bilgileri, kullanılan ilaç veya protez bilgileri gibi bilgiler tereddütsüz bir şekilde sağlık verileri olarak kabul edilebildiği halde, bazı verilerin sağlık veya diğer kategoriye ait olması duruma göre değişebilecektir⁶⁴³. Bu bakımdan, kişisel veri kategorileri belirlenirken kullanım

⁶⁴¹ Kişisel Verileri Koruma Kurulu, 22.07.2020 tarihli ve 2020/559 sayılı karar.

⁶⁴² Altındere, s. 51.

⁶⁴³ Murat Volkan Dülger/ Yavuz Selim Dicle, “Kişisel Sağlık Verilerinin İşlenmesi Sorunu ve Covid 19 Üzerine Değerlendirme - “KVKK Hükümlerinin İş İlişkileri Kapsamında Değerlendirilmesi”ne Katkı”, s. 3, (çevrimiçi), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3792377, 22.10.2021.

amaçlarının dikkate alınması gerekmektedir⁶⁴⁴. Örneğin, alkol veya sigara kullanım bilgisi, sağlık durumu hakkında değerlendirme yapmak amacıyla aktarıldığı durumlarda “sağlık verisi” kapsamında değerlendirileceği halde, amacın sağlık durumu hakkında değerlendirme yapmak olmaması hâlinde ise bu kategoriye dâhil edilmeyecektir⁶⁴⁵. Veri aktarımlarının amacı dikkate alınmadan yapılan tespitler, yanlış sonuçlara neden olabilecektir. Örneğin, gözlüklü birinin fotoğrafının paylaşılması, onun sağlık verilerinin aktarılması sonucunu doğuracaktır⁶⁴⁶.

a. Sağlık ve Cinsel Hayat Dışındaki Kişisel Verilerin Aktarılması

Sağlık ve cinsel hayat dışındaki kişisel veriler; yani kişinin ırkı, etnik kökeni, siyasi düşüncesi, felsefi inancı, dini, mezhebi veya diğer inançları, kılık ve kıyafeti, dernek, vakıf veya sendika üyeliği, ceza mahkûmiyeti ve güvenlik tedbirleriyle ilgili verileri ile biyometrik ve genetik verilerinin, açık rıza aranmaksızın yurt içinde aktarılabilmesi için iki şartın mevcut olması gerekmektedir:

- 1) yeterli önlemlerin alınmış olması
- 2) kanunlarda öngörülen hâller

Kanunlarda öngörülme şartı, sağlık ve cinsel hayat dışındaki özel nitelikli kişisel verilerin yanı sıra, genel nitelikli kişisel verilerin de aktarılması için açık rızaya alternatif hukuka uygunluk sebebi olarak öngörüldüğünden dolayı, önceki bölümde genel nitelikli kişisel veriler açısından söylenenler ve örnekler bu bölüm için de geçerlidir.

Şunu da belirtmek gerekir ki genel nitelikli kişisel veriler açısından “kanunlarda açıkça öngörülme” şartı arandığı halde, özel nitelikli kişisel veriler için sadece “kanunlarda öngörülme” ifadesine yer verilmiştir. Hâlbuki özel nitelikli kişisel verilerin hassas doğası gereği, onların daha sıkı korunmaya tabi tutulması gerekirdi⁶⁴⁷. Kanaatimizce, kanun koyucu bu düzenlemede bilinçli olmaksızın bir

⁶⁴⁴ Dülger, **Kişisel Veriler**, s. 418-419; Bayındır, s. 36; Yücedağ, **Hukuka Uygunluk Sebepleri**, s. 770.

⁶⁴⁵ Dülger/ Dicle, s. 4.

⁶⁴⁶ Dülger/ Dicle, s. 5.

⁶⁴⁷ Küzeci, s. 350; Zor, s. 54; İmançlı, s. 139.

ifade hatasına düşmüştür⁶⁴⁸. Bu nedenle, özel nitelikli kişisel veriler açısından da kanunlarda “açıkça” öngörülme şartı aranması ve düzenlemenin dar yorumlanması gerektiği kanaatindeyiz⁶⁴⁹. Nitekim maddenin gerekçesinde de “kanunlarda açıkça öngörülme” şartı arandığı belirtilmiştir⁶⁵⁰.

b. Sağlık ve Cinsel Hayata İlişkin Kişisel Verilerin Aktarılması

Sağlık ve cinsel hayata dair kişisel verilerin açık rıza aranmaksızın aktarılması için KVKK m.6/f.3'te yer alan şartların sağlanması gerekmektedir. Nitekim Kurul bir kararında⁶⁵¹, sağlık verilerini KVKK m.6'da yer alan işleme şartlarından birine dayanmadan üçüncü bir kişiye aktaran veri sorumlusu eczane hakkında idari para cezası uygulanmasına karar vermiştir. Buna göre, sağlık verilerinin aktarılması için aynı anda üç şartın bulunması gerekecektir:

1) Amaca ilişkin şartlar - sağlık ve cinsel hayata ilişkin veriler; sadece kamu sağlığının korunması, koruyucu hekimlik, tıbbi teşhis, tedavi ve bakım hizmetlerinin yürütülmesi, sağlık hizmetleri ile finansmanının planlanması ve yönetimi gibi amaçlardan herhangi birinin varlığı hâlinde açık rıza olmadan aktarılabilir.

2) Veri işleyene ilişkin şartlar - bu tür veriler sadece sır saklama yükümlülüğü altında bulunan kişi veya yetkili kurum ve kuruluşlar tarafından aktarılabilir.

3) Yeterli önlemlerin alınmış olması - m.8/f.2/b ve m.6/f.4 uyarınca, Kurul tarafından belirlenen yeterli önlemlerin alınması zorunludur.

Kişisel sağlık verilerinin aktarılmasına dair düzenlemelere Kişisel Sağlık Verileri Hakkında Yönetmelik'de de yer verilmiştir. Yönetmeliğin 15'inci maddesi uyarınca, kişisel sağlık verilerinin aktarılması faaliyeti, KVKK'nın 8'inci ve 9'uncu maddelerine riayet edilerek gerçekleştirilir. Şayet kişisel sağlık verilerinin kamu kurum ve kuruluşlarına aktarılması söz konusu ise, buna dair protokol düzenlenerek kişisel veri koruma mevzuatının genel ilkeleri ile veri güvenliğine ilişkin hükümlere

⁶⁴⁸ Erarslan, **Özel Nitelikli Kişisel Veriler**, s. 217.

⁶⁴⁹ Aynı yönde görüşler için bkz.: Küzeci, s. 374; İmançlı, s. 118; Erarslan, **Özel Nitelikli Kişisel Veriler**, s. 217.

⁶⁵⁰ Bkz.: KVKK m.6 gerekçesi.

⁶⁵¹ Kişisel Verileri Koruma Kurulu, 05.12.2018 tarihli ve 2018/143 sayılı karar, (çevrimiçi), <https://www.kvkk.gov.tr/Icerik/5364/2018-143>, 25.11.2021.

ve protokol kapsamında hangi verilerin aktarılacağına yer verilir. Teknik altyapının uygun olduğu durumlarda verilerin aktarımı, KamuNET⁶⁵² üzerinden gerçekleştirilir (Yönetmelik m.15/f.2). Kişisel sağlık verilerinin aktarımı talepleri, talep edilen verilerin ilgili olduğu Bakanlık birimi tarafından değerlendirilir ve sonuca göre Genel Müdürlükçe işlem tesis edilir (Yönetmelik m.15/f.3).

(1) Kamu Sağlığının Korunması

Sağlık ve cinsel hayata ilişkin özel nitelikli kişisel veriler, kamu sağlığının korunması amacıyla ilgili kişinin açık rızası aranmaksızın aktarılabilir. Kamu sağlığı doktrinde “*toplumun, bireylerin, kamu ve özel toplulukların örgütlü çabaları ve bilinçli seçimleri yoluyla hastalığın önlenmesi, yaşam süresinin uzatılması ve sağlığı teşvik etme*” olarak tanımlanmıştır⁶⁵³. Kamu sağlığı, sadece bir kişinin değil, tüm nüfusun sağlığını korumayı amaçlayan bir kavramdır⁶⁵⁴. Kamu sağlığı kapsamında sadece bir hastalık veya yaralanmanın iyileştirilmesi değil, bunun yanı sıra eğitim politikaları geliştirilerek, araştırmalar yapılarak, hizmetler uygulanarak sağlık sorunlarının oluşması ve ortaya çıkmasının önüne geçmek hedeflenmektedir⁶⁵⁵.

Bu anlamada mevzuatta kamu sağlığını korumaya yönelik birçok düzenlemeye yer verilmiştir. Örneğin, 1593 sayılı Umumi Hıfzıssıhha Kanunu’nun⁶⁵⁶ 57’nci maddesi uyarınca, kanunda belirtilen bulaşıcı hastalıklardan herhangi birinin varlığı hâlinde yetkili makamların bilgilendirilmesi gerekmektedir. Yine Sıtmanın İmhası Hakkında Kanun’un⁶⁵⁷ 11’inci maddesi uyarınca, teşhis edilen her sıtma vakasının, kanunda öngörülen yetkili makamlara ihbarı mecburi olduğundan, sağlık çalışanları hastanın adı, soyadı, yaşı, açık adresi ve mücbir sebep

⁶⁵² Kişisel Sağlık Verileri Hakkında Yönetmelik m.4/f.1/ğ uyarınca, “KamuNET: Kamu kurum ve kuruluşları arasındaki veri iletişiminin sağlanması, bu veri iletişiminin internete kapalı, fiziksel ve siber saldırılara karşı daha güvenli sanal bir ağ üzerinden yapılması, siber güvenlik risklerinin minimize edilmesi, mevcut ve kurulacak olan güvenli kapalı devre çözümlere standart sağlanması, ortak uygulamalar için uygun alt yapının tesis edilmesi amaçlarıyla Ulaştırma ve Altyapı Bakanlığı tarafından geliştirilen projeyi ifade eder.”

⁶⁵³ Charles-Edward Amory Winslow, “The Untilled Fields of Public Health”, **Science**, C. 51, S. 1306, 1920, s. 30’dan aktaran Erarslan, **Özel Nitelikli Kişisel Veriler**, s. 206, 207; Bayındır, s. 61, 62.

⁶⁵⁴ Erarslan, **Özel Nitelikli Kişisel Veriler**, s. 206-207; Hakalmaz, s. 103.

⁶⁵⁵ Erarslan, **Özel Nitelikli Kişisel Veriler**, s. 207.

⁶⁵⁶ RG. T. 06.05.1930, S. 1489.

⁶⁵⁷ RG. T. 11.01.1960, S. 10402.

olmadıkça hastadan alınacak kalın damla veya yayma kanı yetkili makamlara aktaracaktır. Bu gibi durumlarda gerçekleştirilecek aktarımların amacı, kamu sağlığını korumak olduğundan aktarım, hukuka uygun kabul edilecektir. Örneğin, Covid-19 test sonucu pozitif çıkan kişinin bu hastalığı diğer insanlara da bulaştırma riski olduğu için kamu sağlığı söz konusu olacaktır. Bu nedenle kişinin karantinada olduğundan emin olmak ve diğer kişilerle temasını önlemek amacıyla, virüse yakalandığına dair sağlık verileri, testin yapıldığı hastane tarafından kişinin bireysel HES koduna işlenmek üzere Sağlık Bakanlığı'na aktarıldığında bu aktarılma hukuka uygun kabul edilecektir.

(2) Koruyucu Hekimlik

Sağlık ve cinsel hayata ilişkin özel nitelikli kişisel veriler, koruyucu hekimlik amacıyla ilgili kişinin açık rızası olmaksızın aktarılabilecektir. Koruyucu hekimlik, hastalığın seyrinin herhangi bir aşamasında ilerlemesini önleyen bütün tedbirleri içerir⁶⁵⁸. Başka bir deyişle, koruyucu hekimlik, *“...klinik hekimliğe ihtiyaç olacak evreye gelmeden, yani daha risk düzeyindeyken hastalıkların önlenmesini içerir”*⁶⁵⁹. Sağlık Hizmetlerinin Yürütülmesi Hakkında Sağlık Bakanlığı Yönergesi'nin 4'üncü maddesine göre, *“koruyucu sağlık hizmetleri, kişileri hastalanmaktan, yaralanmaktan, sakat kalmaktan ve erken ölümden korumak amacıyla verilen sağlık hizmetleridir”*. Örneğin, Türk Kızılayı'nda çalışan bir doktor ekibi, afet bölgesinde “çocuk felci” hastalığının ortaya çıktığını öğrenmeleri üzerine, bölgedeki kişilere tıbbi geçmişlerine dair sorular sorması, cevapları kayıt altına alıp ilgili sağlık kurumuna aktarması, hukuka uygun bir kişisel veri aktarımı olarak kabul edilecektir⁶⁶⁰.

Koruyucu hekimlik, bir hastalığın ortaya çıkmasını engellemek için tedbirlerin alındığı “birincil koruma”, hastalıktan sonraki aşamada hastalığın veya komplikasyonlarının durdurulduğu veya önlendiği “ikincil koruma” ve yaşam

⁶⁵⁸ E.A. Clarke, “What is Preventive Medicine?”, **Official Publication of the College of Family Physicians of Canada**, C. 20, s. 11, 1974, s. 65'den aktaran Bayındır, s. 63.

⁶⁵⁹ Nuri Mehmet Basan/ Nazmi Bilir, “Koruyucu Sağlık Hizmetlerinde Önleme Çelişkisi ve Nedenleri”, **TAF Preventive Medicine Bulletin**, C. 15, S. 1, 2016, s. 44-50.

⁶⁶⁰ Erarslan, **Özel Nitelikli Kişisel Veriler**, s. 210.

kalitesinin artırılması için tedbirlerin alındığı “tersiyer koruma” olmakla üçlü bir ayrıma tabidir⁶⁶¹.

3359 sayılı Sağlık Hizmetleri Temel Kanunu’nda⁶⁶² koruyucu hekimliğe ilişkin düzenlemelere yer verilmiştir. Örneğin, kanunun m.3/j uyarınca, “*vatandaşların hastalıklardan korunma, sağlıklı çevre, beslenme, ana çocuk sağlığı ve aile planlaması ve benzeri konularda eğitilmeleri ve takipleri bütün kamu kuruluşlarının sorumluluğu, kamu kurumu niteliğindeki meslek kuruluşları, özel ve gönüllü kuruluşların işbirliği içerisinde gerçekleştirilecektir.*” Aynı kanunun m.3/f/1 hükmü gereğince, “*engelli çocuk doğumlarının önlenmesi için, gebelik öncesi ve gebelik döneminde tıbbi ve eğitsel çalışmalar yapılacak, yeni doğan bebeklerin metabolizma hastalıkları için gerekli olan testlerden geçirilerek risk taşıyanların belirlenmesine ilişkin tedbirler alınacaktır.*”

(3) Tıbbi Teşhis, Tedavi ve Bakım Hizmetlerinin Yürütülmesi

Tıbbi teşhis, tedavi ve bakım hizmetlerinin yürütülmesi amaçlarıyla sağlık ve cinsel hayata ilişkin özel nitelikli kişisel veriler ilgili kişinin açık rızası aranmaksızın aktarılabilecektir. Tıbbi teşhis, kişide var olduğu sanılan fiziksel veya psikolojik bir rahatsızlığı, hastalığı anlamak ve belirlemek maksadıyla tıp bilimine uygun olarak yapılan bütün faaliyetleri ifade eder⁶⁶³. Başka bir deyişle tıbbi teşhis, kişide gözlemlenen belirtilerin hangi hastalık veya durumu ifade ettiğini belirleme sürecidir⁶⁶⁴.

Tıbbi tedavi, hastalıkları ve sakatlıkları iyileştirme, hafifletme ve ortadan kaldırma amacıyla yapılan işlemleri ihtiva eden bir süreçtir⁶⁶⁵. Tıbbi bakım hizmetleri ise, sağlık personeli tarafından, sağlığın korunması, hastalığın önlenmesi,

⁶⁶¹ Erarslan, **Özel Nitelikli Kişisel Veriler**, s. 209; Bayındır, s. 63; Hakalmaz, s. 105.

⁶⁶² RG. T. 15.05.1987, S. 19461.

⁶⁶³ Polat Tunçer, **Sağlık Hukuku Temel Bilgileri**, 2. bs, Ankara, Adalet, 2017, s. 50.

⁶⁶⁴ Hakan Hakeri, **Tıp Hukuku**, 19. bs., Ankara, Seçkin, 2020, s. 783; Dülger, s. 430; Erarslan, **Özel Nitelikli Kişisel Veriler**, s. 211; Hayrunnisa Özdemir, “Teşhis ve Tedavi Sözleşmesinde Kayda Geçirme ve Sır Saklama Yükümlülüğü”, **Ankara Barosu Sağlık Hukuku Digestası**, C. 1, S. 1, 2009, s. 37; İmançlı, s. 148; Hakalmaz, s. 107.

⁶⁶⁵ Polat Tunçer, s. 50; Özdemir, **Teşhis ve Tedavi**, s. 38; Selvi Özçetin/ Murat Balaban, **Sağlık hukuku**, 2. bs., Ankara, Seçkin, 2015, s. 14; Erarslan, **Özel Nitelikli Kişisel Veriler**, s. 212; Hakalmaz, s. 108.

hastalık veya yaralanmanın tedavisi ile hizmetlerin sağlanmasını ifade eder⁶⁶⁶. Tıbbi bakım hizmetlerine; sağlık durumunun değerlendirilmesi, sağlıklı olma durumunun hastalık durumundan ayrılması, hastalıklarla başa çıkmak için bakım yardımı, hastalığın iyileştirilmesi, hastalığın önlenmesi örnek olarak gösterilebilir⁶⁶⁷. Ayrıca, bakım hizmetlerinin de tıbbi tedavi hizmetleri kapsamında değerlendirilmesi mümkündür⁶⁶⁸.

(4) Sağlık Hizmetleri ile Finansmanın Planlanması ve Yönetimi

Sağlık ve cinsel hayata ilişkin özel nitelikli kişisel veriler, sağlık hizmetleri ve finansmanın planlanması ve yönetimi amaçlarıyla ilgili kişinin açık rızası olmadan aktarılabilecektir. Sağlık Hizmetlerinin Yürütülmesi Hakkında Sağlık Bakanlığı Yönergesi m.4/b uyarınca, sağlık hizmetleri “*insan sağlığına zarar veren çeşitli etmenlerin yok edilmesi ve toplumun bu etmenlerin etkilerinden korunması, hastaların tedavi edilmesi, bedensel ve ruhsal yetenek ve becerileri azalmış olanların rehabilite edilmesi için yapılan hizmetler*” olarak tanımlanmıştır. Başka bir deyişle, sağlık hizmetleri, hastalığın öncesinden başlangıcına, başlangıcından sonuna ve sona erdikten sonraki döneme ait yapılan faaliyetlerin tümünü kapsayan her türlü hizmeti ifade etmektedir⁶⁶⁹. Bu hizmetlerin planlanması ve yönetimi amacıyla gerçekleştirilen aktarımlar, hukuka uygun kabul edilecektir.

Sağlık finansmanı ise, genel olarak “*sağlık hizmet sunucuları ile finanse edenler arasında kaynak aktarımı süreci ve sistemi*” olarak tanımlanmaktadır⁶⁷⁰. Sağlık finansmanı, Dünya Sağlık Örgütü tarafından bireysel veya toplu bir şekilde insanların sağlık ihtiyaçlarının karşılanması için bir sağlık sisteminde paranın hareketi, biriktirilmesi ve tahsisi ile ilgili olan hizmetleri ihtiva etmektedir⁶⁷¹. Sağlık

⁶⁶⁶ Erarslan, **Özel Nitelikli Kişisel Veriler**, s. 212, 213.

⁶⁶⁷ Alfred W. Childs, “The Functions of Medical Care”, **Public Health Reports**, C. 90, S. 1, 1975, s. 10’dan aktaran Erarslan, **Özel Nitelikli Kişisel Veriler**, s. 212.

⁶⁶⁸ İmançlı, s. 148; Hakalmaz, s. 108.

⁶⁶⁹ Küzeci, s. 474-475; Erarslan, **Özel Nitelikli Kişisel Veriler**, s. 214; İmançlı, s. 150; Hakalmaz, s. 109.

⁶⁷⁰ Ali Güvercin/ Halil İbrahim Mil/ Bülent Tarım, “Sağlık Hizmetlerinin Finansmanı ve Sosyal Güvenlik Kurumu (SGK)”, **Bartın Üniversitesi İktisadi ve İdari Bilimler Fakültesi Dergisi**, C. 7, S. 13, 2016, s. 82; İmançlı, s. 150; Hakalmaz, s. 114-115.

⁶⁷¹ World Health Organization, “Health Systems Financing”, Haziran 2008, s. 2, (çevrimiçi), https://www.who.int/healthinfo/statistics/toolkit_hss/EN_PDF_Toolkit_HSS_Financing.pdf, 25.10.2021.

hizmetleri ve finansmanının planlanması ise, gelecekteki sağlık ihtiyaçlarını belirleme, bu ihtiyaçları karşılama yollarını tespit etmek ve bu tespitleri mevcut kaynaklarla karşılaştırarak çeşitli önerilerde bulunma sürecini ifade eder⁶⁷². Bu planlama ve yöntemlerin öngörülmesi ile bireylerin sağlık hizmetlerine erişimi kolaylaşmakla birlikte, sunulan hizmetlerin kalitesi de artmaktadır⁶⁷³. Bu amaçlar doğrultusunda gerçekleştirilen veri aktarımları KVKK m.6/f.3 kapsamında değerlendirilir. Sağlık hizmetlerinin yerine getirilmesi için doğrudan gerekli olmayan tıbbi araştırma, hastalık sigortası masraflarının iadesi veya parasal hakların takibi gibi sonraki işlemler, bu hükmün kapsamına dâhil değildir.

(5) Sır Saklama Yükümlülüğü Altında Bulunan Kişi veya Yetkili Kurum ve Kuruluşlar

Sağlık ve cinsel hayata ilişkin kişisel verilerin açık rıza aranmaksızın yukarıdaki amaçlar doğrultusunda aktarılabilmesi için aranan diğer şart, bu verilerin sır saklama yükümlülüğü altında bulunan kişiler veya yetkili kurum veya kuruluşlar tarafından aktarılmasıdır. Burada kastedilen, taraflar arasında akdedilen herhangi bir özel hukuk sözleşmesinde taraflarca belirlenen sır saklama yükümlülüğü değil, kişinin icra ettiği meslek sebebiyle kanunen sahip olduğu sır saklama yükümlülüğüdür⁶⁷⁴. Bu bakımdan sır saklama yükümlülüğünün ve kimlerin bu yükümlülük altında bulunduğunun belirlenmesi gerekmektedir.

Mevzuatta çeşitli mesleklere ve kuruluşlara sözleşmeyle, kanunla veya diğer düzenlemelerle vâkıf olduğu sırların korunması hususunda bir yükümlülük getirilmiştir. Bu yükümlülüğe sır saklama yükümlülüğü adı verilmektedir⁶⁷⁵. Sır saklama yükümlülüğü, bir kişinin üçüncü kişilerle paylaşmak istemediği bilgilerine hukuki ilişki çerçevesinde erişen kişilere, öğrendikleri bu bilgileri sır sahibinin rızası olmadan başkalarıyla paylaşmama ödevi getiren bir yükümlülüktür⁶⁷⁶.

KVKK'da sır saklama yükümlülüğü, veri sorumlusu ve veri işleyenin veri güvenliğine ilişkin yükümlülüklerinden biri olarak düzenlenmiştir. Buna göre, “Veri

⁶⁷² İmançlı, s. 150,151, Bayındır, s. 66.

⁶⁷³ Hakalmaz, s. 115.

⁶⁷⁴ Hakalmaz, s. 100.

⁶⁷⁵ Erarslan, **Özel Nitelikli Kişisel Veriler**, s. 191.

⁶⁷⁶ Özdemir, **Teşhis ve Tedavi**, s. 154; Hakalmaz, s. 41.

sorumluları ile veri işleyen kişiler, öğrendikleri kişisel verileri bu Kanun hükümlerine aykırı olarak başkasına açıklayamaz ve işleme amacı dışında kullanamazlar. Bu yükümlülük görevden ayrılmalarından sonra da devam eder” (m.12/f.4).

Sağlık ve cinsel hayata ilişkin verilerin aktarılması bağlamında kimlerin sır saklama yükümlülüğü altında bulunan kişiler olduğu kanunda açıkça sayılmamıştır. Bu maddenin iptali için Anayasa Mahkemesi’ne yapılan bir başvuruda mahkeme, bu kişilerin “... avukat, hekim veya mali müşavir gibi kendi kanunlarında görevleri dolayısıyla edindikleri bilgileri zamanla sınırlı olmaksızın açığa vurmaları yasak olan ve bu yasağın ihlali hâlinde hukuki ve cezai sorumluluğu olan kişilerdir.”⁶⁷⁷

Anayasa Mahkemesi’nin bu kararından anlaşılabileceği üzere, madde hükmünde ayrı ayrı düzenlemelerde sır saklama yükümlülüğü öngörölmüş kişilerden bahsedilmektedir. Bu bağlamda, akla gelebilecek ilk örnek hiç şüphesiz sağlık personeldir. Hekimin sır saklama yükümlülüğü, yasal mevzuatta birkaç düzenlemede öngörölmüştür. Şöyle ki Tıbbi Deontoloji Nizamnamesi’nin 4’üncü maddesine göre, “tabip ve dış tabibi, meslek ve sanatının icrası vesilesiyle muttali olduğu sırları, kanuni mecburiyet olmadıkça, ifşa edemez.” Bu anlamda hekim, dış hekimi, psikiyatrist, aile hekimi, sosyal hekim, bilirkişi hekimi, cezaevi hekimi, işyeri hekimi vb. “hekimlik” sıfatını haiz kişilerin tamamı sır saklama yükümlülüğü altındadır⁶⁷⁸. Aynı zamanda hekime faaliyetinde yardımcı olan yardımcı personel ve öğrenimi sırasında sırda vakıf olan tıp öğrencileri de sır saklama yükümlülüğü altındadır⁶⁷⁹.

Ayrıca Hasta Hakları Yönetmeliği⁶⁸⁰ m.20 uyarınca, “ilgili mevzuat hükümleri ve/veya yetkili mercilerce alınacak tedbirlerin gerektirdiği hâller dışında hasta, sağlık durumu hakkında kendisinin, yakınlarının ya da hiç kimsenin bilgilendirilmemesini isteyebilecek, hasta bu talebini istediği zaman değiştirebilecek ve bilgi verilmesini isteyebilecektir.” Türk Tabipler Birliği Hekimlik Meslek Etiği

⁶⁷⁷ AYM kararı, E. 2016/125, K. 2017/143, T. 28.09.2017 (çevrimiçi), <https://normkararlarbilgibankasi.anayasa.gov.tr/Dosyalar/Kararlar/KararPDF/2017-143-nrm.pdf>, 11.10.2021.

⁶⁷⁸ Hakeri, s. 366; Yusuf Büyükay, “Hekimin Sır Saklama Yükümlülüğü”, **Atatürk Üniversitesi Erzincan Hukuk Fakültesi Dergisi**, C. 8, S. 1-2, 2004, s. 384.

⁶⁷⁹ İmançlı, s. 152; Bayındır, s. 69; Hakalmaz, s. 100-101.

⁶⁸⁰ RG. T. 01.08.1998, S. 23420.

Kurallarının 9’uncu maddesine göre hekimin, mesleğini uygularken hastasından öğrendiği sırları açıklaması yasaktır. Hasta ile arasındaki ilişkinin ölüm veya başka herhangi bir nedenle sona ermesi, hekimin sır saklama yükümlülüğünü ortadan kaldırmaz.

Türk Eczacıları Deontoloji Tüzüğü⁶⁸¹ m.4 uyarınca, “*Eczacı, meslek ve sanatının icrası sırasında öğrendiği sırları, kanuni zorunluluk olmadıkça, ifşa edemez*”. Bu anlamda eczacıların da sır saklama yükümlülüğü altında bulunduğu ve KVKK m.6/f.3’te öngörülen amaçlar doğrultusunda özel nitelikli kişisel verileri aktarabilecekleri söylenebilir⁶⁸².

Avukatların sır saklama yükümlülüğüne dair düzenlemeye Avukatlık Kanunu’nun⁶⁸³ 36’ncı maddesinde yer verilmiştir. İlgili hükme göre, “*avukatların, kendilerine tevdi edilen veya gerek avukatlık görevi, gerekse Türkiye Barolar Birliği ve barolar organlarındaki görevleri dolayısıyla öğrendikleri hususları açığa vurmaları yasaktır.*” Aynı zamanda Avrupa Konseyi tarafından ihdas edilen Avukatlık Mesleğinin İcrasındaki Özgürlükler Hakkındaki 9 Numaralı Tavsiye Kararı’nda da avukatın sır saklama yükümlülüğü düzenlenmiştir. Kararın 38’inci maddesi uyarınca, “*tüm avukatların müvekkillerinin işleriyle ilgili sır saklama ödevi vardır. Bu ödev ADHS tarafından garanti altına alınan savunma haklarından biridir.*”

Avukatın saklamakla yükümlü olduğu sırlar, avukatlık mesleği dolayısıyla elde edilen sırlardır⁶⁸⁴. Aynı zamanda bu yükümlülük, avukatın stajyerlerine, yardımcılara, asistanlarına da sirayet etmektedir⁶⁸⁵.

Sır saklama yükümlülüğü altında bulunan kişilere bir diğer örnek işverenlerdir. 4857 sayılı İş Kanunu⁶⁸⁶ m.75/f.1 uyarınca işverenin, işçilerin özlük dosyalarını düzenleme yükümlülüğü, hükmün ikinci fıkrasında ise “*işveren, işçi*

⁶⁸¹ RG. T. 27.07.1968, S. 12961.

⁶⁸² İmançlı, s. 153.

⁶⁸³ RG. T. 07.04.1969, S. 13168.

⁶⁸⁴ Özcan Günergök, “Avukatın Sır Saklama Yükümlülüğü”, **Erzincan Üniversitesi Hukuk Fakültesi Dergisi**, C. 7, S. 1-2, 2003, s. 657; Erarslan, **Özel Nitelikli Kişisel Veriler**, s. 197.

⁶⁸⁵ Erarslan, **Özel Nitelikli Kişisel Veriler**, s. 198.

⁶⁸⁶ RG. T. 10.06.2003, S. 25134.

hakkında edindiği bilgileri dürüstlük kuralları ve hukuka uygun olarak kullanmak ve gizli kalmasında işçinin haklı çıkarı bulunan bilgileri açıklamamakla yükümlüdür” denilmek suretiyle sır saklama yükümlülüğü düzenlenmiştir. Aynı zamanda 6331 sayılı İş Sağlığı ve Güvenliği Kanunu⁶⁸⁷ m.15 uyarınca, işverenin, sağlık muayenesi yaptırılan işçilerin sağlık bilgilerini gizli tutması gerekmektedir.

Yine 3568 sayılı Serbest Muhasebeci Mali Müşavirlik ve Yeminli Mali Müşavirlik Kanunu’nun 43’üncü maddesi uyarınca, serbest muhasebeciler, mali ve yeminli müşavirler ile bu meslek mensuplarının yanlarında çalışan kişilerin, 1512 sayılı Noterlik Kanunu’nun 54’üncü maddesi uyarınca, noter ve noterlik katiplerinin, 5684 sayılı Sigortacılık Kanunu’nun 31/A maddesi uyarınca, sigorta şirketlerinin sır saklama yükümlülüğü hükme bağlanmıştır.

Kanun tarafından yetkili kılınmış kurum ve kuruluşlar da açık rızaya dayanmaksızın kanunda belirtilen amaçlar doğrultusunda sağlık ve cinsel hayata ilişkin verileri aktarma yetkisini haizdir. Söz konusu kurum ve kuruluşlar, hem kamu hem de özel hukuk tüzel kişileri olabilecektir⁶⁸⁸. Maddenin gerekçesinde yetkili kurum ve kuruluşlar olarak Sağlık Bakanlığı, her türlü sağlık kurum ve kuruluşu ve SGK gösterilmiştir⁶⁸⁹. Gerekçede bahsedilen her türlü sağlık kurum ve kuruluşlarına kamu veya özel hastanelerin, eczanelerin, sağlıkla ilgili okul veya üniversitelerin dâhil olduğu söylenebilir⁶⁹⁰.

Bu hüküm kapsamında sır saklama yükümlülüğünün yetkili kurum ve kuruluşlar için de aranıp aranmayacağı sorusu ortaya çıkmaktadır. Bizim de katıldığımız görüşe göre⁶⁹¹, yetkili kurum ve kuruluşlar açısından sır saklama yükümlülüğü aranmamalıdır. Zira hükmün lafzına bakıldığında, “sır saklama yükümlülüğü altında bulunan kişiler” ibaresi ile “yetkili kurum ve kuruluşlar” ibaresi arasında “veya” kullanılmıştır. Ayrıca “sır saklama yükümlülüğü altında bulunan kişiler” ifadesinin gerçek kişilerle birlikte kamu ve özel hukuk tüzel kişilerini de

⁶⁸⁷ RG. T. 30.06.2012, S. 28339.

⁶⁸⁸ İmançlı, s. 158.

⁶⁸⁹ Bkz.: KVKK m.6 gerekçesi.

⁶⁹⁰ Dülger, **Kişisel Veriler**, s. 425; Erarslan, **Özel Nitelikli Kişisel Veriler**, s. 162; İmançlı, s. 159;

⁶⁹¹ İmançlı, s. 159; Hakalmaz, s. 102. Karşı görüş için bkz.: Bayındır, s. 70.

kapsadığı anlaşılmalıdır. Bu nedenle “yetkili kurum ve kuruluşlar”, “sır saklama yükümlülüğü altında bulunan kişiler” ifadesinden bağımsız yorumlanmalıdır⁶⁹².

c. Özel Nitelikli Kişisel Verilerin Aktarılması Zamanı Alınması Gereken Yeterli Önlemler

KVKK m.8/f.2/b uyarınca, özel nitelikli kişisel verilerin ilgili kişinin açık rızası aranmaksızın aktarılabilmesi için Kurul tarafından belirlenen yeterli önlemlerin, veri sorumlusu tarafından alınmış olması gerekmektedir. Özel nitelikli kişisel verilerin hassas niteliği, aktarıldığı takdirde ortaya çıkabilecek riskin boyutu göz önünde bulundurulduğu zaman bu verilerin aktarılması için birtakım önlemlerin alınması zorunluluğu isabetli olmuştur. Yeterli önlemlerin alınması, kişisel verilerin işlenmesine dair “veri güvenliği” ilkesinin bir uzantısıdır⁶⁹³. Nitekim KVKK m.12 uyarınca, *“veri sorumlusu; kişisel verilerin hukuka aykırı olarak işlenmesini önlemek, kişisel verilere hukuka aykırı olarak erişilmesini önlemek, kişisel verilerin muhafazasını sağlamak amacıyla uygun güvenlik düzeyini temin etmeye yönelik gerekli her türlü teknik ve idari tedbirleri almak zorundadır.”*

Bu düzenlemede yeterli önlemlerin alınması, her ne kadar sadece açık rızanın aranmadığı aktarma faaliyeti için öngörülmüş olsa da, kanaatimizce açık rızaya dayalı özel nitelikli kişisel veri aktarımlarında da bu şarta riayet edilmesi gerekmektedir. Zira KVKK m.6/f.4’te herhangi bir ayrıma gidilmeksizin özel nitelikli kişisel verilerin işlendiği bütün durumlarda Kurul tarafından belirlenen yeterli önlemlerin alınması şartı hükme bağlanmıştır. Bundan dolayı yeterli önlemlerin alınması, özel nitelikli kişisel verilerin aktarıldığı bütün durumlar için aranan ortak şart olarak kabul edilmelidir.

Özel nitelikli kişisel verilerin işlenmesi için veri sorumlusu tarafından alınması gereken yeterli önlemler, Kurul tarafından alınan 31.01.2018 tarihli ve 2018/10 sayılı karar⁶⁹⁴ ile belirlenmiştir. Kararın 5’inci maddesinde özel nitelikli

⁶⁹² İmançlı, s. 159, dn. 295.

⁶⁹³ Erarslan, **Özel Nitelikli Kişisel Veriler**, s. 160.

⁶⁹⁴ Bkz.: Kişisel Verileri Koruma Kurulu, “Özel Nitelikli Kişisel Verilerin İşlenmesinde Veri Sorumlularınca Alınması Gereken Yeterli Önlemler” ile ilgili 31.01.2018 tarihli ve 2018/10 sayılı Karar, (çevrimiçi), <https://kvkk.gov.tr/Icerik/4110/2018-10>, 26.06.2021.

kişisel verilerin aktarılacağı durumlarda alınması gereken önlemlere yer verilmiştir. Buna göre:

1) Verilerin e-posta ile aktarılması gerekiyorsa şifreli olarak kurumsal e-posta adresi veya Kayıtlı Elektronik Posta (KEP) hesabı kullanılarak aktarılması gerekir. Kurumsal e-posta, bir şirket veya işletmenin adını veya markasını içeren “@şirketadı.com” şeklinde kullanılan e-posta hesaplarıdır. Ücretsiz e-posta hizmetlerinden farklı olarak kurumsal e-posta daha güvenlidir. Çünkü ücretsiz servisler vasıtasıyla herkes dilediği öntakıyı dilediği kadar oluştursa da, kurumsal e-posta kişiye özeldir.

"Veri Sorumluları Sicili Hakkında Yönetmelik⁶⁹⁵ m.4/f.1/g uyarınca, KEP adresi: “Elektronik iletilerin, gönderimi ve teslimatı da dâhil olmak üzere kullanımına ilişkin olarak hukuki delil sağlayan, elektronik postanın nitelikli hâlini ifade eder.” Aynı tanıma, Kayıtlı Elektronik Posta Sistemine İlişkin Usul ve Esaslar Hakkında Yönetmelik⁶⁹⁶ m.4/f.1/i’de de yer verilmiştir. Aynı yönetmelik gereği, “KEP delili, belirli bir işlemin belirli bir zamanda meydana geldiğini gösteren, KEP sisteminde üretilen ve KEP Hizmet Sağlayıcısının işlem sertifikası ile imzalanmış veriyi; KEP sistemi ise, elektronik iletişim platformları aracılığıyla gerçekleşen, gönderildi ve alındı onayları da dâhil olmak üzere KEP iletilerinin tüm süreçlerine ilişkin olarak KEP delili oluşturulması, güvenli bir şekilde kimlik tespiti yapılması, KEP hesabı, KEP rehberi ve arşiv hizmetleri verilmesi gibi işlemlere sahip sistemi, ifade eder.”

Anlaşıldığı üzere KEP sisteminde gönderici ve alıcının kimlikleri belli olduğu için yasal koruma ve güvence sağlanmaktadır. Standart e-postadan farklı olarak gönderi zamanının, e-posta içeriğinin değiştirilmesi mümkün değildir.

2) Verilerin taşınabilir bellek, CD, DVD gibi ortamlar yoluyla aktarılması gerekiyorsa kriptografik yöntemlerle şifrelenmesi ve kriptografik anahtarın farklı ortamlarda tutulması gerekmektedir. Kriptografi, “bilgileri gizli tutan kodları oluşturma ve anlama pratiği” ve “bilginin, bilgisayar ağlarında güvende tutulması

⁶⁹⁵ RG. T. 30.12.2017, S. 30286.

⁶⁹⁶ RG. T. 25.08.2011, S. 28036.

*için özel kodların kullanılması” olarak tanımlanmaktadır*⁶⁹⁷. Başka bir deyişle kriptografi, okunabilir durumdaki bir verinin içerdiği bilginin, istenmeyen kişiler tarafından anlaşılmayacak bir hâle dönüştürülmesi için kullanılan yöntemlerdir.

Kriptografik yöntemler şifreleme veya şifre çözme işlemlerinde kullanılan matematiksel fonksiyonlardır. Kriptografik algoritma, düz metni şifrelemek için kullanılan anahtarla (bu bir sözcük, sayı, ifade vs. olabilir) birlikte çalışır. Şifreli verilerin güvenliği, anahtarın gizliliğine bağlı olduğundan, kriptografik anahtar sadece yetkili kişilerin erişebileceği ortamda saklanmalı ve yetkisiz erişim önlenmelidir⁶⁹⁸.

Kararda herhangi bir kriptografik yöntemden bahsedilmemiş ve bu husus veri sorumlusunun takdir yetkisine bırakılmıştır⁶⁹⁹. Yine Kurul tarafından kabul edilen Kişisel Veri Güvenliği Rehberi’nde “... *hangi şifreleme yöntemleri kullanılırsa kullanılsın kişisel verilerin tam olarak korunduğundan emin olunmalı ve bu amaçla uluslararası kabul gören şifreleme programlarının kullanımı tercih edilmelidir*” denilmek suretiyle veri sorumlusunun bu husustaki takdir yetkisinin sınırı belirlenmiştir⁷⁰⁰.

Kriptografik yöntemlerle şifrelenmiş özel nitelikli kişisel verilere istenmeyen kişiler tarafından erişilemediği gibi, verileri işlenen kişilerin siber saldırılara uğraması, saldırganların kimliklerinin gizlenmesi veya değiştirilmesinin önüne geçilebilir⁷⁰¹.

3) *Farklı fiziksel ortamlardaki sunucular arasında gerçekleştirilen özel nitelikli kişisel veri aktarımlarının, sunucular arasında VPN (Virtual Private Network) kurularak veya sFTP yöntemiyle gerçekleştirilmesi gerekir.* VPN veya sanal özel ağ (*virtual private network*), internete güvenli bağlantı sağlayan bir yöntemdir. Şöyle ki, VPN hizmeti, bağlantıyı bir sunucu üzerinden yönlendirerek ve

⁶⁹⁷ Erarşlan, **Özel Nitelikli Kişisel Veriler**, s. 171.

⁶⁹⁸ Kişisel Verileri Koruma Kurumu, Kişisel Veri Güvenliği Rehberi (Teknik ve İdari Tedbirler), Ankara, KVKK Yayınları, 2019, s. 21, (çevrimiçi), https://www.kvkk.gov.tr/yayinlar/veri_guvenligi_rehberi.pdf, 06.10.2021.

⁶⁹⁹ Dülger, **Kişisel Veriler**, s. 544.

⁷⁰⁰ Kişisel Verileri Koruma Kurumu, **Veri Güvenliği Rehberi**, s. 21.

⁷⁰¹ Erarşlan, **Özel Nitelikli Kişisel Veriler**, s. 132.

çevrimiçi işlemleri gizleyerek internete güvenli bir şekilde erişim imkânı sunar. VPN kullanıldığı zaman kullanıcının verileri şifrelenir ve bu veriler internet servis sağlayıcısına, daha sonra ise VPN sunucusuna şifreli olarak iletilir⁷⁰². VPN sunucusu, kullanıcı adına internete bağlanan üçüncü taraftır. Yani VPN kullanıldığında erişilmek istenen site, internet trafiğinin kaynağı olarak kullanıcıyı değil, VPN sunucusunu görmektedir. Bu nedenle erişilmek istenen site tarafından ne kullanıcının verilerine ne de bilgisayarındaki verilere ulaşılmaktadır⁷⁰³. Veri akışı görünse bile, şifrelendiği için bu akışın içeriğini görmek mümkün değildir⁷⁰⁴. Bu işlevlerinden dolayı, özel nitelikli kişisel verilerin aktarılması zamanı VPN kullanımı, verilerin gizliliğinin ve yetkisiz erişimlerin engellenmesinin sağlanması bakımından iyi bir güvenlik önlemidir⁷⁰⁵.

FTP veya dosya aktarım protokolü (*file transfer protocol*), bilgisayar dosyalarının sunucu ve alıcı arasında aktarımı için kullanılan standart ağ protokolünü ifade ederken, sFTP veya güvenli dosya aktarım protokolü (*secure file transfer protocol*) ise, FTP'nin güvenli bir sürümünü ifade etmektedir⁷⁰⁶. Başka bir deyişle sFTP dosya aktarımı yapılırken kullanılan FTP yönteminin şifrelenmiş hâlidir⁷⁰⁷.

4) *Verilerin kâğıt ortamı yoluyla aktarılması gerekiyorsa evrakın çalınması, kaybolması ya da yetkisiz kişiler tarafından görülmesi gibi risklere karşı gerekli önlemlerin alınması ve evrakın “gizlilik dereceli belgeler” formatında gönderilmesi gerekir. “Gizlilik derecesi” kavramı ve özel nitelikli kişisel verilerin hangi gizlilik derecesine dâhil olduğu, “Bilgi Varlıklarının Gizlilik Derecelerinin Sınıflandırılması”⁷⁰⁸ ile düzenlenmektedir. Buna göre, “gizlilik derecesi: Bilmesi gereken kişiler dışındakilere açıklanmasının veya verilmesinin millî güvenlik veya kişisel güvenlik açısından sakıncalı görülen bilgi varlığının, ülke menfaatine, gerçek ve tüzel kişiler ile kamu kurum/kuruluşlarına zarar vermesini önlemek amacıyla*

⁷⁰² Dülger, **Kişisel Veriler**, s. 536; Mehmet Bedii Kaya, a.y; Hakalmaz, s. 131, dn. 531.

⁷⁰³ Erarslan, **Özel Nitelikli Kişisel Veriler**, s. 181.

⁷⁰⁴ Dülger, **Kişisel Veriler**, s. 546.

⁷⁰⁵ Erarslan, **Özel Nitelikli Kişisel Veriler**, s. 181.

⁷⁰⁶ Bkz.: (çevrimiçi) <https://www.techopedia.com/definition/1879/secure-file-transfer-protocol-sftp>, 23.11.2021.

⁷⁰⁷ Dülger, **Kişisel Veriler**, s. 546.

⁷⁰⁸ Bkz.: Ulaştırma ve Altyapı Bakanlığı Teknik Çalışma Grubu, (çevrimiçi) <https://hgm.uab.gov.tr/uploads/pages/siber-guvenlik/siberbilgi.pdf>, 12.09.2021.

önem derecesine göre sınıflandırılması ve adlandırılması” olarak tanımlanmıştır. Söz konusu düzenleme bilgi varlıklar, gizlilik derecelerine göre sekiz başlık (çok gizli, gizli, özel, hizmete özel, ticari gizli, ticari özel, kişiye gizli, kişiye özel, tasnif dışı) altında sınıflandırılmış ve özel nitelikli kişisel veriler “*Kişiye gizli*” gizlilik derecesine dâhil edilmiştir.

Her ne kadar kararda Kurul tarafından, özel nitelikli kişisel verilerin özellikle aktarılmasına dair spesifik güvenlik önlemleri belirlenmişse de kanaatimizce, kişisel verilerin işlenmesi kavramı, aktarılma kavramını da kapsadığı için özel nitelikli kişisel verilerin aktarılması zamanı, kararda verilerin işlenmesi ve muhafazası için öngörülen diğer önlemler de dikkate alınmalıdır. Örneğin; özel nitelikli kişisel verilerin işlenmesi süreçlerinde yer alan çalışanlara yönelik; a) çalışanlara düzenli olarak eğitimler verilmesi, b) çalışanlarla gizlilik sözleşmelerinin yapılması, c) verilere erişim yetkisi olan kullanıcıların, yetki kapsamlarının ve sürelerinin net olarak belirlenmesi, ç) görev değişikliği veya işten ayrılma durumunda çalışanların bu alandaki yetkilerinin derhâl kaldırılması, veri sorumlusu tarafından kendisine tahsis edilen envanterin iade alınması gibi önlemler öngörülmüştür⁷⁰⁹.

Ayrıca özel nitelikli kişisel verilerin işlendiği, muhafaza edildiği veya erişildiği ortam, elektronik ise; a) verilerin kriptografik yöntemler kullanılarak muhafaza edilmesi ve kriptografik anahtarların güvenli ve farklı ortamlarda tutulması, b) verilerin bulunduğu ortamlara dair güvenlik güncellemelerinin sürekli takip edilmesi, gerekli güvenlik testlerinin düzenli olarak yapılması ve sonuçların kayıt altına alınması, c) verilere uzaktan erişim gerekiyorsa en az iki kademeli kimlik doğrulama sisteminin sağlanması; özel nitelikli kişisel verilerin işlendiği, muhafaza edildiği veya erişildiği ortam, fiziksel ise; a) ortamın niteliğine göre yeterli güvenlik önlemlerinin alındığından emin olunması ve b) yetkisiz giriş çıkışların engellenmesi gerekmektedir⁷¹⁰.

Yukarıda belirtilen önlemlerin yanı sıra Veri Güvenliği Rehberi’nde belirtilen uygun güvenlik düzeyini temin etmeye yönelik teknik ve idari tedbirler de dikkate

⁷⁰⁹ Kişisel Verileri Koruma Kurulu, 31.01.2018 tarihli ve 2018/10 sayılı karar, m.2.

⁷¹⁰ Kişisel Verileri Koruma Kurulu, 31.01.2018 tarihli ve 2018/10 sayılı karar, m.3, m.4.

alınmalıdır. İdari tedbirlere; mevcut risk ve tehditlerin belirlenmesi, çalışanların eğitilmesi ve farkındalık çalışmaları, kişisel veri güvenliği politikalarının ve prosedürlerinin belirlenmesi, kişisel verilerin mümkün olduğunca azaltılması, veri işleyenler ile ilişkilerin yönetimi dâhildir⁷¹¹.

Teknik tedbirlere ise; siber güvenliğin sağlanması, kişisel veri güvenliğinin takibi, kişisel veri içeren ortamların güvenliğinin sağlanması, kişisel verilerin bulutta depolanması, bilgi teknolojileri sistemleri tedariği, geliştirme ve bakımı, kişisel verilerin yedeklenmesi dâhildir⁷¹².

IV. Kişisel Verilerin Yurt Dışına Aktarılması

A. Genel Olarak

KVKK'nın uygulama alanı dikkate alındığında kişisel verilerin korunması kural olarak Türkiye sınırları dâhilinde mümkün olacaktır. Başka bir deyişle, kanunda öngörülen yaptırımların yurt dışında da uygulanması beklenemeyecektir. Buna karşılık uluslararası düzeyde veri aktarım faaliyeti oldukça yaygındır. Hatta günümüz dünyasında kişisel verilerin yabancı ülkelere aktarılmasını beklemek olağan değildir⁷¹³. Böyle bir beklenti ülkeler arasında ekonomik ve ticari ilişkilerin sonlandırılması anlamına gelecektir. Hem bu ilişkilere zarar vermemek hem de kişisel verilerin en az müdahaleye uğrayacağı şekilde korunması adına yurt dışına veri aktarımları, Kanun'da özel bir hükümle düzenlenmiş ve yurt içinde veri aktarımlarından daha sıkı şartlara tabi tutulmuştur⁷¹⁴.

Yurt içinde yapılan aktarımlara ilişkin madde 8'in gerekçesinde kişisel verilerin üçüncü kişilere aktarılmasından bahsedilse de, yurt dışına yapılan aktarımları düzenleyen madde 9'un gerekçesinde benzer ifadeye yer verilmemiştir⁷¹⁵.

⁷¹¹ Kişisel Verileri Koruma Kurumu, Veri Güvenliği Rehberi, s. 7-14.

⁷¹² Kişisel Verileri Koruma Kurumu, Veri Güvenliği Rehberi, s. 15-26.

⁷¹³ Murat Volkan Dülger, "Kişisel Verileri Koruma Kurulu'nun 108 Sayılı Sözleşme Hakkındaki Kararı ve Yurtdışına Veri Aktarımı Sorunu", s. 2, (çevrimiçi) https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3792396, 18.10.2021.

⁷¹⁴ Dülger, **Kişisel Veriler**, s. 326; Çekin, **Kişisel Verilerin Korunması**, s. 113; Kişisel Verileri Koruma Kurumu, Yurt Dışına Veri Aktarımı Kamuoyu Duyurusu, (çevrimiçi), <https://www.kvkk.gov.tr/icerik/6828/yurtdisina-veri-aktarimi-kamuoyu-duyurusu>, 25.10.2021.

⁷¹⁵ Bkz.: KVKK m.9 gerekçesi.

Buradan çıkan sonuca göre, yurt dışına aktarımdan bahsedilebilmesi için veri alıcısının, üçüncü kişi niteliğini haiz olması şart olmayıp, verilerin ülke sınırlarının dışına çıkması yeterli kabul edilmiştir⁷¹⁶. Bu anlamda Türkiye’de yerleşik bir şirketin yurt dışında yerleşik şubesine veya çalışanlarına yönelik veri paylaşımları da yurt dışına veri aktarımı olarak kabul edilecektir. Ayrıca, veri alıcısı fiziksel olarak ülke sınırları dışında bulunmasa bile aktarım sırasında yurt dışı tabanlı bir sunucu kullanıldığı takdirde yine yurt dışına aktarım söz konusu olacaktır⁷¹⁷. Nitekim Kurul da bir kararında⁷¹⁸ bu yönde karar vermiştir. Aynı zamanda söz konusu kararda, sunucuları yurt dışında bulunan veri sorumlularından/ veri işleyenlerden temin edilen saklama hizmetlerinin de yurt dışına veri aktarımı olarak kabul edileceği kabul edilmiştir. Bu noktadan hareketle, verilere yalnızca yurt içinden erişiliyor olsa dahi, sunucuları yurt dışında bulunan bulut hizmetleri kullanıldığı takdirde veriler konum olarak yurt dışında bulunacağından bu tür hizmetlerin kullanımı da yurt dışına veri aktarımına ilişkin kurallara tabi tutulmalıdır⁷¹⁹.

Açıklanması gereken bir diğer husus ise kimlerin veri aktaran olarak yurt dışına veri aktarımı gerçekleştirebileceğidir. KVKK m.9/f.2/b hükmünün lafzından anlaşıldığı üzere, yazılı taahhütnameleri onaylatmak suretiyle yurt dışına veri aktarımı, yalnızca veri sorumluları tarafından gerçekleştirilebilecektir. Aynı şekilde Kurum’un 10 Nisan 2020 tarihli duyurusunda⁷²⁰ yeni bir aktarım mekanizması olarak belirlenen bağlayıcı şirket kuralları da sadece veri sorumlularının başvurabileceği bir hukuki araç olarak kabul edilmiştir. Bunların dışında kalan durumlarda (örneğin, aktarım için ilgili kişinin açık rızasının alınması veya verilerin aktarılacağı ülkede yeterli korumanın bulunması) gerçekleştirilecek veri aktarımları açısından herhangi

⁷¹⁶ Dülger, **Kişisel Veriler**, s. 327, 437; Çelik, s. 70.

⁷¹⁷ Dülger, **Kişisel Veriler**, s. 438; Çelik, s. 70.

⁷¹⁸ Bkz.: Kişisel Verileri Koruma Kurulu, 31/05/2019 tarihli ve 2019/157 sayılı Karar, (çevrimiçi), <https://www.kvkk.gov.tr/Icerik/5493/2019-157>, 19.10.2021.

⁷¹⁹ Dülger, **Kişisel Veriler**, s. 440; Erarslan, **Verilerin Aktarılması**, s. 96; Kişisel Verileri Koruma Kurumu, Uzaktan Eğitim Platformları Hakkında Kamuoyu Duyurusu, (çevrimiçi) <https://www.kvkk.gov.tr/icerik/6723/uzaktan-egitim-platformlari-hakkinda-kamuoyu-duyurusu>, 16.12.2021; Kişisel Verileri Koruma Kurumu, **Doğru Bilinen Yanlıklar 2**, s. 34; Çelik, s. 70-71. Yurt dışına veri aktarımı açısından bulut hizmetlerinin durumuna ilişkin detaylı bilgi için bkz.: Dülger, **Kişisel Veriler**, s. 439-443.

⁷²⁰ Bkz.: Kişisel Verileri Koruma Kurumu, Bağlayıcı Şirket Kuralları Hakkında Duyuru, 10.04.2020, (çevrimiçi), <https://www.kvkk.gov.tr/icerik/6728/yurt-disina-kisisel-veri-aktariminda-baglayici-sirket-kurallari-hakkinda-duyuru>, 28.10.2021.

bir açıklama bulunmamaktadır. KVKK m.3/f.1/ı uyarınca veri işleme faaliyetini, veri sorumlusu veya KVKK m.3/f.1/ğ uyarınca veri sorumlusunun verdiği yetkiye dayanarak veri sorumlusu adına veri işleyen gerçekleştirebilir⁷²¹. Verilerin aktarılması da bir işleme türü olduğundan aksi belirtilen durumlar (Kurul'un onayladığı yazılı taahhütnameler ve bağlayıcı şirket kurallarına dayalı veri aktarımları) saklı kalmak kaydıyla, bu hükmün dikkate alınabileceği kanaatindeyiz.

Veri aktaranın kimliğine ilişkin bu belirsizlik, ilgili kişi tarafından yapılan veri paylaşımlarının da yurt dışına aktarım olarak kabul edilip edilmeyeceği sorusunu gündeme getirmektedir. Şöyle ki bazen gerçek kişiler, herhangi bir hizmetten yararlanmak için ad, soyad, e-posta adresi, telefon numarası vs. gibi kişisel verilerini yurt dışında yerleşik bir şirketle veya elde ettiği verileri yurt dışında bulunan sunucularda tutan bir şirketle paylaşabilmektedirler. Bu gibi durumlarda Türkiye sınırlarını aşan veri paylaşımı söz konusu olduğundan yurt dışına aktarıma ilişkin hükümlerin uygulanıp uygulanmayacağı sorusuna açıklık getirmek gerekmektedir⁷²².

Doktrinde mevcut olan bir görüşe⁷²³ göre ilgili kişinin, kendi verilerini ülke sınırlarını aşacak şekilde paylaşmasının yurt dışına veri aktarımı olarak kabul edilmesi, veri sorumlusu ile ilgili kişi arasındaki hukuki ilişkiyi sona erdireceğinden, bu şekilde bir yorum isabetli olmayacaktır. Şöyle ki, ilgili kişinin yurt dışına aktarım yaptığının kabulü hâlinde, aktarımı KVKK'ya uygun şekilde gerçekleştirmekle yükümlü olan veri sorumlusu ile verileri işlenen ilgili kişinin niteliklerinin aynı kişide birleştirilmesi söz konusu olacağı için, verilerin korunmasına ilişkin kanunda öngörülen yükümlülükler ortadan kalkacak ve ilgili kişinin haklarının yöneltilebileceği bir taraf mevcut olmayacaktır⁷²⁴. Ayrıca KVKK m.9 kapsamında öngörülen yükümlülükler, aktarım faaliyetini gerçekleştiren gerçek ve tüzel kişilere yöneliktir. Verilen örneklerde ise ilgili kişi veri işleme faaliyetini

⁷²¹ Çelik, s. 69.

⁷²² Çelik, s. 70.

⁷²³ Çelik, s. 71.

⁷²⁴ Çelik, s. 71-72.

gerçekleştirmemekte, aksine ilgili kişinin verileri işleme faaliyetine konu edilmektedir⁷²⁵.

Kurul ise bu hususla ilgili farklı yönde karar vermiş ve 03.09.2021 tarihli ve 2021/891 sayılı kararında, sunucuları yurt dışında bulunan Whatsapp LLC'nin, verdiği hizmet karşılığında Türkiye'de bulunan ilgili kişilerden elde ettiği verileri işleminin KVKK m.9 hükümlerine tabi olduğunu ifade etmiştir⁷²⁶. Bu konuda Kurul'un verdiği kararı hatalı bulduğumuzu ve yukarıda belirtilen görüşe katıldığımızı belirtmek isteriz. Nitekim EDPB de bu hususla ilgili, kişisel verilerin doğrudan ilgili kişi tarafından veya ilgili kişinin inisiyatifıyla veri alıcısına ifşa edilmesi hâlinde bir veri aktaranın varlığından söz edilemeyeceğini, dolayısıyla bu durumun üçüncü ülkelere veya uluslararası kuruluşlara veri aktarımı olarak değerlendirilemeyeceğini belirtmiştir⁷²⁷.

Kişisel verilerin ülke sınırları dışında hareket etmesi hâlinde ilgili kişilerin, kişisel verilerin korunması haklarını kullanmalarının daha fazla risk altında olduğu kesindir. Zira kişisel veri yurt dışına aktarıldığı zaman ilgili kişinin, artık o veri üzerinde hâkimiyeti azalmakta ve dolayısıyla haklarının korunması da daha fazla risk altına girmektedir⁷²⁸. Şöyle ki kişisel verilerin yurt dışına kanuna aykırı bir şekilde aktarıldığı tespit edilse bile, buna karşı ilgili kişinin yurt dışında hukuki bir mücadele başlatması beklenemeyeceğinden ve Kurul'un yurt dışına müdahale imkânı bulunmadığından, Kanun'un 9'uncu maddesinde bazı ek şartlar öngörülmeyle, yurt içinde öngörülen koruma seviyesinin yurt dışında da sağlanması amaçlanmaktadır⁷²⁹.

KVKK m.9 uyarınca, ilgili kişinin açık rızası olmaksızın kişisel veriler yurt dışına aktarılamaz. Kişisel verilerin yurt içinde aktarılabilmesi için aranan açık rıza hususunda yukarıda yapılan açıklamalar bu çerçevede de geçerlidir. Bu nedenle bu

⁷²⁵ Çelik, s. 71.

⁷²⁶ Kişisel Verileri Koruma Kurumu, Whatsapp Uygulaması Hakkında Yürütülen Resen İncelemeye İlişkin Kamuoyu Duyurusu, (çevrimiçi), <https://www.kvkk.gov.tr/icerik/7045/whatsapp-uygulaması-hakkında-yurutulen-resen-incelemeye-iliskin-kamuoyu-duyurusu>, 22.10.2021.

⁷²⁷ EDPB, **Guidelines 05/2021**, s.5.

⁷²⁸ Dülger, **108 sayılı Sözleşme**, s. 2; Baran Kızıllırmak, "Kişisel Verilerin Yurt Dışına Aktarımında KVKK Uygulamasının Eleştirisi", 2020, (çevrimiçi), <https://law.khas.edu.tr/tr/kisisel-verilerin-yurt-disina-aktariminda-kvkk-uygulamasinin-elestirisi>, 15.09.2021; Çelik, s. 4.

⁷²⁹ Çekin, **Kişisel Verilerin Korunması**, s. 114; Dülger, **108 sayılı sözleşme**, s. 2; Dülger, **Kişisel Veriler**, s. 437; Kama Işık, s. 266; Çelik, s. 4.

bölümde sadece kişisel verilerin açık rıza aranmaksızın yurt dışına aktarılması faaliyeti ele alınacaktır.

Açık rızanın bulunmadığı durumlarda ise kişisel verilerin yurt dışına aktarılması için kanun koyucu tarafından iki aşamalı korumanın söz konusu olduğu bir düzenlemeye gidilmiştir. Başka bir deyişle KVKK m.9/f.2 uyarınca, açık rıza olmaksızın kişisel verilerin yurt dışına aktarılabilmesi için aynı anda iki şartın varlığı aranmaktadır. Bunlardan ilki, KVKK m.5/f.2 ve m.6/f.3'te belirtilen hukuka uygunluk şartlarından birinin mevcut olmasıdır. Söz konusu hukuka uygunluk sebeplerinden herhangi birinin varlığı, kişisel verilerin yurt içinde aktarılmasını meşru kılsa da, yurt dışına aktarım için tek başına yeterli bulunmamıştır. Şöyle ki kişisel verilerin, açık rıza aranmaksızın yurt dışına aktarılabilmesi için bu hukuka uygunluk sebeplerinin yanı sıra kişisel verilerin aktarılacağı yabancı ülkede yeterli korumanın bulunması (KVKK m.9/f.2/a) veya Türkiye'deki ve ilgili yabancı ülkedeki veri sorumlularının yeterli bir korumayı yazılı olarak taahhüt etmeleri ve Kurul'un izninin bulunması gerekmektedir (KVKK m.9/f.2/b).

Bu bağlamda kişisel verilerin açık rıza olmadan yurt dışına aktarılmasının iki alternatifi mevcuttur:

1. Yeterli korumanın bulunduğu durumlarda yapılan aktarımlar (m.9/f.2/a)
2. Yeterli korumanın bulunmadığı durumlarda yapılan aktarımlar (m.9/f.2/b)

Yeterli korumanın bulunup bulunmamasından bağımsız olarak, Kanun'da kişisel verilerin sadece Kurul'un izniyle yurt dışına aktarılabilceği durumlar da öngörülmüştür. Şöyle ki m.9/f.5 uyarınca, *uluslararası sözleşme hükümleri saklı kalmak üzere*, Türkiye'nin veya ilgili kişinin menfaatinin ciddi bir şekilde zarar göreceği durumlarda⁷³⁰, kişisel veriler ancak ilgili kamu kurum veya kuruluşunun görüşü alınarak Kurul'un izniyle yurt dışına aktarılabilir. Hükmün lafzından anlaşıldığı üzere, verilerin yurt dışına aktarılması bağlamında uluslararası sözleşmelere öncelik tanınmıştır. Buradan çıkan sonuca göre, kişisel verilerin

⁷³⁰ “Türkiye'nin veya ilgili kişinin menfaatinin ciddi bir şekilde zarar göreceği durumlar” ifadesinden ne anlaşılması gerektiği muğlak olduğundan doktrinde eleştirilmektedir. Bkz.: Küzeci, s. 413; Kama Işık, s. 268.

Türkiye’den başka bir ülkeye aktarılması, herhangi bir uluslararası sözleşmenin kapsamına dâhil olduğu takdirde, m.9’da öngörülen şartların (açık rıza, yeterli koruma sağlayan ülke, taahhütname vs) aranmasına gerek kalmayacaktır⁷³¹. Veri aktarımına ilişkin hükümler içeren ve Türkiye’nin de taraf olduğu uluslararası sözleşmelere; Hukuki ve Ticari Konularda Yabancı Ülkelerde Delil Sağlanması Hakkında Sözleşme, Vergi Konularında Karşılıklı İdari Yardımlaşma Sözleşmesi, Türkiye Cumhuriyeti Hükümeti ile ABD Hükümeti Arasında “Genişletilmiş Bilgi Değişimi Yoluyla Uluslararası Vergi Uyumunun Artırılması Anlaşması” örnek olarak gösterilebilir.

Şunu da belirtmek gerekir ki KVKK m.9/f.6 uyarınca, kişisel verilerin yurt dışına aktarılmasına ilişkin diğer kanunlarda yer alan hükümler saklıdır. Örneğin, 2920 sayılı Türk Sivil Havacılık Kanunu’nun 40’inci maddesi uyarınca, havayolu ile seyahat edecek kişilerin bilgileri kişilerin seyahatini kolaylaştırmak veya güvenlik ve risk değerlendirmesi yapmak amacıyla KVKK çerçevesinde toplanabilir, kaydedilebilir, işlenebilir, paylaşılabilir. Bu kapsamda, yolcu bilgileri talep hâlinde havayolu işletmeleri veya kurumlar tarafından üçüncü ülkelerle İçişleri Bakanlığının uygun görüşü ile paylaşılabilir.

Yine 5411 sayılı “Bankacılık Kanunu”⁷³² m.73/f.3 uyarınca, diğer kanunlarda yer alan emredici düzenlemeler saklı kalmak kaydıyla, müşteri sırrı niteliğini haiz bilgiler, m.73’te belirtilen istisnalar dışında, KVKK uyarınca müşterinin açık rızası alınsa dahi müşteriden bu yönde gelen bir talep veya talimat olmadan yurt dışındaki ve yurt içindeki üçüncü kişilerle paylaşılamaz ve bunlara aktarılamaz.

Şunu da belirtmek gerekir ki, Anayasa m.90/f.5 uyarınca usulüne uygun yürürlüğe konulan milletlerarası antlaşmalar kanun hükmündedir ve temel hak ve özgürlüklere ilişkin milletlerarası antlaşmalar ile kanunların aynı konuda farklı hükümler içermesi nedeniyle çıkabilecek uyuşmazlıklarda milletlerarası antlaşma hükümleri esas alınacaktır. Fakat diğer kanunlarda yer alan yurt dışına aktarıma ilişkin hükümler ile KVKK m.9 hükümlerinin çelişmesi durumunda ne tür bir yol

⁷³¹ Altındağ, s. 126; Sertçe, s. 121; Çelik, s. 52.

⁷³² RG. T. 01.11.2005, S. 25983 (mükerrer).

izlenmesi gerektiği KVKK’da açıkça düzenlenmemiştir. Bu hususta yukarıda kişisel verilerin yurt içinde aktarılmasına ilişkin hükümler içeren kanunlar açısından belirtilen bulgular saklıdır⁷³³.

B. Yeterli Korumanın Bulunduğu Durumlarda Aktarılma

Yukarıda da belirtildiği üzere açık rıza aranmaksızın kişisel verilerin yurt dışına aktarılmasının birinci yolu, verilerin yeterli korumanın bulunduğu ülkelere aktarılmasıdır. Öncelikle “yeterli koruma” kavramından ne anlaşılması gerektiğini hatırlatmakta fayda var. Kurum’un rehber ve kararlarında bununla ilgili herhangi bir açıklama bulunmasa da AB hukukuna istinaden “yeterli koruma”nın “eşdeğer koruma” düzeyini ifade ettiğini söylemek mümkündür. Şöyle ki buna göre, verilerin aktarılacağı yabancı ülkenin; Türkiye’yle aynı değil, Türkiye’dekine eşdeğer bir korumaya sahip olması beklenmektedir.

Yeterli korumaya sahip olan ülkelere kişisel veri aktarımı gerçekleştirmek için öncelikle aktarılacak verilerin genel veya özel nitelikte olmasına bağlı olarak, Kanun’un 5.2 veya 6.3 maddesinde yer alan şartlardan herhangi birinin varlığı aranacaktır. Bu şartlardan herhangi biri bulunduğu takdirde verilerin aktarılacağı ülkenin “yeterli korumaya sahip ülke” olarak belirlenip belirlenmediği kontrol edilmelidir.

KVKK m.9/f.3 uyarınca, yeterli korumanın bulunduğu ülkeler Kurul tarafından belirlenerek ilan edilir. Kurul, güvenli ülke statüsünün tayinine ilişkin çalışmalarını Adalet Bakanlığı, Dışişleri Bakanlığı ve Ticaret Bakanlığı ile iş birliği içerisinde yürütmektedir. Ayrıca diğer kamu kurum ve kuruluşları, sivil toplum kuruluşları, meslek örgütleri ve diğer paydaşlar tarafından hakkında yeterlilik kararı verilmesinin yararlı olacağı düşünülen ülkelere ilişkin Kurul’a öneride bulunulabilir⁷³⁴.

Kurul’un yabancı ülkede yeterli korumanın bulunup bulunmadığını değerlendirirken dikkate alacağı kriterler KVKK m.9/f.4’de belirlenmiştir. Buna

⁷³³ Bkz.: yuk. Üçüncü Bölüm, “Kişisel Verilerin Yurt İçinde Aktarılması/ Kanunlarda Açıkça Öngörülme” başlığı.

⁷³⁴ Kişisel Verileri Koruma Kurumu, **Yurt Dışına Veri Aktarımı Kamuoyu Duyurusu**.

göre, Kurul yeterli koruma değerlendirmesi yaparken; 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 verin 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* dikkate alacaktır. Aynı zamanda Kurul'un 02.05.2019 tarihli ve 2019/125 sayılı kararı ile "Yeterli Korumaya Sahip Ülkelerin Belirlenmesinde Esas Alınacak Kriterler" belirlenmiştir⁷³⁵. Buna göre yeterli korumanın bulunup bulunmamasına dair değerlendirme aşağıdaki kriterlere göre yapılacaktır:

- Karşılıklılık durumu,
- İlgili ülkenin kişisel verilerin işlenmesine ilişkin mevzuatı ve uygulaması,
- Bağımsız veri koruma otoritesinin bulunması,
- Kişisel verilerin korunması ile ilgili uluslararası anlaşmalara taraf olma ile uluslararası kuruluşlara üye olma durumu,
- Ülkemizin üye olduğu küresel ve bölgesel örgütlere üye olma durumu,
- İlgili ülke ile yürütülen ticaretin hacmi vs.

Kurum, karşılıklılık durumunun, ülkemizde faaliyet gösteren veri sorumlusu ve veri işleyenlerin kişisel verilerin güvenli, maliyetsiz ve hızlı bir şekilde aktarım olanağından aynı şekilde yararlanabilmeleri, ekonomik kazanç sağlayabilmeleri ve bu bakımdan tek taraflı tanımının yaratacağı asimetri nedeniyle dezavantajlı konumda bulunmamaları için büyük önem arz ettiğini belirtmiştir. Buna karşılık Dülger, bu alanda henüz yeni bir ülke olarak, karşılıklılık durumu aranmasının, diğer kriterler karşılanırsa bile birçok ülkenin yeterli koruma sağlayan ülke olarak kabul edilemeyeceğine sebep olacağını belirtmiştir⁷³⁶.

Şimdiye kadar Kurul tarafından herhangi bir ülke hakkında yeterlilik kararı yayınlanmamıştır. Esasında Kurul tarafından yeterli koruma bulunup bulunmadığına

⁷³⁵ Bkz.: Kişisel Verileri Koruma Kurumu, Yeterli Korumaya Sahip Ülkelerin Belirlenmesinde Esas Alınacak Kriterler, (çevrimiçi), <https://kvkk.gov.tr/sharedfolderserver/cmsfiles/60d987a1-ba9d-4285-a8ce-c3f41ff4e47f.pdf>, 05.11.2021.

⁷³⁶ Dülger, **Kişisel Veriler**, s. 447.

ilişkin yapılacak değerlendirmenin; çeşitli ve birbirinden oldukça farklı ulusal hukuk düzenlerinin mevcudluğu, bazı ülkelerde genel nitelikte bir veri koruma düzenlemesinin bulunmaması veya sadece belli alanları kapsayan düzenlemelerin bulunması ve federal devletlerde eyaletler arasındaki farklılıklar göz önünde bulundurulduğunda titizlikle yürütülmesi gereken yoğun ve uzun bir süreç olduğunun kabul edilmesi gerekir⁷³⁷. Fakat kanunun yürürlüğe girmesinden bu yana uzun bir süre geçse de henüz Kurul tarafından belirlenen yeterli korumaya sahip ülkeler listesi bulunmaması her daim eleştiri konusu olmuştur. Zira bu durum Türkiye’de bulunan ve yurt dışına veri aktarımı gerçekleştirmek isteyen veri sorumlularını diğer veri aktarımı alternatiflerine muhtaç duruma düşürmüştür. Kanaatimizce, bu zamana kadar en azından AB üyesi ülkeler hakkında Kurul tarafından yeterlilik kararları verilebilirdi. Zira hem KVKK, GDPR hükümleri baz alınarak kabul edilmiş olup hem de Kurul verdiği kararlarda ve rehberlerinde yoğun bir şekilde GDPR hüküm ve gerekçelerine atıfta bulunmaktadır. Böyle bir durumda bu hükümlere tabi olan ülkelerin kendi aralarında güvenli kabul edilirken Türkiye açısından güvenli kabul edilmesinde de bir sakınca olmamalıdır⁷³⁸. Bu hususla ilgili Kurum, karşılıklı yeterlilik kararı verilmesine ilişkin AB ile resmî ve gayriresmî istişarelerde bulunduğunu belirtmiştir⁷³⁹.

Kurum tarafından yayınlanan “Yurtdışına Veri Aktarımı Kamuoyu Duyurusu”nda yeterlilik kararları, “*yaşayan birer doküman*” olarak nitelendirilmiştir. Şöyle ki, herhangi bir ülke hakkında yeterlilik kararı yayınlansa bile bu kararlar, periyodik gözden geçirmelere tabi tutulacak ve değişen koşullara göre söz konusu yeterlilik kararları değiştirilebilecek, askıya alınabilecek veya kaldırılacaktır⁷⁴⁰. Dolayısıyla, güvenli ülke statüsünün belirlenmesi, kapsamlı ve uzun bir süreç olduğu gibi aynı zamanda bu koruma düzeyinin sürekliliğinin takip edilmesini gerektiren dinamik bir süreci de ifade etmektedir⁷⁴¹.

⁷³⁷ Kişisel Verileri Koruma Kurumu, **Yurt Dışına Veri Aktarımı Kamuoyu Duyurusu**.

⁷³⁸ Dülger, **108 sayılı Sözleşme**, s. 4; Dülger, **Kişisel Veriler**, s. 447; Erarslan, **Verilerin Aktarılması**, s. 107.

⁷³⁹ Kişisel Verileri Koruma Kurumu, **Yurt Dışına Veri Aktarımı Kamuoyu Duyurusu**.

⁷⁴⁰ Ayözger Öngün, s. 201; Çelik, s. 83.

⁷⁴¹ Kişisel Verileri Koruma Kurumu, **Yurt Dışına Veri Aktarımı Kamuoyu Duyurusu**.

C. Yeterli Korumanın Bulunmadığı Durumlarda Aktarılma

Günümüzde kişisel verilerin işleme süreçlerinde sadece bir ülke sınırlarında kalması olağan bir durum değildir. Bunun aksine verilerin birkaç ülkede dolaşımı kuraldır. Fakat her ne kadar uygulamada kişisel verilerin yurt dışına aktarım ihtiyacı mevcut olsa da, Kurul'un güvenli ülke tayini hususunda çekimser davranması, çelişkili bir durum ortaya çıkarmıştır. Buna karşılık alternatif aktarım imkânları gündeme gelmektedir⁷⁴². KVKK m.9/f.2/b uyarınca, yeterli korumanın bulunmaması durumunda Türkiye'deki ve ilgili yabancı ülkedeki veri sorumlularının yeterli korumayı yazılı olarak taahhüt etmeleri ve Kurul'un izninin bulunması kaydıyla kişisel veriler, ilgili kişinin açık rızası aranmaksızın yurt dışına aktarılabilir. Ayrıca Kurum'un 10.04.2020 tarihinde yayınladığı duyuruda⁷⁴³, çok uluslu şirket toplulukları arasında yapılacak veri aktarımlarını kolaylaştırmak adına yeterli korumanın bulunmadığı ülkelere veri aktarımı gerçekleştirmek için yeni bir yöntem olarak "bağlayıcı şirket kuralları" da belirlenmiştir.

1. Yazılı Taahhütnameler

a. Genel Olarak

KVKK m.9/f.2/b uyarınca, verilerin aktarılacağı yabancı ülkede yeterli koruma bulunmadığı durumlarda, Türkiye'de ve verilerin aktarılacağı ülkede bulunan veri sorumlularının yeterli korumayı yazılı olarak taahhüt etmesi ve Kurul'un izninin alınması kaydıyla, ilgili kişinin açık rızası alınmadan kişisel verilerin yurt dışına aktarılması mümkündür. Bunun için aynı anda üç şartın mevcut olması gerekmektedir:

1. Kanun m.5/f.2 veya m.6/f.3'de öngörülen hukuka uygunluk sebeplerinden herhangi biri,
2. Yazılı bir taahhütname,
3. Kurul'un izni.

⁷⁴² Çekin, **Kişisel Verilerin Korunması**, s. 117; Çelik, s. 84.

⁷⁴³ Bkz.: Kişisel Verileri Koruma Kurumu, Bağlayıcı Şirket Kuralları Hakkında Duyuru, 10.04.2020, (çevrimiçi), <https://www.kvkk.gov.tr/icerik/6728/yurt-disina-kisisel-veri-aktariminda-baglayici-sirket-kurallari-hakkinda-duyuru>, 28.10.2021.

Öncelikle, aranması gereken ilk şart KVKK m.5/f.2 veya m.6/f.3 maddesinde bulunan şartlardan birinin varlığıdır. Şayet söz konusu şartlardan hiçbiri yok ise ilgili kişinin açık rızasının alınması gerekecektir. Açık rızaya dayalı aktarımlar ise taahhütnamelere konu edilemeyecektir.

KVKK m.9/f.2/b hükmünde sadece veri sorumluları arasında yapılan aktarımlardan bahsedilse de, Kurul hükmün kapsamını Türkiye’de bulunan veri sorumlusundan yeterli korumanın bulunmadığı yabancı ülkede yerleşik veri işleyene yapılan aktarımları da kapsayacak şekilde genişletmiştir. Şöyle ki, Kurum tarafından “veri sorumlusundan veri sorumlusuna” ve “veri sorumlusundan veri işleyene” olmak üzere iki ayrı taahhütname şablonları⁷⁴⁴ yayınlanmıştır. “Veri sorumlusundan veri işleyene” aktarıma ilişkin taahhütname örneğinin konu kısmında, Türkiye’de bulunan veri sorumlusundan yeterli koruma bulunmayan yabancı ülkede yerleşik veri işleyene yapılacak aktarımların, KVKK m.12/f.2 uyarınca hazırlanacak olan sözleşmeye dayanabileceği belirtilmiştir⁷⁴⁵. Bu hukuki temellendirmeyi hatalı bulan doktrin görüşüne⁷⁴⁶ göre, Kurulun KVKK m.22/f.1/a-e ve g bentlerine dayanması daha uygun olacaktır. Zira KVKK m.12/f.2 hükmü, veri sorumlusunun, işleme faaliyetine veri işleyeni dahil ettiği durumlarda veri sorumlusu ile veri işleyenin veri güvenliğine ilişkin tedbirlerin alınması hususunda müştereken sorumlu olmasına ilişkindir. Bunun aksine m.22/f.1/e bendinde Kurulun görev alanı ile Kurumun işleyişine, m.22/f.1/g bendinde ise veri sorumlusunun ve temsilcinin görev, yetki ve sorumluluklarına ilişkin konularda düzenleyici işlemler yapabileceği belirtilmiştir⁷⁴⁷.

Aktarımı gerçekleştirecek olan veri sorumlusu, yeterli korumanın bulunmadığı yabancı ülkedeki veri sorumlusu veya veri işleyenle birlikte şablonda gösterilen hükümleri içeren taahhütnameyi imzalamalı ve daha sonra Kurul’a başvurarak aktarım için izin almalıdır. Nitekim Kurul’un “Amazon Turkey”

⁷⁴⁴ Bkz.: Kişisel Verileri Koruma Kurumu, Yurtdışına Veri Aktarımında Veri Sorumlularınca Hazırlanacak Taahhütnamede Yer Alacak Asgari Unsurlar, 16.05.2018, (çevrimiçi), <https://www.kvkk.gov.tr/icerik/4236/yurtdisina-veri-aktariminda-veri-sorumlularinca-hazirlanacak-taahhutnamede-yer-alacak-asgari-unsurlar>, 25.10.2021.

⁷⁴⁵ Kişisel Verileri Koruma Kurumu, Veri Sorumlusundan Veri İşleyene Aktarım, (çevrimiçi), s. 3, <https://www.kvkk.gov.tr/SharedFolderServer/CMSFiles/d4ef9857-ff4e-4c5b-925c-fdd3e4eca73d.doc>, 25.10.2021.

⁷⁴⁶ Bilgi Information Technology Law Institute, s. 12; Çelik, s. 89- 90.

⁷⁴⁷ Bilgi Information Technology Law Institute, s. 12; Çelik, s. 90.

kararında da taahhütname başvurusunda bulunmuş olmanın tek başına veri aktarımı için yeterli olmadığı, söz konusu taahhütnamenin Kurul tarafından onaylanması gerektiği yinelenmiştir⁷⁴⁸. Kurul, taahhütname başvurularını değerlendirirken yabancı ülkelerde yeterli korumanın bulunup bulunmadığına ilişkin kriterlere (KVKK m.9/f.4) dayanarak karar vermektedir.

Veri aktarımına ilişkin yazılı taahhütnameler, GDPR’da düzenlenen standart sözleşme hükümlerine tekabül etmektedir. Fakat AB hukukunda yeterli düzeyde korumanın bulunmadığı ülkelere yapılan aktarımlar açısından en çok kullanılan hukuki araç, standart sözleşme hükümleri olsa da Türk hukukunda taahhütnamelere dayalı aktarımlar uygulamada karşılık bulamamıştır. Kanaatimizce, bunun esas sebebi standart sözleşme hükümlerine dayalı aktarımın gerçekleşmesi için herhangi bir veri koruma otoritesinin onayı gerekmesi de, yazılı taahhütnamelere dayalı veri aktarımlarının Kurul’un iznine tabi tutulmuş olmasıdır⁷⁴⁹. Bu da doğal olarak süreci geciktirmektedir. Ayrıca Kurul’un, taahhütnameleri değerlendirme sürecinin herhangi bir süreyle sınırlandırılmaması, veri aktarım sürecini belirsiz hale getirmektedir⁷⁵⁰. Sonuç olarak Kanun’un yürürlüğe girmesinden bu yana, bu çalışmanın yapıldığı tarih itibarıyla Kurul tarafından sadece dört taahhütname başvurusu hakkında olumlu sonuca varılmış ve yayınlanmıştır⁷⁵¹.

b. Taahhütname Başvurularında Dikkat Edilmesi Gereken Hususlar

Kurum, taahhütname başvurularının geç sonuçlanmasının bir sebebi olarak, başvurularda taahhütnamelerin ekinde yer alan söz konusu kişisel veri aktarımının dayandığı işleme şartına, amacına, aktarıma konu veri kategorilerine, veri konusu kişi grubuna veya gruplarına, aktarım yapılacak tarafın alacağı idari ve teknik

⁷⁴⁸ Sertçe, s. 126-127.

⁷⁴⁹ Sertçe, s. 139.

⁷⁵⁰ Çelik, s. 91.

⁷⁵¹ Bkz.: TEB Arval Araç Filo Kiralama Anonim Şirketi tarafından yapılan taahhütname başvurusu hakkında 9 Şubat 2021 tarihli duyuru, (çevrimiçi) <https://kvkk.gov.tr/icerik/6867/taahhutname-basvurusu-hakkinda-duyuru>, 22.03.2021; Amazon Turkey Perakende Hizmetleri Ltd. Şti. ve Amazon Turkey Yönetim Destek Hizmetleri Ltd. Şti. tarafından yapılan taahhütname başvurusu hakkında 4 Mart 2021 tarihli duyuru, (çevrimiçi) <https://kvkk.gov.tr/icerik/6898/taahhutname-basvurusu-hakkinda-duyuru>, 22.03.2021; Türksport Spor Ürünleri San. Tic. Ltd. Şti. (Decathlon Türkiye) tarafından yapılan taahhütname başvurusu hakkında 23 Haziran 2021 tarihli duyuru, (çevrimiçi) <https://kvkk.gov.tr/icerik/6985/taahhutname-basvurusu-hakkinda-duyuru>, 29.06.2021; Türkiye Futbol Federasyonu tarafından yapılan taahhütname başvurusu hakkında 18 Ocak 2022 tarihli duyuru, (çevrimiçi) <https://kvkk.gov.tr/icerik/7161/taahhutname-basvurusu-hakkinda-duyuru>, 02.02.2022.

tedbirlere ve saklama süresi gibi unsurlar ile ilgili açıklamaların aktarıma izin verilip verilmeyeceğine ilişkin değerlendirmeye esas teşkil edebilecek açıklıkta olmadığını, ayrıca, yapılan başvuruların idari makamlara yapılacak başvurularda riayet edilmesi gereken usul ve esaslara uygun olmadan gerçekleştirildiğini belirtmiştir⁷⁵². Bunun üzerine taahhütnamelerin hazırlanmasında veri sorumluları tarafından hem usule hem de esasa ilişkin dikkat edilmesi gereken hususlar ile ilgili duyuru Kurum tarafından yayınlanmıştır⁷⁵³.

(1) Usule İlişkin Dikkat Edilmesi Gereken Hususlar

Taahhütnameye izin verilmesi için yapılan başvurularda aşağıdaki hususlar dikkate alınmalıdır⁷⁵⁴:

1. Başvuru gerçek kişi tarafından yapıldığı takdirde yetkili kişinin adı, soyadı, adresi, imzası ve imzaya yetkili olduğuna dair tevsik edici belgeler; tüzel kişilerin yapacağı başvurularda başvurunun, ilgili veri sorumlusunu bu konuda temsil ve ilzama yetkili kişi tarafından yapıldığına dair tevsik edecek belgeler; vekil ile yapılan başvurularda ise vekâletnamenin aslı ve onaylı örneği başvuruya eklenmelidir.

2. Taahhütname ekinin sonunda imza ve kaşe, her bir sayfasında ise imzacıların parafı bulunmalıdır.

3. Taahhütname ekine Türkiye’de yerleşik şirketler için ticaret sicili müdürlükleri tarafından düzenlenen sicil tasdiknamesi, Yabancı Resmî Belgelerin Tasdiki Mecburiyetinin Kaldırılması Sözleşmesi’ne⁷⁵⁵ taraf olan ülkelerde yerleşik veri alıcısı bakımından ise imzalayanın imzaya yetkili olduğunu gösteren apostil şerhli belgenin aslı veya onaylı örneği eklenmelidir.

⁷⁵² Kişisel Verileri Koruma Kurumu, **Yurt Dışına Veri Aktarımı Kamuoyu Duyurusu**.

⁷⁵³ Kişisel Verileri Koruma Kurumu, Yurt Dışına Kişisel Veri Aktarımında Hazırlanacak Taahhütnamelerde Dikkat Edilmesi Gereken Hususlara İlişkin Duyuru, 07.05.2020, (çevrimiçi), <https://www.kvkk.gov.tr/icerik/6741/yurt-dısına-kıssel-veri-aktarımında-hazırlanacak-taahhutnamelerde-dikkat-edilmesi-gereken-hususlara-iliskin-duyuru>, 28.10.2021.

⁷⁵⁴ Kişisel Verileri Koruma Kurumu, **Veri Sorumlusundan Veri Sorumlusuna Aktarım**, s. 1; Kişisel Verileri Koruma Kurumu, **Veri Sorumlusundan Veri İşleyene Aktarım**, s. 1; Kişisel Verileri Koruma Kurumu, **Yurt Dışına Kişisel Veri Aktarımında Hazırlanacak Taahhütnamelerde Dikkat Edilmesi Gereken Hususlara İlişkin Duyuru**.

⁷⁵⁵ Hague Conference on Private International Law, Convention Abolishing the Requirement of Legalisation for Foreign Public Documents, 05.10.1961, (çevrimiçi), <https://assets.hcch.net/docs/b12ad529-5f75-411b-b523-8eebe86613c0.pdf>, 30.03.2021.

4. Yabancı dildeki belgelerin noter onaylı çevirisi bulunmalıdır.

5. Kurum tarafından yayımlanan şablon taahhütname örneklerinde yer verilen hükümlere asgari olarak aynen yer verilmeli, ilave hükümlere ihtiyaç olduğunda “İlave Hükümler” başlığı altında bu hükümlere ayrıca yer verilmelidir.

6. Taahhütnamede yer alan taahhüt içeren cümlelerde gelecek zaman kullanılmalıdır.

(2) Esasa İlişkin Dikkat Edilmesi Gereken Hususlar

Taahhütnameler düzenlenirken esasa ilişkin aşağıdaki hususlara yer verilmelidir⁷⁵⁶:

1. Taraflar arasındaki ilişki doğru bir şekilde belirlenmeli ve alıcı tarafın niteliğine uygun taahhütname hazırlanmalıdır. Tarafların hukuki statülerine (veri sorumlusu veya veri işleyen) ilişkin detaylı açıklamaya yer verilmeli ve taraflar arasındaki ilişkiyi gösteren tevsik edici belgeler bulunması hâlinde taahhütnameye eklenmesi gerekmektedir.

2. Taahhütname hazırlanırken Kurum tarafından yayınlanan şablonlarda yer alan hükümlerin aynısına yer verilmeli, ilave hükümlere yer verilecek olması durumunda ise, bu hükümlere “İlave Hükümler” başlığı altında ayrıca yer verilmelidir.

3. Kanunda yer alan terminoloji aynen kullanılmalı, yapılacak tanımlar mevzuatta yer alan tanımlarla uyumlu olmalıdır.

4. Hangi veri konusu kişi grubunun, hangi kişisel verilerinin, hangi amaca ve hukuki sebebe bağlı olarak aktarılacağı hususu söz konusu başlıklar arasında bağ kurulmak suretiyle anlaşılır detayda açıklanmalıdır.

5. İlgili kişinin açık rızası bulunduğu takdirde aktarım, taahhütname konusu edilmemelidir.

⁷⁵⁶ Kişisel Verileri Koruma Kurumu, **Yurt Dışına Kişisel Veri Aktarımında Hazırlanacak Taahhütnamelerde Dikkat Edilmesi Gereken Hususlara İlişkin Duyuru**.

6. Taahhütname hazırlanırken kanunda yer alan genel veri işleme ilkelerinin gözetilmesi gerekmektedir.

7. Yukarıda belirtilenlerin yanı sıra taahhütname örneklerine eklenen Ek-1’de yer alan başlıklar (örneğin; veri konusu kişi grubu ve grupları, veri kategorileri, veri aktarımının amaçları, veri aktarımının hukuki sebebi, alıcı ve alıcı grupları, veri alıcısı tarafından alınacak teknik ve idari tedbirler, irtibat kişisi iletişim bilgileri, ek faydalı bilgiler vs.)⁷⁵⁷ altında yer verilen hususlara da dikkat edilmesi gerekmektedir.

c. Taahhütnamelerde Yer Alması Gereken Asgari Yükümlülükler

Yurt dışına veri aktarımına ilişkin taahhütnameler, Türkiye’deki veri sorumlusu ile aktarım yapılacak olan tarafın niteliğine, başka bir deyişle veri sorumlusu veya veri işleyen sıfatlarına göre ayrı ayrı düzenlenmelidir⁷⁵⁸. Tarafların, kişisel verilerin korunması adına yeterli korumayı tesis edeceklerini asgari olarak şablon sözleşme hükümlerini içerecek şekilde taahhüt etmeleri gerekmektedir⁷⁵⁹.

Türkiye’de yerleşik veri sorumlusundan yabancı ülkede yerleşik veri sorumlusuna yapılacak aktarımlara ilişkin taahhütname örneğinde Türkiye’deki veri sorumlusu “veri aktaran”, yabancı ülkedeki veri sorumlusu ise “veri alıcısı” olarak ifade edilmiştir⁷⁶⁰. Bu taahhütname kapsamında veri aktaranın taahhüt ettiği hususlar aşağıdaki şekildedir⁷⁶¹:

- Kişisel verileri, KVKK ve ilgili diğer mevzuata uygun aktarmak,
- her türlü teknik ve idari tedbirleri almak ve veri alıcısının da taahhütname yükümlülüklerini yerine getirebilecek teknik ve idari yeterliliğe sahip olduğundan emin olmak,
- kişisel verilerin KVKK ve sözleşme hükümlerine uygun şekilde işleneceğine dair veri alıcısını bilgilendirmek,
- tabi olduğu ilgili mevzuat hakkında veri alıcısına bilgi vermek,

⁷⁵⁷ Bkz.: Kişisel Verileri Koruma Kurumu, **Veri Sorumlusundan Veri Sorumlusuna Aktarım**, s. 6-7; Kişisel Verileri Koruma Kurumu, **Veri Sorumlusundan Veri İşleyene Aktarım**, s. 6-7.

⁷⁵⁸ Ünsal Özden/ Uz/ Karamustafaoğlu, s. 22.

⁷⁵⁹ Çelik, s. 93.

⁷⁶⁰ Kişisel Verileri Koruma Kurumu, Veri Sorumlusundan Veri Sorumlusuna Aktarım, s. 3, (çevrimiçi), <https://www.kvkk.gov.tr/SharedFolderServer/CMSFiles/9243078f-3a85-4f02-ae4b-e9b18048f43f.doc>, 25.05.2021.

⁷⁶¹ Kişisel Verileri Koruma Kurumu, **Veri Sorumlusundan Veri Sorumlusuna Aktarım**, m.1, s. 3-4.

- aktarılan kişisel verilerin, kanuni olmayan yollarla elde edilmesi hâlinde veri aktaranı bilgilendirmesi gerektiğine dair veri alıcısına bilgi vermek,
- sözleşme hükümlerinin ihlali hâlinde, söz konusu ihlal ortadan kaldırılana kadar aktarımı askıya almak veya sözleşmeyi feshetmek; bu durumla ilgili bilgileri ve veri alıcısından aldığı bildirimleri Kurul'a bildirmek.

Aynı taahhütname kapsamında veri alıcısının taahhüt ettiği hususlar aşağıdaki şekildedir⁷⁶²:

- Kişisel verilerin güvenliği açısından her türlü teknik ve idari tedbirleri almak, sözleşmeden doğan yükümlülüklerini yerine getirebilecek idari ve teknik yeterliliğe sahip olduğunu kabul etmek,
- kişisel verilerin veri alıcısı adına başka bir gerçek veya tüzel kişi tarafından işlenmesi hâlinde, belirtilen idari ve teknik tedbirlerin alınması hususunda veri işleyenle birlikte müştereken sorumlu olmak,
- kişisel verileri KVKK ve veri aktaranla arasındaki sözleşmeye uygun olarak işlemek, sözleşmeye aykırı herhangi bir ulusal düzenleme olmadığını beyan etmek, herhangi bir sebeple Kanuna ve sözleşmeye uygunluk sağlanamazsa veya sözleşmede yer alan taahhütlerini yerine getirmesini etkilemesi muhtemel bir mevzuat değişikliği yapılırsa veri aktaranı derhâl bilgilendirmek ve böyle durumlarda veri aktaranın aktarımı askıya alma ve sözleşmeyi feshetme hakkına sahip olacağını kabul etmek,
- kişisel verilere ilişkin adli bir makamdan gelen talepleri derhâl veri aktarana bildirmek,
- veri aktarandan gelen soruları en kısa sürede cevaplandırmak ve aktarıma konu kişisel verilerin işlenmesine ilişkin Kurul'un karar ve görüşlerine uymak,
- veri aktaranın denetim yapma ve yaptırma yetkisini kabul etmek ve bu yönde kolaylık sağlamak,
- sözleşmenin feshedilmesi veya sona ermesi durumunda, aktarıma konu kişisel verilerin yedekleri ile birlikte veri aktarana geri göndermek veya

⁷⁶² Kişisel Verileri Koruma Kurumu, **Veri Sorumlusundan Veri Sorumlusuna Aktarım**, m.2, s. 4-5.

tamamen yok etmek, mevzuatta bunu engelleyen hüküm varsa, kişisel verilerin gizliliğini güvence altına almak için her türlü teknik ve idari tedbirler alacağını ve veri işlemeyi durduracağını kabul etmek,

- kişisel verileri alt işverene aktarması gereken durumlarda veri aktaranı ispat edilebilir şekilde bilgilendirmek ve onayını almak.

Türkiye’de yerleşik veri sorumlusundan yabancı ülkede yerleşik veri işleyene yapılacak aktarımlara ilişkin Kurum’un yayınladığı taahhütname örneğinde yer alan yükümlülüklerin büyük bir kısmı veri sorumlusundan veri sorumlusuna aktarıma ilişkin taahhütname örneğindeki yükümlülükler ile ortaktır⁷⁶³. Bununla birlikte yurt dışında bulunan tarafın veri işleyen olduğu durumlarda veri sorumlusunun, aktarılan verileri sadece kendisi adına ve KVKK ile sözleşme hükümlerine uygun işlemesi yönünde veri işleyene talimat vereceği düzenlenmiştir⁷⁶⁴. Bunun karşılığında veri işleyenin de veri sorumlusu adına ve onun talimatlarına uygun şekilde veri işleyeceğini ve bunun sağlanamadığı durumlarda veri sorumlusunu bilgilendireceğini taahhüt ettiği düzenlenmiştir⁷⁶⁵.

Her iki taahhütname örneğinde veri aktaran ile veri alıcısının, işledikleri kişisel verileri KVKK hükümlerine aykırı olarak başkasına açıklaması veya işleme amacı dışında kullanması yasaklanmış ve bu yükümlülük herhangi bir süreyle sınırlandırılmamıştır⁷⁶⁶.

2. Bağlayıcı Şirket Kuralları

Yukarıda da bahsedildiği üzere, uzun yıllar yeterli korumanın bulunmadığı ülkelere yapılan aktarımlar açısından tek yol, yazılı taahhütname olarak kalmaktaydı. Fakat Kurul’un taahhütname başvurularını kabul etme konusunda çekimser davranması, veri sorumlularını ya hukuka aykırı veri aktarımı gerçekleştirmeye ya da ilgili kişiden açık rıza almaya mecbur bırakmıştır⁷⁶⁷. Nitekim “Amazon Turkey” kararında da Kurul, Amazon şirketinin taahhütname

⁷⁶³ Çelik, s. 97.

⁷⁶⁴ Kişisel Verileri Koruma Kurumu, **Veri Sorumlusundan Veri İşleyene Aktarım**, m.1/d, s. 3.

⁷⁶⁵ Kişisel Verileri Koruma Kurumu, **Veri Sorumlusundan Veri İşleyene Aktarım**, m.2/b, s. 4.

⁷⁶⁶ Kişisel Verileri Koruma Kurumu, **Veri Sorumlusundan Veri İşleyene Aktarım**, m.3/b-c, s. 5; Kişisel Verileri Koruma Kurumu, **Veri Sorumlusundan Veri Sorumlusuna Aktarım**, m.3/a-b, s. 5.

⁷⁶⁷ Altınağ, s. 124.

başvurularıyla ilgili henüz bir karar verilmediğini ve yeterli korumaya sahip ülkelerin de henüz belirlenmediğini belirterek kişisel verilerin yurt dışına aktarılmasının tek yolunun ilgili kişiden açık rıza almak olduğunu açıkça ifade etmiştir⁷⁶⁸. Bu durum her ne kadar gerçek kişiler veya küçük işletmeler için mümkün görünse de, büyük şirketler açısından her gün gerçekleştirilen binlerce veri aktarımının her biri için açık rıza alınması olağan dışı bir durum ortaya çıkarmıştır⁷⁶⁹. Ayrıca taahhütnameler, genelde aralarında organik bağ bulunmayan şirketler arasında gerçekleştirilecek iki taraflı veri aktarımlarını kolaylaştırırsa da çok uluslu şirket toplulukları arasında yapılacak veri aktarımları bakımından yetersiz kalması nedeniyle, Kurul tarafından yayımlanan bir duyuru⁷⁷⁰ ile çok uluslu şirketler arasında gerçekleştirilecek veri aktarımlarında kullanılmak üzere pratik bir yöntem olarak “bağlayıcı şirket kuralları” uygulamaya koyulmuştur⁷⁷¹. Nitekim ilgili duyuruda 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 kuralları”* olarak nitelendirilmiştir⁷⁷².

Bağlayıcı Şirket Kuralları Başvuru Formu’nda yer verilen tanımdan anlaşıldığı üzere, bağlayıcı şirket kuralları; şirketler topluluğuna bağlı olarak Türkiye’de yerleşik bir veri sorumlusundan, 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 için kullanılabilir⁷⁷³. Dolayısıyla, bağlayıcı şirket kuralları kapsamında belirtilen

⁷⁶⁸ Kaya, **Elektronik Ticaret**, s. 150-151; Çelik, s. 51.

⁷⁶⁹ Dülger, **108 sayılı Sözleşme**, s. 5; Murat Volkan Dülger/ Cansu Ceren Kahraman, “KVKK’dan Kişisel Verilerin Yurt Dışına Aktarımında Önemli Bir Adım: Bağlayıcı Şirket Kuralları”, s. 1, (çevrimiçi), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3792375, 23.05.2021; Altındağ, s. 125; Sertçe, s. 116, 128.

⁷⁷⁰ Bkz.: Kişisel Verileri Koruma Kurumu, Bağlayıcı Şirket Kuralları Hakkında Duyuru, 10.04.2020, (çevrimiçi), <https://www.kvkk.gov.tr/icerik/6728/yurt-disina-kisisel-veri-aktariminda-baglayici-sirket-kurallari-hakkinda-duyuru>, 28.10.2021.

⁷⁷¹ Ünsal Özden/ Uz/ Karamustafaoğlu, s. 23; Öztürk/ Altınok Çalışkan/ Seyhan, s. 81; Çelik, s. 101.

⁷⁷² Kişisel Verileri Koruma Kurumu, **Bağlayıcı Şirket Kuralları Hakkında Duyuru**.

⁷⁷³ Kişisel Verileri Koruma Kurumu, Veri Sorumluları İçin Bağlayıcı Şirket Kuralları Başvuru Formu, s. 4, (çevrimiçi), <https://www.kvkk.gov.tr/SharedFolderServer/CMSFiles/0aa5e8ce-8e4e-403c-a444-7212f581ad23.docx>, 26.03.2021; Kişisel Verileri Koruma Kurumu, Veri Sorumluları İçin Bağlayıcı

yükümlülükler, veri sorumlusu olan grup üyelerinin yanı sıra grup içindeki faaliyetlere veri işleyen olarak dâhil olan kişiler için de geçerlidir⁷⁷⁴. Bağlayıcılığın sağlanması amacıyla bağlayıcı şirket kuralları kapsamında yer alacak veri sorumlusu ile veri işleyen arasında bir hizmet sözleşme düzenlenmeli ve bütün veri işleyenler tarafından imzalanmalıdır⁷⁷⁵.

Taahhütname örneklerinde olduğu gibi bağlayıcı şirket kuralları da Kurul iznine tabidir⁷⁷⁶. Söz konusu iznin alınabilmesi için Türkiye’de yerleşik merkezi bulunan grup üyesi; Türkiye’de yerleşik merkezi bulunmadığı takdirde ise bu amaçla yetkilendirilen Türkiye’de yerleşik bir grup üyesi ilgili formu doldurarak Kurum’a bağlayıcı şirket kuralları başvurusunda bulunmalıdır⁷⁷⁷.

Başvuru yapmaya yetkili kişi, başvuru formu ile birlikte bağlayıcı şirket kuralları metnini ve başvuruya ilgili tüm bilgi ve belgeleri de elden veya posta yoluyla Kurul’a sunmalıdır. Başvuruda asgari olarak aşağıdaki hususlarla ilgili bilgilere yer verilmelidir⁷⁷⁸:

1. Başvurucunun bilgileri (şirketler topluluğu ve başvuru işlemini gerçekleştiren bakımından),

2. Bağlayıcı şirket kurallarına ilişkin bilgiler (bağlayıcılık unsuru, etkili uygulama, kurum ile koordinasyon, kişisel verilerin işlenmesi ve aktarımı, raporlama ve kayıt değişikliği mekanizmaları, veri güvenliği, hesap verilebilirlik ve diğer esaslar/araçlar, yardımcı bilgi ve belgeler).

Kurul, başvuruları resmî başvuru tarihinden itibaren bir yıl içerisinde değerlendirerek karara varır. Gerektiği takdirde bu süre, altı aylık sürelerle uzatılabilir⁷⁷⁹. Başvuru Kurul tarafından onaylanırsa, bu durum Kurum tarafından

Şirket Kurallarında Bulunması Gereken Temel Hususlara İlişkin Yardımcı Doküman, s. 4, (çevrimiçi) <https://www.kvkk.gov.tr/SharedFolderServer/CMSFiles/62fb06e5-d623-404d-b3a1-c492891a3bbb.docx>, 26.03.2021; Çelik, s. 101.

⁷⁷⁴ Kişisel Verileri Koruma Kurumu, **BŞK Yardımcı Doküman**, s. 4

⁷⁷⁵ Kişisel Verileri Koruma Kurumu, **BŞK Başvuru Formu**, s. 3.

⁷⁷⁶ Çelik, s. 103.

⁷⁷⁷ Kişisel Verileri Koruma Kurumu, **BŞK Başvuru Formu**, s. 3; Dülger/ Kahraman, **Bağlayıcı Şirket Kuralları**, s. 3.

⁷⁷⁸ Dülger/ Kahraman, **Bağlayıcı Şirket Kuralları**, s. 5.

⁷⁷⁹ Kişisel Verileri Koruma Kurumu, **BŞK Başvuru Formu**, s. 3.

ilgili kişiye bildirilir ve gerekirse ilan edilir. Bu noktada fazlasıyla uzun bir değerlendirme süresinin öngörülmesi ve hangi durumlarda ek süre verileceğinin açıkça belirtilmemiş olmasının uygulamada belirsizliğe ve keyfiyete yol açabileceğine dair görüşe⁷⁸⁰ katılıyoruz. Başvuruların sonuçlanması için süre belirlenmiş olsa da, onaylanmış bağlayıcı şirket kurallarının uygulanması herhangi bir süreyle sınırlandırılmamıştır.

Başvuru formunda yer alan “Genel Hükümler”e göre, grup üyelerinin her biri bağlayıcı şirket kurallarının yorumlanması ve uygulanmasıyla ilgili Kurum’un talimatlarına uygun hareket etmeyi, aktarılan kişisel verileri KVKK’ya ve bağlayıcı şirket kurallarına uygun olarak işlemeyi ve uygunluk sağlanamadığı takdirde derhâl Kurum’a bildirmeyi kabul eder. Bu durumda Kurum, veri aktarımını feshetme veya askıya alma hakkına sahiptir⁷⁸¹.

Grup üyelerinden herhangi birinin grupla bağının kesilmesi, bağlayıcı şirket kurallarının herhangi bir şekilde sona ermesi hâlinde, aktarıma konu olan kişisel veriler yedekleri ile birlikte Türkiye’de yerleşik merkeze veya yetkili grup üyesine gönderilmeli ve yok edilmelidir. Ulusal mevzuatta bu yükümlülüğün yerine getirilmesini engelleyen hüküm mevcutsa verilerin güvenliğini sağlamak için gerekli teknik ve idari tedbirler alınarak işleme faaliyeti sınırlandırılmalıdır⁷⁸².

Grup üyeleri, aktarıma faaliyeti sonucunda elde ettikleri kişisel verileri kanuna aykırı olarak başkasına açıklayamaz ve işleme amacı dışında kullanamaz. Aktarılan veriler, kanuni olmayan yollarla başkaları tarafından elde edilirse, en kısa sürede Türkiye’de yerleşik merkeze veya yetkili grup üyesine, bunlar aracılığıyla ise Kurul’a durumla ilgili bilgilendirme yapılmalıdır.

Şunu da belirtmek gerekir ki bağlayıcı şirket kuralları sadece grup içerisinde ve grup üyeleri arasındaki aktarımlar için geçerlidir. Bu durumda Türkiye’de yerleşik olmayan grup üyesinden, grup üyesi olmayan bir şirkete veri aktarımı (ileri aktarım) yapılması gerekirse “taahhütnameler”in kullanılması gerekecektir.

⁷⁸⁰ Çelik, s. 104.

⁷⁸¹ Kişisel Verileri Koruma Kurumu, **BŞK Başvuru Formu**, s. 15.

⁷⁸² Kişisel Verileri Koruma Kurumu, **BŞK Başvuru Formu**, s. 16.

D. Yurt Dışına Veri Aktarımında 108 Sayılı Sözleşme'nin Yeri

Daha önce belirtildiği üzere kişisel verilerin yurt dışına aktarılması açısından teoride birçok yöntem mevcut olsa da, pratikte bu yöntemlerin uygulanmasıyla ilgili yaşanan zorluklar nedeniyle (güvenli ülkeler listesinin belirlenmemiş olması, Kurul'un yazılı taahhütnamelere geç geri dönüş yapması, bağlayıcı şirket kurallarının yeni kabul edilmiş olması vs.) başka çözüm yolları aranmaktadır⁷⁸³. Bu kapsamda 108 sayılı Sözleşme'nin de yurt dışına veri aktarımına tek başına hukuki dayanak teşkil edip etmeyeceğine dair tartışmalar gündeme gelmektedir.

Sözleşme'nin 12. maddesinde; sözleşmeye taraf olan bir ülkenin, sözleşmeye taraf olan diğer bir ülkeye kişisel veri aktarımını yalnızca özel yaşamın korunması gerekçesiyle yasaklayamayacağı veya özel izne tabi tutamayacağı belirtilmiştir. Bununla birlikte, sözleşmeye taraf olan ülkelerin iç hukukunda, belli kişisel veri kategorileri veya otomatik işleme tabi tutulmuş kişisel veri dosyaları için söz konusu verilerin veya dosyaların doğasından kaynaklanan özel düzenlemelerin öngörülmesine rağmen, diğer tarafın düzenlemelerinin eşdeğer bir koruma içermediği durumlarda (m.12/f.3/a) veya sözleşmeye taraf olan ülkelere birinin, diğer ülkenin iç hukukundaki boşluktan yararlanarak sözleşmeye taraf olmayan bir ülkeye yaptığı aktarımı engellemek amacıyla (m.12/f.3/b) yukarıdaki hükme istisna getirilebilir.

KVKK m.9/f.5'te yer alan “...uluslararası sözleşmeler saklı kalmak üzere...” ifadesinin lafzi yorumundan da anlaşıldığı üzere, kanunda uluslararası sözleşmelerin kişisel veri aktarımlarına hukuki dayanak teşkil etmesi imkânı kabul edilmiştir. Bu bakımdan, 108 sayılı Sözleşme m.12/f.3'te belirtilen istisnalar kapsamında herhangi bir sınırlandırma veya özel izne tabi tutulmaya ilişkin Türkiye tarafından yapılan herhangi bir işlem bulunmadığı; aynı zamanda Anayasa m.90/f.5 uyarınca, temel hak ve özgürlüklere ilişkin bir sözleşme olması nedeniyle ulusal kanunlarla çelişen hükümler içermesi hâlinde 108 sayılı Sözleşme hükümlerinin esas alınması gerektiği gibi hususlar dikkate alındığında, KVKK m.9'da belirtilen koşullar aranmaksızın Sözleşme'ye taraf olan ülkelere veri aktarımı gerçekleştirmenin önünde hukuki bir

⁷⁸³ Dülger, 108 sayılı Sözleşme, s. 6.

engel bulunmadığı şeklinde bir yorum ortaya çıkmaktadır⁷⁸⁴. Ne var ki Kurul bu yönde farklı bir karar vererek 108 sayılı Sözleşme'nin yurt dışına kişisel veri aktarımlarına tek başına dayanak teşkil etmeyeceğini ifade etmiştir⁷⁸⁵.

Kurul söz konusu kararında; 108 sayılı Sözleşme'nin ilgili hükmünün yalnızca özel hayatın korunması gerekçesiyle yapılan sınırlandırmalara ilişkin olduğunu, "108 sayılı Sözleşme'ye ilişkin Açıklayıcı Rapor"⁷⁸⁶ (Açıklayıcı Rapor) göre bu düzenlemenin, sözleşmeye taraf ülkeler arasında veri akışını kolaylaştırmak amacı taşıdığını ve bu hükmün, sözleşmeye taraf ülkeler arasındaki veri aktarımlarının bildirim tabi tutulmasına veya belirli durumlarda yasaklanmasına yönelik düzenlemeler yapma imkânını ortadan kaldırmadığını hatırlatarak, KVKK m.9 ile öngörülen kişisel veri aktarım rejiminin 108 sayılı Sözleşme ile uyumlu olduğuna kanaat getirmiştir⁷⁸⁷. KVKK m.9 ile getirilen yurt dışına veri aktarımlarına ilişkin sınırlandırmaların 108 sayılı Sözleşme ile uyumlu olduğunun belirtilmesine karşın, söz konusu sınırlandırmaların Sözleşme'nin 12. maddesi uyarınca hangi istisnaya dayandığına dair açıklama yapılmaması ise doktrinde eleştirilmiştir⁷⁸⁸.

Kurul, Anayasa m.90/f.5 hükmü bağlamında yaptığı açıklamada ise; söz konusu düzenlemenin uygulama alanı bulabilmesi için uluslararası sözleşme hükümlerinin doğrudan uygulanabilir olması, yani yeterince açık, kesin, koşulsuz ve uygulaması için ilave bir tedbir alınmasını gerektirmeyecek nitelikte olması gerektiğini, doğrudan uygulanabilir olmayan daha soyut ve genel nitelikli bir uluslararası sözleşme hükmü ile bir kanun hükmü arasında oluşan uyumsuzluğun Anayasa m.90/f.5 kapsamında değerlendirilmeyeceğini, dolayısıyla genel nitelikli uluslararası sözleşme hükmü ile kanun hükmünün çelişmesi hâlinde, çelişen kanun

⁷⁸⁴ Bkz.: Kurul'un 22.07.2020 tarihli ve 2020/559 sayılı kararında, veri sorumlusundan alınan savunma yazısının özeti; Dülger, **108 sayılı Sözleşme**, s. 7; Çelik, s. 59.

⁷⁸⁵ Bkz.: Kişisel Verileri Koruma Kurulu, 22.07.2020 tarihli ve 2020/559 sayılı kararı, (çevrimiçi), <https://kvkk.gov.tr/Icerik/6790/2020-559>, 28.10.2021.

⁷⁸⁶ Council of Europe, Explanatory Report to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, 28.01.1981, s. 12, (çevrimiçi), <https://rm.coe.int/16800ca434>, 26.10.2021.

⁷⁸⁷ Kişisel Verileri Koruma Kurulu, 22.07.2020 tarihli ve 2020/559 sayılı karar; Kurum'un aynı yönde açıklaması için bkz.: Kişisel Verileri Koruma Kurulu, **Yurt Dışına Veri Aktarımı Kamuoyu Duyurusu**.

⁷⁸⁸ Çelik, s. 60.

hükümlerinin esas alınması gerektiğini ifade etmiştir⁷⁸⁹. 108 sayılı Sözleşme m.4/f.1 hükmünden⁷⁹⁰ Sözleşme hükümlerinin taraf devletlerin iç hukukunda doğrudan hüküm ve sonuç doğurmadığı, sadece ulusal veri koruma düzenlemelerine hakim olması gereken temel ilkeleri ve ilgili kişilere sağlanacak güvenceye ilişkin usul ve esasları belirlediği anlaşılmaktadır. Nitekim Açıklayıcı Rapor’da da, Sözleşme’nin doğrudan uygulanabilir nitelikte olmadığı ve bu nedenle taraf devletlerin, veri koruma hükümlerini iç hukuklarına dahil etmekle yükümlü kılındıkları belirtilmiştir. Bu bulgular ışığında Kurul, doğrudan uygulanabilir nitelikte olmayan 108 sayılı Sözleşme’nin 12. maddesinde yer alan hükmün öncelikle uygulanmayacağına ve KVKK m.9 ile öngörülen düzenlemenin 108 sayılı Sözleşme m.12’ye aykırı olmadığına, aksine her iki düzenlemenin birbirini tamamlayıcı nitelikte olduğuna karar vermiştir⁷⁹¹.

Söz konusu kararla ilgili doktrindeki bir görüş⁷⁹² yurt dışına aktarıma ilişkin KVKK m.9 hükümlerinin, 108 sayılı Sözleşme ve 181 sayılı Ek Protokol ile çatışmadığı ve ona uygun olarak yorumlanıp uygulandığı durumda uygulama alanı bulacağını, aksi takdirde çıkan uyuşmazlıklarda Anayasa m.90/f.5 uyarınca, 108 sayılı Sözleşme ve 181 sayılı Ek Protokol’ün esas alınacağını ifade etmektedir. Dolayısıyla, 108 sayılı Sözleşme’ye taraf olan ülkelere yapılacak aktarımlar yasaklanmamalı, Sözleşme’ye aykırı şekilde sınırlandırılmamalı ve KVKK m.9’a uygun olmadığı gerekçesiyle hukuka aykırı olarak kabul edilip engellenmemelidir⁷⁹³.

Başka bir görüş⁷⁹⁴ ise 108 sayılı Sözleşme’nin, Anayasa m.90/f.5 uyarınca *“usule uygun şekilde yürürlüğe giren temel hak ve özgürlüklere ilişkin bir milletlerarası antlaşma”* olma şartını karşıladığını kabul etmekle birlikte⁷⁹⁵, Sözleşme’nin 12. maddesinde öngörülen düzenlemenin yalnızca özel hayatın

⁷⁸⁹ Kişisel Verileri Koruma Kurulu, 22.07.2020 tarihli ve 2020/559 sayılı karar.

⁷⁹⁰ “Her bir Taraf, kendi iç hukukunda bu bölümde yer alan verilerin korunmasına ilişkin temel ilkelere işlerlik kazandırmak amacıyla gerekli önlemleri alır” (108 sayılı Sözleşme m.4/f.1).

⁷⁹¹ Kişisel Verileri Koruma Kurulu, 22.07.2020 tarihli ve 2020/559 sayılı karar.

⁷⁹² Akçalı Gür, s.867; Bilgi Information Technology Law Institute, s. 56-57; Pelen, s. 1730.

⁷⁹³ Bilgi Information Technology Law Institute, s. 58.

⁷⁹⁴ Dülger, **108 sayılı Sözleşme**, s. 14-15; Çelik, s.61-62.

⁷⁹⁵ Dülger’e göre, Kurul’un herhangi bir başkaca mahkeme kararı veya doktrin görüşlerine dayanmadan Anayasa m.90 hükmünü ve gerekçelerini yorumlaması isabetli olmamıştır. Bkz.: Dülger, **108 sayılı Sözleşme**, s. 12-13.

korunması gerekçesiyle yapılan aktarımlara ilişkin olduğu ve Sözleşme'nin aktarıma ilişkin hükümlerinin genel ve soyut nitelikli olması nedeniyle KVKK m.9 ile aralarında bir çatışma oluşmayacağı yönünde Kurul'un vardığı kanaate katılmaktadır.

Bu hususta ikinci görüşü daha isabetli bulduğumuzu, KVKK m.9 hükmü ile 108 sayılı Sözleşme m.12 hükmünün birbirini tamamlayıcı nitelikte olduğu ve bu bağlamda iki düzenleme arasında bir çatışma olmadığı yönündeki yoruma katıldığımızı belirtmek isteriz.

Her ne kadar 108 sayılı Sözleşme yurt dışına yapılan veri aktarımları için tek başına hukuki gerekçe oluşturmaya da, tamamen göz ardı edilmeyeceği de kararda belirtilmiştir⁷⁹⁶. Şöyle ki, KVKK m.9/f.4 uyarınca Kurul'un aktarıma izin verip vermeyeceğine ilişkin değerlendirmede dikkate alacağı kriterlerden biri de Türkiye'nin taraf olduğu uluslararası sözleşmelerdir. Bu bağlamda verilerin aktarılacağı ülkenin 108 sayılı Sözleşme'ye taraf olmasının Kurul'un değerlendirmesine esas teşkil edecek unsurlardan biri olduğu anlaşılmaktadır⁷⁹⁷. Nitekim yeterli korumanın bulunduğu ülkelerin Kurulca belirlenmesinde kullanılmak üzere Kurul'un 02/05/2019 tarihli ve 2019/125 kararı ile kabul edilen kriterler arasında 108 sayılı Sözleşme de yer almaktadır.

E. Kişisel Verilerin Yurt Dışına Aktarılmasına Dair Türk ve Avrupa Birliği Hukukundaki Yaklaşımların Karşılaştırılması

KVKK, AB mevzuatı örnek alınarak hazırlanmış olsa da, Kanun'da AB hukukundan farklı birçok düzenleme bulunmaktadır⁷⁹⁸. Özellikle, kişisel verilerin yurt dışına aktarılması açısından mevcut olan farklar nispeten daha fazladır. Örneğin, verilerin Birlik dışına aktarılmasına ilişkin GDPR hükümlerinde; kişisel verilerin uluslararası kuruluşlara aktarılması, ileri aktarımlar gibi hususlara yer verilse de, KVKK'da bunlarla ilgili duruma açıklık getirilmemiştir.

⁷⁹⁶ Bkz.: Kişisel Verileri Koruma Kurulu, 22.07.2020 tarihli ve 2020/559 sayılı karar.

⁷⁹⁷ Kişisel Verileri Koruma Kurumu, **Yurt Dışına Veri Aktarımı Kamuoyu Duyurusu**; Kişisel Verileri Koruma Kurumu, **Doğru Bilinen Yanlılar 2**, s. 30.

⁷⁹⁸ Sertçe, s. 136.

Yine KVKK'da yabancı ülkenin tamamının yeterli korumayı sağlayıp sağlamadığı dikkate alınırken, GDPR'da yeterlilik kararlarının kapsamı üçüncü ülke dâhilindeki bir bölge veya belli bir sektörü de içerecek şekilde genişletilmiştir. Ayrıca, yeterli koruma sağlamayan ülkelere veri aktarımı gerçekleştirmek için GDPR'da çok sayıda alternatif öngörülmüş ve bunlardan sadece ikisi için (özel sözleşme hükümleri ve kamu kuruluşları arasındaki idari düzenlemelere eklenecek uygulanabilir hükümler) veri koruma otoritelerinin onayı aransa da, söz konusu aktarım imkânlarından yalnızca biri - veri sorumlularının yeterli korumayı yazılı olarak taahhüt etmesi - KVKK'da öngörülmüş, daha sonra yayınlanan bir duyuru ile bağlayıcı şirket kuralları da Kurum tarafından kabul edilmiştir. Hem yazılı taahhütnamelere hem de bağlayıcı şirket kurallarına dayalı aktarımlar Kurul'un izne tabi tutulmuştur⁷⁹⁹. Sonuç olarak, açık rıza ve uluslararası sözleşmelere dayalı aktarımlar dışında bütün aktarımlar sadece Kurul'un kontrolü dâhilinde gerçekleştirilebilecektir.

Bu iki hukuk sistemi arasında kişisel verilerin aktarılmasına ilişkin basit düzenleme farklarından ziyade, genel bir yaklaşım farkı söz konusudur. Şöyle ki, kişisel verilerin yurt dışına aktarımını belirli şartlara bağlı olarak sınırlayan düzenlemeler içerisinde temel olarak iki farklı eğilim bulunmaktadır. Bunlardan birincisi kişisel verilerin yurt dışına aktarımını, ilgili kişinin iznine bağlı tuturak yurt dışına çıkan kişisel verilerin akıbeti ile ilgilenmeme yönünde politika izlemektir⁸⁰⁰. İkinci ise ilgili kişilerin rolünü mümkün olduğu kadar azaltarak kişisel verilerin yurt dışına aktarımını hukuki sınırlamalara tabi kılmak ve veriler üzerindeki denetimin, bağlayıcı yükümlülükler sayesinde verilerin aktarılacağı ülkede de devam ettirilmesidir⁸⁰¹.

Türkiye ve AB'nin konuya ilişkin mevzuatına bakıldığında, Türkiye'nin birinci, AB'nin ise ikinci politikayı benimsediği anlaşılmaktadır. Zira GDPR'da kişisel verilerin aktarılması açısından açık rızanın kullanım imkânı oldukça kısıtlıdır. Şöyle ki, açık rıza diğer kişisel veri aktarma mekanizmalarının (yeterlilik kararı,

⁷⁹⁹ Erarslan, **Verilerin Aktarılması**, s. 110; Sertçe, s. 139.

⁸⁰⁰ Aşıkoğlu/ Uzun, s. 933.

⁸⁰¹ Aşıkoğlu/ Uzun, a.y.

güvenli önlemlerin sağlanması) bulunmadığı zamanlarda başvurulabilecek istisnalardan sadece biri olarak öngörülmüştür. AB'nin, üye ülkeler dışında 14 ülkeyle ilgili yeterlilik kararı bulunduğu, bu kararların olmadığı durumlar için madde 46'da birçok güvenlik önlemi öngörüldüğü göz önünde bulundurulduğunda gerçekten de kişisel verilerin AB'den üçüncü bir ülkeye aktarılması için ilgili kişinin açık rızasına nadiren ihtiyaç duyulacaktır. Ayrıca, GDPR'da öngörülen Birlik dışına kişisel veri aktarımı imkânlarının hemen hemen tamamı, veri alıcısının GDPR'a yani AB düzenleme ve denetimine tabi olmasını sağlamaktadır⁸⁰². Dolayısıyla AB'nin ilgili kişinin izni yerine veri akışını engellemeden kişisel verilerin korunmasına yönelik bir politikayı takip ettiği ve bu kapsamda kendi hukuk kurallarını diğer ülkelere ihraç etme amacı güttüğü sonucuna varmak mümkündür⁸⁰³.

Bunun aksine Türk hukukunda kişisel verilerin aktarılması açısından ilgili kişinin iznine büyük önem verildiği gözlemlenmektedir⁸⁰⁴. Şöyle ki, kişisel verilerin yurt dışına aktarılması, ilgili kişinin açık rızasına bağlı kılınmıştır. Açık rıza olmadan veri aktarım imkânları ise Kanun'da tahdidi olarak sayılmıştır. Başka bir deyişle, AB'nin aksine Türk hukukunda kişisel verilerin aktarılması bağlamında açık rızanın varlığı kural, olmadığı durumlar ise istisna olarak düzenlenmiştir⁸⁰⁵. Ayrıca GDPR'da açık rızaya ilişkin daha sıkı şartlar (hem rızanın niteliğine ilişkin: rızanın unsurları, rızanın geri alınabilir olması, hizmet sağlanması için ön şart olmaması vs.; hem de uygulanmasına ilişkin: aktarım için gerekli olması, aktarımın tekrarlayan olmaması) öngörülse de, Türk hukukundaki düzenlemeler açık rızanın kullanım imkânlarının önünü açmaya yöneliktir.

Her ne kadar Kurum tarafından yapılan açıklamalarda, açık rızanın diğer hukuka uygunluk sebepleri karşısında bir üstünlüğü bulunmadığı belirtilse de, diğer hukuki uygunluk sebepleri kişisel veri aktarımı için tek başına yeterli olmayıp, ilave şartların bulunması (yeterli korumanın bulunması, yazılı taahhütnameler) gerekmektedir. Hâlbuki ilgili kişinin açık rızasını ifade etmesi, kişisel verilerinin

⁸⁰² Aşıkoğlu/ Uzun, s. 935.

⁸⁰³ Aşıkoğlu/ Uzun, a.y.

⁸⁰⁴ Aşıkoğlu/ Uzun, s. 934; Bilgi Information Technology Law Institute, **Veri Aktarım Raporu**, s. 110.

⁸⁰⁵ Dülger, **Kişisel Veriler**, s. 226; Kızılırmak, **Yurt Dışına Aktarım**.

aktarılması için yeterlidir. Hatta açık rızaya dayalı aktarımların Kurul iznine konu edilmeyeceği Kurum tarafından yayınlanan duyuruda da belirtilmiştir⁸⁰⁶.

Ayrıca, kanun koyucunun konuya yaklaşımı sonucu teoride kural olarak belirlenen açık rıza, Kurul'un sergilediği tutum sonucunda uygulamada da tek yol olarak kalmaktadır. Şöyle ki, kanunda yeterli korumanın bulunması, yazılı taahhütnameler, bağlayıcı şirket kuralları gibi açık rızaya alternatifler öngörülse de, bu çalışma tarihi itibarıyla Kurul tarafından güvenli ülkeler listesinin yayınlanmaması, taahhütnamelerin onaylanmasının uzun bir süreci kapsamaması ve bu zamana kadar çok az sayıda taahhütnamenin onaylanmış olması, bağlayıcı şirket kurallarının henüz yeni kabul edilmiş olması, veri sorumlularına verilerin aktarılması için başka seçenek bırakmamıştır⁸⁰⁷. Bu durumda veri sorumluları ya hukuka aykırı veri aktarımı gerçekleştirmeli ya da her bir aktarım için ilgili kişinin açık rızasını almak zorundadır. Görüldüğü üzere, kişisel verilerin yurt dışına aktarılması açısından, AB hukukunda öngörülen hiyerarşik ve çok katmanlı çağdaş yaklaşımın aksine, Türk hukukunda hayli kısıtlayıcı ve uygulanması neredeyse imkânsız bir düzenlemeye gidilmiştir⁸⁰⁸. Kanaatimizce, KVKK'ya GDPR'da öngörülen alternatif imkânların (kamu kuruluşları veya organları arasında yasal bağlayıcılığı bulunan ve icra edilebilir bir belge, onaylanmış davranış kuralları, onaylanmış belgelendirme mekanizması, kamu kuruluşları ya da organları arasındaki idari düzenlemelere eklenecek olan icra edilebilir ve etkili veri sahibi haklarını kapsayan hükümler vs.) dâhil edilmesi hem veri sorumlularının veri aktarımı faaliyetini kolaylaştıracak hem de Kurul'un iş yükünü hafifletecektir.

Kanaatimizce, kişisel verilerin yurt dışına aktarılmasının sadece ilgili kişinin rızasına dayandırılması, verilerin aktarılacağı ülkedeki akıbetini belirsiz kılmaktadır. Zira rıza tek başına yalnızca işleme meşruluk kazandırmakta olup, verilerin aktarıldığı ülkede korunmasını kendiliğinden sağlamamaktadır⁸⁰⁹. Hâlbuki kişisel verilerin yurt dışına aktarılmasının ayrı düzenlenmesindeki amaç, veriler

⁸⁰⁶ Kişisel Verileri Koruma Kurumu, **Doğru Bilinen Yanlıklar 2**, s. 32; Aşıkoğlu/ Uzun, s. 936; Tepe, s. 72.

⁸⁰⁷ Kızılırmak, **Yurt Dışına Aktarım**; Çelik, s. 160.

⁸⁰⁸ Bilgi Information Technology Law Institute, s. 46, 111.

⁸⁰⁹ Kızılırmak, **Yurt Dışına Aktarım**; Çelik, s. 45.

aktarıldıktan sonra bile eşdeğer korumanın temin edilmesidir. Bu durumda aktarımı yalnızca rızaya bağlamak, sorumluluğu sadece ilgili kişiye yüklemek anlamına gelmektedir⁸¹⁰.



⁸¹⁰ Kızılırmak, **Yurt Dışına Aktarım**.

SONUÇ

Kişisel verilerin aktarılmasına ilişkin hükümler içeren ilk düzenlemeler 1970’li yıllarda çeşitli Avrupa ülkelerinde ulusal düzeyde kabul edilmiştir. 1980’li yıllardan itibaren ise OECD, AK, BM gibi uluslararası kuruluşlar, kişisel verilerin sınır ötesi aktarılmasına yönelik düzenlemelerini kabul etmeye başlamıştır. Bu hususta ilk uluslararası düzenleme, 1980 yılında OECD tarafından kabul edilen “Özel Yaşamın Gizliliğinin ve Sınır Ötesi Kişisel Veri Dolaşımının Korunmasına İlişkin Rehber İlkeler”, ilk bağlayıcı belge ise 1981 yılında AK tarafından kabul edilen 108 sayılı “Kişisel Verilerin Otomatik İşleme Tabi Tutulması Karşısında Bireylerin Korunması Sözleşmesi” olmuştur. Kişisel verilerin korunmasına yönelik AB düzeyinde çalışmalar da 1970’li yıllarda başlasa da, bu hususta kapsamlı bir düzenlemeye gidilmesi, 1995 yılında 95/46/EC sayılı DPD’nin kabul edilmesi ile mümkün olmuştur. 2016 yılında ise 95/46/EC sayılı DPD’nin yerine, üye devletlerde doğrudan uygulanabilecek Genel Veri Koruma Tüzüğü kabul edilmiştir. Türkiye’de ise bu konu, sadece 1990’lı yıllarda tartışma hâline gelmiştir. 2010 yılında yapılan Anayasa değişikliği ile birlikte ilk kez kişisel verileri korunması hakkı Anayasa’da yerini almış olsa da, bu hususta özel bir kanunun kabul edilmesi 2016 yılında gerçekleşmiştir.

Hem Türk hem de AB hukukunda kişisel verilerin aktarılması, kişisel veri işleme faaliyetinin bir türü olarak düzenlenmiştir. Buna rağmen, her iki mevzuatta da kavramın tanımına yer verilmemiştir. Doktrindeki baskın görüşlere göre, üçüncü kişilere yönelik her türlü veri paylaşımı, Türk hukukunda veri aktarımı olarak kabul edilirken, AB hukukunda ise yalnızca üçüncü bir ülkeye veya uluslararası bir kuruluşa aktarılmasının ardından işlenen veya işlenmesi amaçlanan veriler, veri aktarım faaliyeti kapsamında değerlendirilecektir (GDPR m.44). Ayrıca, AB hukukunda kişisel verilerin aktarılması, sadece verilerin Birlik dışına iletilmesini ifade ederken, Birlik sınırları dâhilinde verilerin serbest dolaşımı kabul edilmiştir. Buna karşılık, KVKK’da kişisel verilerin yurt içinde ve yurt dışına aktarılması olarak iki farklı düzenleme öngörülmüştür (KVKK m.8, m.9).

Yurt içinde gerçekleşen bir veri aktarımından bahsedebilmek için, aktarım faaliyeti boyunca veri alıcısının yurt dışında bulunmaması gerekmektedir. Türk hukukunda, veri alıcısının ülke sınırlarının dışında bulunması, yurt dışına aktarımın gerçekleşmiş olması için yeterli kabul edilmektedir. Bunun aksine, kişisel verilerin yurt dışında bulunduğu fakat herhangi bir işleme tabi tutulmadığı süreç, aktarım olarak kabul edilmemektedir. Bunun yerine kişisel verilerin transit geçişi kavramı tercih edilmektedir.

Hem mülga 95/46/EC sayılı DPD’de hem de hâlihazırda yürürlükte olan GDPR’da Avrupa Tek Pazarı’nın gelişimini desteklemek amacıyla, kişisel verilerin AB’ye üye devletler arasında dolaşımı serbest kılınmıştır. Buna göre, kişisel verilerin işlenmesi ile ilgili olarak gerçek kişilerin korunmasına yönelik sebeplerle Birlik içinde kişisel verilerin serbest akışına kısıtlama ve yasaklar getirilmez (GDPR m.1/f.3). Ayrıca, 1993 yılında kabul edilen Avrupa Ekonomik Alanı’na dair anlaşma ile Norveç, İzlanda ve Lihtenştayn gibi ülkeler de verilerin serbest dolaşımı alanına dâhil olmuştur. Kişisel verilerin Birlik dışına aktarılması ise GDPR’ın 5. bölümünde öngörülen belirli kısıtlamalara uymakla gerçekleştirilebilir. Verilerin Birlik dışına aktarılabilmesi için GDPR’da hiyerarşik bir düzenleme öngörülmüştür. Şöyle ki, üçüncü ülkeye veri aktarımı gerçekleştirmek için öncelikle söz konusu ülkenin yeterli korumayı sağlayıp sağlamadığı belirlenmelidir.

GDPR’da değinilmese de ABAD’a göre “yeterli koruma”, AB hukukunun temin ettiği güvencelere temelde eşdeğer korumayı ifade etmektedir. Verilerin aktarılacağı üçüncü ülkede yeterli korumanın bulunup bulunmadığı, AB Komisyonu tarafından kabul edilen yeterlilik kararları ile belirlenmektedir. Yeterlilik kararları Birlik dışındaki herhangi bir ülke veya ülke dâhilindeki bir bölge veya bir veya daha fazla sayıda sektörün yeterli düzeyde koruma sağladığını tespit edebilir. Yeterlilik kararlarının en az dört yılda bir olmak üzere, üçüncü ülkedeki tüm gelişmeleri dikkate alan bir incelemeye tabi tutulması gerekmektedir. Bu incelemenin sonucu olarak Komisyon, üçüncü ülkenin artık yeterli koruma sağlamadığını tespit ederse, kararını değiştirebilir, askıya alabilir veya yürürlükten kaldırabilir.

Verilerin aktarılabacağı ülke hakkında Komisyonca kabul edilmiş bir yeterlilik kararı bulunmadığı takdirde, veri sahibi için uygulanabilir haklar ve yasal çözümler de dâhil olmak üzere veri sorumlusu veya veri işleyen tarafından GDPR m.46'da öngörülen uygun güvenlik önlemlerinin alınmış olması gerekmektedir. Buna göre, uygun güvenceler, bir denetim makamının iznine gerek olmaksızın; kamu kuruluşları veya organları arasında yasal bağlayıcılığı bulunan ve uygulanabilir bir belge, bağlayıcı şirket kuralları, Komisyon tarafından kabul edilen standart veri koruma hükümleri, denetim makamı tarafından kabul edilen ve Komisyon tarafından onaylanan standart veri koruma hükümleri, onaylanmış davranış kuralları, onaylanmış belgelendirme mekanizması (GDPR m.46/f/2) gibi önlemlerle ve yetkili denetim makamından alınan izne tabi olarak; veri sorumlusu veya veri işleyen ile üçüncü ülke veya uluslararası kuruluştaki veri sorumlusu veya veri işleyen arasındaki sözleşme maddeleri, kamu kuruluşları ya da organları arasındaki idari düzenlemelere eklenecek olan uygulanabilir ve etkili veri sahibi haklarını kapsayan hükümler (GDPR m.46/f/3) gibi önlemlerle sağlanabilir.

Hiyerarşi gereğince, hem yeterlilik kararının hem de veri sorumlusu/ işleyen tarafından alınmış uygun güvenlik önlemlerinin bulunmadığı durumlarda Birlik dışına veri aktarımları yalnızca GDPR m.49'da belirtilen spesifik durumlarda mümkün olacaktır. Bunlara; a) veri sahibinin, bir yeterlilik kararı ve uygun güvencelerin bulunmaması nedeniyle söz konusu aktarımların kendisine yönelik riskleri hakkında haberdar edilmesinin ardından, önerilen aktarıma açık bir şekilde rıza göstermesi, b) aktarımın, veri sahibi ile veri sorumlusu arasındaki bir sözleşmenin yürütülmesi veya veri sahibinin talebiyle alınan sözleşme öncesi tedbirlerin uygulanması açısından gerekli olması, c) aktarımın, veri sorumlusu ile başka bir gerçek veya tüzel kişi arasında veri sahibi yararına yapılan bir sözleşmenin imzalanması veya yürütülmesi açısından gerekli olması, d) aktarımın, kamu yararına ilişkin önemli sebeplerden dolayı gerekli olması, e) aktarımın, hukuki iddialarda bulunulması, bu iddiaların uygulanması veya savunulması açısından gerekli olması, f) veri sahibinin fiziksel veya hukuki olarak rıza veremeyecek durumda olması hâlinde, aktarımın veri sahibi veya diğer kişilerin hayati menfaatlerinin korunması açısından gerekli olması, g) verilerin kamuya açık sicilden aktarılması dâhildir. Adı

geçen istisnai durumların dar yorumlanması gerekmektedir. Aksi takdirde bu istisnalar kural hâline gelecektir.

Üçüncü ülkelere veri aktarımı gerçekleştirmenin bir başka yolu da, veri aktarımının uluslararası sözleşmelerde öngörülmüş olmasıdır. Şöyle ki, GDPR'ın, AB ile üçüncü ülkeler arasında akdedilen ve kişisel veri aktarımlarını düzenleyen uluslararası sözleşmelere hâlel getirmeyeceği giriş bölümünün 102'nci paragrafında belirtilmiştir. Bu tür anlaşmalar, veri sahipleri için uygun korumalar içermeleridir. AB ile üçüncü ülkeler arasında belirli amaçlarla kişisel veri aktarımı düzenleyen uluslararası düzenlemelere PNR anlaşmaları, SWIFT anlaşması örnek olarak gösterilebilir.

KVKK'da kişisel verilerin yurt içinde aktarılması ve yurt dışına aktarılması faaliyetleri için farklı düzenlemeler öngörülmüştür. KVKK m.8 uyarınca, *“kişisel veriler ilgilinin açık rızası olmaksızın aktarılamaz”*. Sadece *“...5'inci maddenin ikinci fıkrasında ve yeterli önlemler alınmak kaydıyla, 6'ncı maddenin üçüncü fıkrasında belirtilen şartlardan birinin bulunması hâlinde...”*, açık rıza alınmadan kişisel veriler aktarılabilir. Ayrıca aktarımla ilgili diğer kanunlarda yer alan hükümler de saklıdır. Anlaşıldığı üzere, kişisel verilerin yurt içinde aktarılması için aşağıdaki hukuki dayanaklardan birinin varlığı aranmaktadır:

- 1) İlgili kişinin açık rızasının bulunması,
- 2) Kişisel verilerin işlenmesi için 5'inci ve 6'ncı maddelerde öngörülen hukuka uygunluk sebeplerinden birinin mevcut olması,
- 3) Aktarımla ilgili diğer kanunlarda yer alan hükümler.

Bu noktada belirtmek gerekir ki her ne kadar hükmün ifade şeklinden açık rızanın diğer hukuka uygunluk sebepleri karşısında bir üstünlüğü olması izlenimi oluşmuş olsa da, Kurum'un yayınladığı rehberlerde açık rıza ile diğer hukuka uygunluk sebeplerinin eşit değerde olduğu belirtilmiştir.

Genel nitelikli kişisel verilerin, açık rıza aranmaksızın aktarılabilmesi için KVKK m.5/f.2'te belirtilen hukuka uygunluk sebeplerinden birinin (kanunlarda

açıkça öngörölme; fiilî imkânsızlık nedeniyle rızasını açıklayamayacak durumda bulunan veya rızasına hukuki geçerlilik tanınmayan kişinin kendisinin veya bir başkasının hayati bütünlüğünün korunması; sözleşmenin kurulması veya ifasıyla doğrudan ilişkili olması kaydıyla; sözleşme taraflarına dair verilerin kişisel verilerin işlenmesi; veri sorumlusunun hukuki yükümlülüğünün yerine getirilmesi; verilerin ilgili kişinin kendisi tarafından alenileştirilmiş olması; hakkın tesisi, kullanılması veya korunması için veri işlemenin zorunlu olması; veri sorumlusunun meşru menfaatleri) varlığı aranacaktır. Özel nitelikli kişisel verilerin açık rıza olmaksızın aktarılması söz konusu olduğunda ise, KVKK'da ikili bir ayrıma gidilmiştir. Şöyle ki, KVKK m.6/f.3 uyarınca, sağlık ve cinsel hayata ilişkin veriler dışında kalan özel nitelikli kişisel veriler (kişinin ırkı, etnik kökeni, siyasi düşüncesi, felsefi inancı, dini, mezhebi veya diğer inançları, kılık ve kıyafeti, dernek, vakıf veya sendika üyeliği, ceza mahkûmiyeti ve güvenlik tedbirleriyle ilgili verileri ile biyometrik ve genetik verileri) kanunlarda öngörülen hâllerde açık rıza olmaksızın aktarılabilir. Sağlık ve cinsel hayata ilişkin verilerin aktarılması için ise KVKK'da belirtilen amaca ilişkin şartlarla (kamu sağlığının korunması; koruyucu hekimlik; tıbbi teşhis, tedavi ve bakım hizmetlerinin yürütülmesi; sağlık hizmetleri ile finansmanın planlanması ve yönetilmesi) veri işleyene yönelik şartların (sır saklama yükümlülüğü altında bulunan kişiler veya yetkili kurum ve kuruluşlar) birlikte mevcut olması gerekmektedir. Bu koşulların yanı sıra, özel nitelikli kişisel veriler aktarılırken yeterli önlemler alınmış olmalıdır. Veri sorumlusu tarafından alınması gereken yeterli önlemler, Kurul tarafından kabul edilen 31.01.2018 tarihli ve 2018/10 sayılı karar ile belirlenmiştir.

Yurt içinde yapılan aktarımlar gibi, yurt dışına yapılan aktarımlar da veri sahibinin açık rızası olmadan gerçekleştirilemez (KVKK m.9/f.1). Açık rıza aranmaksızın kişisel verilerin yurt dışına aktarılabilceği durumlar, yurt içinde yapılan aktarımlar açısından öngörülen durumlarla aynı olsa da (KVKK m.5/f.2; m.6/f.3) bu hukuka uygunluk sebepleri yurt dışına yapılan aktarımlar için tek başına yeterli olmayacaktır. Bu hukuka uygunluk sebeplerinin yanı sıra, kişisel verilerin aktarılacağı ülkede yeterli korumanın bulunması veya yeterli korumanın veri sorumlusu tarafından temin edilmesi gerekmektedir.

Yeterli koruma saęlayan lkelerin listesi; Adalet Bakanlıęı, Dışışleri Bakanlıęı ve Ticaret Bakanlıęı ile işbirlięi çerçevesinde Kurul tarafından belirlenmelidir. Fakat bugüne kadar hiçbir lke hakkında yeterli koruma saęladığına dair karar verilmemiştir. Bu kapsamda Kurul, sadece 02.05.2019 tarihli ve 2019/125 sayılı kararı ile “Yeterli Korumaya Sahip lkelerin Belirlenmesinde Esas Alınacak Kriterler”i kabul etmiştir. Herhangi bir lke hakkında yeterlilik kararı kabul edilse bile bu kararlar, periyodik gözden geçirmelere tabi tutulacak ve deęişen koşullara göre söz konusu yeterlilik kararları deęiştirilebilecek, askıya alınabilecek veya kaldırılabilir.

Verilerin aktarılaçağı lkede yeterli korumanın bulunmadığı durumlarda ise, yeterli korumanın Türkiye’deki veri sorumlusu ile ilgili yabancı lkedeki veri sorumlusu tarafından yazılı olarak taahhüt edilmesi ve aktarım için Kurul’un izninin alınması gerekmektedir. Bu kapsamda Kurul tarafından iki taahhütname örneęi (“veri sorumlusundan veri sorumlusuna” ve “veri sorumlusundan veri işleyene”) kabul edilmiş ve taahhütnameelerde yer alması gereken asgari unsurlar belirlenmiştir. Kurul, bu çalışmanın yapıldığı tarih itibarıyla taahhütname başvurularından sadece üçünü onaylamıştır. Kişisel Verileri Koruma Kurumu, taahhütname başvurularının geç sonuçlanmasının bir sebebi olarak, başvuruların idari makamlara yapılacak başvurularda riayet edilmesi gereken usul ve esaslara uygun olmadığını belirtmiştir. Bu nedenle Kurum, bir duyuru yayınlayarak taahhütname hazırlanmasında veri sorumluları tarafından usule ve esasa ilişkin dikkat edilmesi gereken hususları belirtmiştir.

Kanun’da öngörölme de Kurum’un 10.04.2020 tarihinde yayınladığı duyuru ile bağlayıcı şirket kuralları da yeterli korumanın bulunmadığı lkelere veri aktarımı gerçekleştirmek için yeni bir yöntem olarak belirlenmiştir. Kurum’un bu kararı kişisel verilerin yurt dışına aktarılması faaliyeti açısından olumlu bir gelişmedir. Zira güvenli lkeler listesinin yayınlanmamış olması, Kurul’un taahhütname başvurularını onaylamakta çekimser davranması, yurt dışına veri aktarımı gerçekleştirecek olan veri sorumlularını açık rızaya dayalı aktarımlara mecbur bırakmıştır. Böyle bir durumda bağlayıcı şirket kurallarının uygulamaya konulması veri sorumlularına kolaylık saęlayacaktır.

Yeterli korumanın bulunup bulunmamasından bağımsız olarak, Kanun'da kişisel verilerin sadece Kurul'un izniyle yurt dışına aktarılabilceğı durumlar da öngörölmüştür. Şöyle ki m.9/f.5 uyarınca, *uluslararası sözleşme hükümleri saklı kalmak üzere*, Türkiye'nin veya ilgili kişinin menfaatinin ciddi bir şekilde zarar göreceğı durumlarda, kişisel veriler ancak ilgili kamu kurum veya kuruluşunun görüşü alınarak Kurul'un izniyle yurt dışına aktarılabilir. Hükümün lafzından anlaşıldığı üzere, verilerin yurt dışına aktarılması bağlamında uluslararası sözleşmelere öncelik tanınmıştır. Buradan çıkan sonuca göre, kişisel verilerin Türkiye'den başka bir ülkeye aktarılabilmesi için öncelikle herhangi uluslararası sözleşmenin bulunup bulunmadığı aranacaktır. Böyle bir sözleşmenin bulunmadığı durumlarda ise kanunda öngörölen diğer mekanizmalar uygulamaya koyulacaktır. Ayrıca, m.9/f.6 uyarınca, kişisel verilerin yurt dışına aktarılmasına ilişkin diğer kanunlarda yer alan hükümler saklıdır.

KAYNAKÇA

- Akgül, Aydın: “Kişisel Verilerin Korunması Açısından İdarenin Hukuki Sorumluluğu ve Yargısal Denetimi”, Doktora Tezi, Kocaeli Üniversitesi, 2013.
- Akçalı Gür, Berna: “Uluslararası Hukuk ve AB Hukuku Boyutuyla Kişisel Verilerin Yurt Dışına Aktarılması”, **Marmara Üniversitesi Hukuk Fakültesi Hukuk Araştırmaları Dergisi**, C. 25, S. 2, 2019, s. 850-872.
- Akıncı, Ayşe Nur: **Avrupa Birliği Genel Veri Koruma Tüzüğü’nün Getirdiği Yenilikler ve Türk Hukuku Bakımından Değerlendirilmesi**, Kalkınma Bakanlığı, Ankara, 2017.
- Akipek, Jale/
Akıntürk, Turgut/
Ateş, Derya: **Türk Medeni Hukuku Başlangıç Hükümleri Kişiler Hukuku**, C. 1, 15. bs., İstanbul, Beta Basım, 2019.
- Aksoy, Hüseyin Can: **Medeni Hukuk ve Özellikle Kişilik Hakkı Yönünden Kişisel Verilerin Korunması**, Ankara, Çakmak Yayınevi, 2010.
- Altındağ, Halil: **Kişisel Verileri Koruma Kurulu Tarafından Verilen İdari Para Cezaları**, Ankara, Adalet, 2021.
- Altındere, Murat: **Kişisel Verilerin Korunması Hukuku ve Uygulaması**, Ankara, Adalet, 2020.

- Amery, Chris: “The European Union Data Protection Directive – Where are we? How did we get here? What next?”, **Information on Security Technical Report**, C. 2, S. 1, 1997, s. 29-37.
- Amory Winslow, Charles-Edward: “The Untilled Fields of Public Health”, **Science**, C. 51, S. 1306, 1920, s. 23-30, (çevrimiçi), pubmed.ncbi.nlm.nih.gov/17838891/, 12.06.2022.
- Anı, Nevzat Ali: “Kişisel Verilerin İşlenmesi ve Açık Rıza”, Yüksek Lisans Tezi, İstanbul Üniversitesi, 2018.
- Arslan, Çetin: “Avrupa Birliği Hukukunda Kişisel Verilerin Üçüncü Ülkelere Aktarılması”, **Galatasaray Üniversitesi Hukuk Fakültesi Dergisi**, C. 9, S. 1, 2010, s. 447-487.
- Article 29 Data Protection Working Party: Opinion 01/2016 on the EU - U.S. Privacy Shield Draft Adequacy Decision, 13.04.2016, (çevrimiçi), <https://ec.europa.eu/newsroom/article29/items/640157>, 12.06.2022.
- Article 29 Data Protection Working Party: Opinion 15/2011 on the Definition of Consent, 13.07.2011, (çevrimiçi), https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2011/wp187_en.pdf, 12.06.2022, (Definition of Consent).

Article 29 Data
Protection Working Party: Opinion 4/2007 on the Concept of Personal Data,
20.06.2007, (çevrimiçi),
www.clinicalstudydatarequest.com/Documents/Privacy-European-guidance.pdf, 12.06.2022
(Personal Data).

Article 29 Data
Protection Working Party: Recommendation 1/2007 on the Standard
Application for Approval of Binding Corporate
Rules for the Transfer of Personal Data,
10.01.2007, (çevrimiçi),
https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/index_en.htm, 12.06.2022.

Article 29 Data
Protection Working Party: Working Document Establishing a Model
Checklist Application for Approval of Binding
Corporate Rules, 14.04.2005, (çevrimiçi),
https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2005/wp108_en.pdf,
12.06.2022 (Model Checklist).

Article 29 Data
Protection Working Party: Working Document on a Common Interpretation
of Article 26(1) of Directive 95/46/EC of 24
October 1995, 25.11.2005, (çevrimiçi),
ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2005/wp114_en.pdf,
12.06.2022, (Common Interpretation of Article
26(1)).

Article 29 Data
Protection Working Party: Working Document Setting up a Framework for the Structure of Binding Corporate Rules, 24.06.2008, (çevrimiçi), ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2008/wp154_en.pdf, 12.06.2022 (The Structure of BCR).

Article 29 Data
Protection Working Party: Working Document Setting up a Table with the Elements and Principles to Be Found in Processor Binding Corporate Rules, 06.02.2018, (çevrimiçi), <https://ec.europa.eu/newsroom/article29/items/614110/en>, 12.06.2022.

Article 29 Data
Protection Working Party: Working Document Transfers of Personal Data to Third Countries: Applying Article 26(2) of the EU Data Protection Directive to Binding Corporate Rules for International Data Transfers, 03.06.2003, (çevrimiçi), https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2003/wp74_en.pdf, 12.06.2022.

Aşıkoğlu, Şehriban İpek: **Avrupa Birliği ve Türk Hukukunda Kişisel Verilerin Korunması ve Büyük Veri**, İstanbul, On İki Levha, 2018, (Kişisel Veriler).

Aşıkoğlu, Şehriban İpek: “Kişisel Verilerin İşlenmesinde Hukuka Uygunluk Sebepleri”, **Türk Hukukunun Avrupa**

Birliđi Hukukuna Uyumu Özel Hukuk: Acquis Communautaire’in Alınması, Açıklamalar, Deđerlendirmeler, Öneriler içinde, Ed.: Arslan Kaya, Baki İlkay Engin, Ali Paslı, Şehriban İpek Aşıkođlu, Elif Ođuz, İstanbul, İstanbul Üniversitesi Yayınevi, 2020, s. 1057-1079, (Hukuka Uygunluk Sebepleri).

Aşıkođlu, Şehriban İpek/ Uzun, Fatih Burak: “Kişisel Verilerin Yurtdışına Aktarımının Açık Rızaya Dayandırılmasının Yarattığı Sorunlar ve Çözüm Önerileri”, **Prof. Dr. Türkan Rado’nun Anısına Armađan** içinde, Yayına Hazırlayan: Abuzer Kendigelen, İstanbul, On İki Levha, 2020, s. 921-967.

Atasoy, Kemal: “Kişilik Hakkı Kapsamında Sosyal Medyada Kişisel Verilerin Korunması ve Veri Sahibinin Rızası”, **Marmara Üniversitesi Hukuk Fakóltesi Hukuk Araştırmaları Dergisi**, C. 22, S. 3, 2016, s. 269-299.

Avcı Braun, Cihan: “Kişisel Verilerin İşlenmesinde Rıza”, **Yeditepe Üniversitesi Hukuk Fakóltesi Dergisi**, C. 15, S. 1, 2018, s. 13-31.

Ayözger Öngün, Çiğdem: **Kişisel Verilerin Korunması Hukuku: Elektronik Haberleşme Sektörüne İlişkin Özel Düzenlemeler Dahil**, 2. bs., İstanbul, Beta Basım, 2019.

Barcelo, Rosa: “Seeking Suitable Options for Importing Data from the European Union”, **The International**

Lawyer, C. 36, S. 3, 2001, s. 985-1005.

Basan, Nuri Mehmet/
Bilir, Nazmi:

“Koruyucu Sağlık Hizmetlerinde Önleme Çelişkisi ve Nedenleri”, **TAF Preventive Medicine Bulletin**, C. 15, S. 1, 2016, s. 44-50.

Başalp, Nilgün:

“Kişisel Verilerinin İnternette Açıklanması Üzerine Bir Avrupa Topluluğu Adalet Divanı Kararı: Kişisel Verilerin ve Özellikle Sağlık Verilerin İnternette Açıklanması 95/46 sayılı Yönergenin Uygulama Alanına Girer Mi?”, **Bilişim ve Hukuk Dergisi**, C. 1, S. 10, 2009, s. 19-21 (ABAD Kararı).

Başalp, Nilgün:

Kişisel Verilerin Korunması ve Saklanması, Ankara, Yetkin, 2004 (Kişisel Veriler).

Bayındır, Hamza:

Özel Sağlık Kurumları Kapsamında Kişisel Sağlık Verilerinin İşlenmesi ve Korunması, İstanbul, On İki Levha, 2020.

Benli, Salih:

“Yolcu İsim Kayıtları”, **Terazi Hukuk Dergisi**, C. 10, S. 103, 2015, s. 41-48.

Büyükcay, Yusuf:

“Hekimin Sır Saklama Yükümlülüğü”, **Atatürk Üniversitesi Erzincan Hukuk Fakültesi Dergisi**, C. 8, S. 1-2, 2004, s. 383-396.

Bygrave, Lee Andrew:

Data Protection Law, (Approaching Its Rationale, Logic and Limits), The Hague, Kluwer Law International, 2002, (Data

Protection).

- Bygrave, Lee A.: **Data Privacy Law: An International Perspective**, New York, Oxford University Press, 2014, (Data Privacy).
- Bygrave, Lee A.: “Privacy and Data Protection in an International Perspective”, **Scandinavian Studies in Law**, 2010, s. 165-200, (Privacy and Data Protection).
- Charlesworth, Andrew: “Information Privacy Law in the European Union: E Pluribus Unum or Ex Uno Plures?”, **Hastings Law Journal**, C. 54, S. 4, 2003, s. 931-969.
- Childs, Alfred W.: “The Functions of Medical Care”, **Public Health Reports**, C. 90, S. 1, 1975, s. 10-14.
- Christakis, Theodore: “Transfer of EU Personal Data to U.S. Law Enforcement Authorities After the CLOUD Act: Is There a Conflict with the GDPR?”, Ed.: RANDAL MILCH, Sebastian Benthall, **Cybersecurity and Privacy in a Globalized World - Building Common Approaches**, New York University School of Law, 2019.
- Clarke, E.A.: “What is Preventive Medicine?”, **Official Publication of The College of Family Physicians of Canada**, C. 20, S. 11, 1974.

Commission of the European Communities: “Community Policy on Data Processing”, 21.11.1973, Brussels, (çevrimiçi), <http://aei.pitt.edu/6337/1/6337.pdf>, 12.06.2022.

Compagnucci, Marcelo Corrales/
Aboy, Mateo/
Minssen, Timo: “Cross-Border Transfers of Personal Data after Schrems II: Supplementary Measures and New Standard Contractual Clauses (SCCs)”, 27.10.2021, (çevrimiçi), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3951085, 12.06.2022.

Council of Europe: Explanatory Report to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, 28.01.1981, (çevrimiçi), <https://rm.coe.int/16800ca434>, 12.06.2022.

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**, C. 74, S. 2, 2016, s. 629-642, (Big Data ve İrade Serbestisi).

Çekin, Mesut Serdar: **Kişisel Verilerin Korunması Hukuku: Avrupa Birliği Hukukuyla Mukayeseli Olarak 6698 Sayılı Kanun Çerçevesinde**, 3. bs., İstanbul, On İki Levha, 2020, (Kişisel Verilerin Korunması).

Çelik, Işıl: **Kişisel Verilerin Yurt Dışına Aktarılması: 6698**

Sayıli Kişisel Verilerin Korunması Kanunu ve 2016/679 Sayılı Avrupa Birlięi Genel Veri Koruma Tüzüęü Kapsamında, İstanbul, On İki Levha, 2022.

Develioęlu, Hüseyin Murat: **6698 Sayılı Kişisel Verilerin Korunması Kanunu ile Karşılaştırmalı Olarak Avrupa Birlięi Genel Veri Koruma Tüzüęü Uyarınca Kişisel Verilerin Korunması Hukuku**, İstanbul, On İki Levha, 2017.

Dural, Mustafa/
Öęüz, Tufan: **Kişiler Hukuku: Gerçek ve Tüzel Kişiler**, 22. bs., İstanbul, Filiz Kitabevi, 2021.

Dülger, Murat Volkan: “Kişisel Verileri Koruma Kurulu’nun 108 Sayılı Sözleşme Hakkındaki Kararı ve Yurtdışına Veri Aktarımı Sorunu”, (çevrimiçi), papers.ssrn.com/sol3/papers.cfm?abstract_id=3792396, 12.06.2022, (108 sayılı Sözleşme).

Dülger, Murat Volkan: **Kişisel Verilerin Korunması Hukuku**, 3. bs., İstanbul, Hukuk Akademisi Yayınları, 2020, (Kişisel Veriler).

Dülger, Murat Volkan/
Dicle, Yavuz Selim: “Kişisel Sağlık Verilerinin İşlenmesi Sorunu ve Covid 19 Üzerine Deęerlendirme - “KVKK Hükümlerinin İş İlişkileri Kapsamında Deęerlendirilmesi”ne Katkı”, (çevrimiçi), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3792377, 12.06.2022.

Dülger, Murat Volkan/
Kahraman, Cansu Ceren:

“KVKK’dan Kişisel Verilerin Yurt Dışına Aktarımında Önemli Bir Adım: Bağlayıcı Şirket Kuralları”, (çevrimiçi), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3792375, 12.06.2022, (Bağlayıcı Şirket Kuralları).

Dülger, Murat Volkan/
Kahraman, Cansu Ceren:

“GDPR ve KVKK Ekseninde Bağlayıcı Şirket Kuralları”, **Hukuk ve Daha Fazlası**, 2021, s. 61-76, (çevrimiçi), papers.ssrn.com/sol3/papers.cfm?abstract_id=3853724, 12.06.2022, (GDPR ve KVKK Ekseninde).

Ellen McIntire, Mary:

“How a Law Seminar Inspired a Student to Bring a Case to Europe’s Top Court”, 07.10.2015, (çevrimiçi), <https://www.chronicle.com/article/how-a-law-seminar-inspired-a-student-to-bring-a-case-to-europes-top-court/>, 12.06.2022.

Erarslan, Sevgi:

Özel Nitelikli Kişisel Verilerin İşlenmesinde Açık Rızanın Aranmadığı Haller, 2. bs., İstanbul, On İki Levha, 2020, (Özel Nitelikli Kişisel Veriler).

Erarslan, Sevgi:

“Türk Hukukunda Kişisel Verilerin Yurt Dışına Aktarılması Sorunu: Açık Rıza Kapsamında Bir Değerlendirme”, **Kırıkkale Hukuk Mecmuası**, C. 1, S. 1, 2021, s. 82-115, (Erarslan, Verilerin Aktarılması).

Erbschloe, Michael/
Vacca, John:

Net Privacy: A Guide to Developing and Implementing an Ironclad Ebusiness Privacy Plan, Mc-Graw Hill, 2001.

European Commission:

Communication from the Commission to the European Parliament and the Council on the Functioning of the Safe Harbour from the Perspective of EU Citizens and Companies Established in the EU, Brussels, 27.11.2013, (çevrimiçi), <https://eur-lex.europa.eu/legal-content/en/txt/?uri=celex%3a52013dc0847>, 12.06.2022.

European Commission:

“European Commission and United States Joint Statement on Trans-Atlantic Data Privacy Framework”, 25.03.2022, (çevrimiçi), https://ec.europa.eu/commission/presscorner/detail/en/ip_22_2087, 12.06.2022.

European Commission:

“First Orientations on Transfers of Personal Data to Third Countries - Possible Ways Forward in Assessing Adequacy”, 26.06.1997, (çevrimiçi), https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/1997/wp4_en.pdf, 12.06.2022, (First Orientation on Transfers).

European Commission:

Proposal for a Regulation of the European Parliament and of the Council on the protection of

individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation), 25.01.2012, Brussels, (çevrimiçi), <https://eur-lex.europa.eu/legal-content/en/txt/pdf/?uri=celex:52012pc0011&from=en>, 12.06.2022.

European Commission:

Transfers of Personal Data to Third Countries: Applying Articles 25 and 26 of the EU Data Protection Directives, 24.07.1998, (çevrimiçi), https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/1998/wp12_en.pdf, 12.06.2022.

European Data
Protection Board:

Guidelines 04/2021 on Codes of Conduct as Tools for Transfers, 14.07.2021, (çevrimiçi), edpb.europa.eu/our-work-tools/documents/public-consultations/2021/guidelines-042021-codes-conduct-tools-transfers_en, (Codes of Conduct).

European Data
Protection Board:

Guidelines 05/2020 on Consent under Regulation 2016/679, 04.05.2020, (çevrimiçi), https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_202005_consent_en.pdf, 12.06.2022, (Consent).

European Data
Protection Board:

Guidelines 05/2021 on the Interplay between the Application of Article 3 and the Provisions on International Transfers as per Chapter V of the

GDPR, 18.11.2021, (çevrimiçi), https://edpb.europa.eu/our-work-tools/documents/public-consultations/2021/guidelines-052021-interplay-between-application_en, 12.06.2022, (Guidelines 05/2021).

European Data
Protection Board:

Guidelines 1/2018 on Certification and Identifying Certification Criteria in Accordance with Articles 42 and 43 of the General Data Protection Regulation (2016/679), 04.06.2019, (çevrimiçi), https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-42018-accreditation-certification-bodies-under_en, 12.06.2022, (Certification).

European Data
Protection Board:

Guidelines 1/2019 on Codes of Conduct and Monitoring Bodies under Regulation 2016/679, 04.06.2019, (çevrimiçi), edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-12019-codes-conduct-and-monitoring-bodies-0_en, 12.06.2012, (Monitoring Bodies).

European Data
Protection Board:

Guidelines 2/2018 on Derogations of Article 49 under Regulation 2016/679, 25.05.2018, (çevrimiçi), https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-22018-derogations-article-49-under-regulation_en, 12.06.2022, (Derogations).

European Data

Guidelines 2/2020 on Articles 46 (2) (a) and 46

Protection Board: (3) (b) of Regulation 2016/679 for Transfers of Personal Data between EEA and Non-EEA Public Authorities and Bodies, 18.01.2020, (çevrimiçi), https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-22020-articles-46-2-and-46-3-b-regulation_en, 12.06.2022.

European Data
Protection Board: Recommendations 01/2020 on Measures That Supplement Transfer Tools to Ensure Compliance with the EU Level of Protection of Personal Data, 10.11.2020, (çevrimiçi), https://edpb.europa.eu/our-work-tools/documents/public-consultations/2020/recommendations-012020-measures-supplement_en, 12.06.2022, (Guidelines on articles 46/2a and 46/3b).

European Data
Protection Board: Statement 02/2022 on Personal Data Transfers to the Russian Federation, 12.07.2022, (çevrimiçi), edpb.europa.eu/system/files/2022-07/edpb_statement_20220712_transferstorussia_en.pdf, 20.07.2022.

European Data
Protection Supervisor: Opinion of the European Data Protection Supervisor on the Data Protection Reform Package, 07.03.2012, (çevrimiçi), https://edps.europa.eu/sites/default/files/publication/12-03-07_edps_reform_package_en.pdf, 12.06.2022.

- European Data Protection Supervisor: The Transfer of Personal Data to Third Countries and International Organisations by EU Institutions and Bodies, 14.07.2014, (çevrimiçi), https://edps.europa.eu/sites/edp/files/publication/14-07-14_transfer_third_countries_en.pdf, 12.06.2022, (The Transfer of Personal Data).
- European Parliament: US NSA: Stop Mass Surveillance Now or Face Consequences, MEPs Say, 12.03.2014, (çevrimiçi), <https://www.europarl.europa.eu/news/en/press-room/20140307IPR38203/us-nsa-stop-mass-surveillance-now-or-face-consequences-meps-say>, 12.06.2022.
- European Parliament Committee on Civil Liberties, Justice and Home Affairs: “Draft Report on the Proposal For a Regulation of the European Parliament and of the Council on the Protection of Individual with Regard to the Processing of Personal Data and on the Free Movement of Such Data (General Data Protection Regulation)”, 16.01.2013, (çevrimiçi), https://www.europarl.europa.eu/doceo/document/A-7-2013-0402_EN.html, 12.06.2022.
- Giakoumopoulos, Christos/
Buttarelli, Giovanni/
O’Flaherty, Michael: **Handbook on European Data Protection Law**, Lüksemburg, Publications Office of the European Union, 2018.
- Fishman, William L.: “Introduction to Transborder Data Flows”, **Stanford Journal of International Law**, S. 16,

1980, s. 1-26.

Fuster, Gloria Gonzalez: “Un-Mapping Personal Data Transfers”, **European Data Protection Review**, C. 2, S. 2, 2016, s. 160-168.

Göçmen Uyarer, Sinem: **Kişisel Verilerin Korunması: KVKK ve TCK Kapsamında**, 2. bs., Ankara, Seçkin, 2020.

Greenleaf, Graham: “The influence of European data privacy standards outside Europe: Implications for globalisation of Convention 108?”, **International Data Privacy Law**, C. 2, S. 2, 2012, s. 1-34.

Gültekin Varkonyı, Gizem: “Yolcu İsim Kayıtlarının Terörle Mücadele Kapsamında Yurt Dışına Yasal Aktarımı: Avrupa Birliği Uygulamaları ve Türkiye”, **Türkiye Barolar Birliği Dergisi**, C. 30, S. 132, 2017, s. 339-382.

Günergök, Özcan: “Avukatın Sır Saklama Yükümlülüğü”, **Erzincan Üniversitesi Hukuk Fakültesi Dergisi**, C. 7, S. 1-2, 2003, s. 655-667.

Gür, İkbâl: **Kişisel Verilerin Korunması Hususunda AB İle ABD Arasında Çıkan Uyuşmazlıklar ve Çözüm Yolları**, Ankara, Turhan Kitabevi, 2010.

Güvercin, Ali/
Mil, Halil İbrahim: “Sağlık Hizmetlerinin Finansmanı ve Sosyal Güvenlik Kurumu (SGK)”, **Bartın Üniversitesi**

- Tarım, Bülent: **İktisadi ve İdari Bilimler Fakültesi Dergisi**, C. 7, S. 13, Bartın, 2016, s.80-92.
- Hakalmaz, Ezgi: **Hekimlik Sözleşmesi Bağlamında Kişisel Sağlık Verilerinin İşlenmesi ve Korunması**, İstanbul, On İki Levha, 2021.
- Hakeri, Hakan: **Tıp Hukuku**, 19. bs., Ankara, Seçkin, 2020.
- Helvacı, Serap: **Gerçek Kişiler**, 9. bs., İstanbul, Legal, 2021.
- Henkoğlu, Türkay: **Bilgi Güvenliği ve Kişisel Verilerin Korunması**, Ankara, Yetkin, 2015.
- Hon, W. Kuan/
Millard, Christian: “Data Export in Cloud Computing – How Can Personal Data Be Transferred Outside The EEA?”, (çevrimiçi), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2034286, 12.06.2022.
- Hon, W. Kuan: **Data Localization Laws and Policy: The EU Data Protection International Transfers Restriction Through a Cloud Computing Lens**, Massachusetts, Edward Elgar Publishing, 2017.
- Hondius, Frits W.: “A Decade of International Data Protection”, **Netherlands International Law Review**, C. 30, S. 2, 1983, s. 103-128.
- İmançlı, Canan: **Kişisel Sağlık Verilerinin Korun(a)mamasından Doğan Özel Hukuk Sorumluluğu**, İstanbul, On İki Levha, 2020.

Bilgi Information

Technology Law Institute:

**Kişisel Verilerin Korunmasına İlişkin
Düzenlemeler Çerçevesinde Uluslararası Veri
Aktarımı: Yeni Gelişmeler ve Uygulamaya
İlişkin Hukuki Değerlendirmeler**, İstanbul,
06.03.2020, “CoE 108+ and the GDPR: A
Modernised Look and Nexus at Protecting
Personal Data Worldwide” Konferansı
(çevrimiçi),

https://itlaw.bilgi.edu.tr/media/2020/3/30/Final%20Veri_Aktarimi_Raporu_30.03.2020.pdf,

12.06.2022.

Kama Işık, Sezen:

**Avrupa Veri Koruma Hukukuna Anayasal Bir
Bakış: 2016/679 sayılı GVKT (GDPR) ile 6698
sayılı KVKK’nın Detaylı Analiz ve
Karşılaştırılması** ile, İstanbul, On İki Levha,
2020.

Kamara, Irene/
Leenes, Ronald/
Lachaud, Eric/
Stuurman, Kees/
van Lieshout, Marc/
Bodea, Gabriela:

Data Protection Certification Mechanisms: Study
on Articles 42 and 43 of the Regulation (EU)
2016/679, Final Report, Brussels, Justice and
Consumers, (çevrimiçi),
https://ec.europa.eu/info/sites/default/files/data_protection_certification_mechanisms_study_final.pdf, 12.06.2022.

Kaya, Cemil:

**Assessing the Transfer of Personal Data in the
European Union in the Light of the Data
Protection Directive**, İstanbul, On İki Levha,
2011, (Transfer of Personal Data).

Kaya, Cemil: “Avrupa Birliđi Veri Koruma Direktifi Ekseninde Hassas (Kişisel) Veriler ve İşlenmesi”, **İstanbul Üniversitesi Hukuk Fakóltesi Mecmuası**, C. 69, S. 1-2, 2011, s. 317-333, (Hassas Veriler).

Kaya, Mehmet Bedii: **Elektronik Ticaret Hukuku: Ticari Elektronik İletiler**, 2. bs., İstanbul, On İki Levha, 2020, (Elektronik Ticaret).

Kaya, Mehmet Bedii: “Kişisel Verilerin İşlenmesi ve Korunması Arasında Denge”, **Güncel Gelişmeler Işığında Kişisel Verilerin Korunması Hukuku** içinde, Ed.: Leyla Keser Berber, Ali Cem Bilgili, İstanbul, On İki Levha, 2019, s. 33-64, (Kişisel Verilerin İşlenmesi).

Kessler, David J./
Nowak, Jamie/
Khan, Sumera: “The Potential Impact of Article 48 of the General Data Protection Regulation on Cross Border Discovery From the United States”, **The Sedona Conference Journal**, C. 17, S. 2, 2016, s. 575-611.

Kızılırmak, Baran: “Cross-Border Transfer of Personal Data Under GDPR Regime and Turkish Legal Framework”, Master Thesis, University of Hamburg, 2020, (Cross-Border Transfer).

Kızılırmak, Baran: “Kişisel Verilerin İşlenmesinde Adli ve Önleyici Amaçla Öngörülen İstisnaların Ulusal ve Uluslararası Hukuka Göre Deđerlendirilmesi”, **Kadir Has Üniversitesi Hukuk Fakóltesi**

Dergisi, C. 7, S. 2, 2019, s. 225-261, (Kişisel Verilerin İşlenmesinde).

Kızıllırmak, Baran:

“Kişisel Verilerin Yurt Dışına Aktarımında KVKK Uygulamasının Eleştirisi”, 2020, (çevrimiçi), <https://law.khas.edu.tr/tr/kisisel-verilerin-yurt-disina-aktariminda-kvkk-uygulamasinin-elestirisi>, 12.06.2022, (Yurt Dışına Aktarım).

Kişisel Verileri
Koruma Kurumu:

100 Soruda Kişisel Verileri Koruma Kanunu, Ankara, KVKK Yayınları No 3, 2019, (çevrimiçi), <https://www.kvkk.gov.tr/sharedfolderserver/cmsfiles/185c2130-8070-4b2b-a91e-1d48322ca352.pdf>, 12.06.2022.

Kişisel Verileri
Koruma Kurumu:

6698 Sayılı Kişisel Verilerin Korunması Kanunu Hakkında Doğru Bilinen Yanlışlar, KVKK Yayınları No: 31, Ankara, 2020, (çevrimiçi), <https://kvkk.gov.tr/SharedFolderServer/CMSFiles/ca752cda-c3df-4645-8d5e-e2a507e63200.pdf>, 12.06.2022, (Doğru Bilinen Yanlışlar).

Kişisel Verileri
Koruma Kurumu:

6698 Sayılı Kişisel Verilerin Korunması Kanunu Hakkında Doğru Bilinen Yanlışlar - 2, (çevrimiçi), <https://www.kvkk.gov.tr/sharedfolderserver/cmsfiles/d077b665-66b6-4615-975a-249f93e084ba.pdf>, 12.06.2022, (Doğru Bilinen Yanlışlar 2).

Kişisel Verileri
Koruma Kurumu: 6698 Sayılı Kanun'da Yer Alan Kurumsal Terimler, (çevrimiçi),
<https://www.kvkk.gov.tr/yayinlar/6698%20sayili%20kanun%e2%80%99da%20yer%20alan%20kurumsal%20ter%c4%b0mler.pdf>, 12.06.2022.

Kişisel Verileri
Koruma Kurumu: 6698 sayılı Kanun'da Yer Alan Temel Kavramlar, (çevrimiçi),
<https://www.kvkk.gov.tr/Icerik/4187/6698-Sayili-Kanun'da-Yer-Alan-Temel-Kavramlar>,
12.06.2022.

Kişisel Verileri
Koruma Kurumu: Açık Rıza Rehberi, (çevrimiçi),
<https://www.kvkk.gov.tr/SharedFolderServer/CMFiles/e3c6aa10-9de4-46f8-9b51-71bcf07c09b5.pdf>, 12.06.2022.

Kişisel Verileri
Koruma Kurumu: Kişisel Veri Güvenliği Rehberi (Teknik ve İdari Tedbirler), Ankara, KVKK Yayınları, 2019, (çevrimiçi),
[kvkk.gov.tr/SharedFolderServer/CMSFiles/7512d0d4-f345-41cb-bc5b-8d5cf125e3a1.pdf](https://www.kvkk.gov.tr/SharedFolderServer/CMSFiles/7512d0d4-f345-41cb-bc5b-8d5cf125e3a1.pdf),
12.06.2022, (Veri Güvenliği Rehberi).

Kişisel Verileri
Koruma Kurumu: Kişisel Verilerin Korunması Kanununa İlişkin Uygulama Rehberi, Ankara, KVKK Yayınları No 1, 2019, (çevrimiçi),
<https://www.kvkk.gov.tr/sharedfolderserver/cmsfiles/41784a70-2bac-4e4a-830f-35c628468646.pdf>,
12.06.2022, (Uygulama Rehberi).

Kişisel Verileri
Koruma Kurumu: Kişisel Verilerin Yurtdışına Aktarılması Rehberi,

Koruma Kurumu: (çevrimiçi),
<https://www.kvkk.gov.tr/SharedFolderServer/CMFiles/9178818a-12c7-4d7f-a839-bdb8b6f358b1.pdf>, 12.06.2022.

Kişisel Verileri
Koruma Kurumu: Kişisel Verilerin Korunması Kanunu Hakkında
Sıkça Sorulan Sorular, Ankara, KVKK Yayınları,
2019, (çevrimiçi),
<https://www.kvkk.gov.tr/Icerik/4196/Kisisel-Verilerin-Korunmasi-Kanunu-Hakkinda-Sikca-Sorulan-Sorular>, 12.06.2022, (Sıkça Sorulan Sorular).

Kişisel Verileri
Koruma Kurumu: Veri Sorumluları İçin Bağlayıcı Şirket Kuralları
Başvuru Formu, (çevrimiçi),
[kvkk.gov.tr/sharedfolderserver/cmsfiles/0aa5e8ce-8e4e-403c-a444-7212f581ad23.docx](https://www.kvkk.gov.tr/sharedfolderserver/cmsfiles/0aa5e8ce-8e4e-403c-a444-7212f581ad23.docx),
12.06.2022, (Başvuru Formu).

Kişisel Verileri
Koruma Kurumu: Veri Sorumluları İçin Bağlayıcı Şirket
Kurallarında Bulunması Gereken Temel
Husurlara İlişkin Yardımcı Doküman,
[kvkk.gov.tr/sharedfolderserver/cmsfiles/62fb06e5-d623-404d-b3a1-c492891a3bbb.docx](https://www.kvkk.gov.tr/sharedfolderserver/cmsfiles/62fb06e5-d623-404d-b3a1-c492891a3bbb.docx),
12.06.2022 (Yardımcı Doküman).

Kişisel Verileri
Koruma Kurumu: Veri Sorumlusundan Veri İşleyene Aktarım,
[kvkk.gov.tr/sharedfolderserver/cmsfiles/d4ef9857-ff4e-4c5b-925c-fdd3e4eca73d.doc](https://www.kvkk.gov.tr/sharedfolderserver/cmsfiles/d4ef9857-ff4e-4c5b-925c-fdd3e4eca73d.doc), 12.06.2022.

Kişisel Verileri
Veri Sorumlusundan Veri Sorumlusuna Aktarım,

Koruma Kurumu: kvkk.gov.tr/sharedfolderserver/cmsfiles/9243078f-3a85-4f02-ae4b-e9b18048f43f.doc, 12.06.2022.

Kişisel Verileri Koruma Kurumu: Yeterli Korumaya Sahip Ülkelerin Belirlenmesinde Esas Alınacak Kriterler, kvkk.gov.tr/sharedfolderserver/cmsfiles/60d987a1-ba9d-4285-a8ce-c3f41ff4e47f.pdf, 12.06.2022.

Kong, Lingjie: “Data Protection and Transborder Data Flow in the European and Global Context”, **The European Journal of International Law**, C. 21, S. 2, 2010, s. 441-456.

Korkmaz, İbrahim: **Kişisel Verilerin Ceza Hukuku Kapsamında Korunması**, 2. bs., Ankara, Seçkin, 2019.

Kuner, Christopher: “Data Protection, Data Transfers, and International Agreements: the CJEU’s Opinion 1/15”, (çevrimiçi), verfassungsblog.de/data-protection-data-transfers-and-international-agreements-the-cjeus-opinion-115/, 12.06.2012, (CJEU Opinion).

Kuner, Christopher: “Developing an Adequate Legal Framework for International Data Transfers”, **Reinventing Data Protection?** içinde, Ed.: Serge Gutwirth, Yves Poullet, Paul de Hert, Cecile de Terwagne, Sjaak Nouwt, Springer, 2009, s. 263-273, (International Data Transfers).

Kuner, Christopher: **European Data Protection Law: Corporate**

- Compliance and Regulation**, 2. bs., Oxford University Press, 2007, (European Data Protection).
- Kuner, Christopher: “Regulation of Transborder Data Flows under Data Protection and Privacy Law: Past, Present, and Future”, **OECD Digital Economy Papers**, S. 187, 2010, (Privacy Law).
- Kuner, Christopher: “Reality and Illusion in EU Data Transfer Regulation Post Schrems”, **German Law Journal**, C. 18, S. 4, 2017, s. 882-919, (Reality and Illusion).
- Kuner, Christopher/
Bygrave, Lee A./
Docksey, Christopher/
Drechsler, Laura: **The EU General Data Protection Regulation: A Commentary**, Oxford University Press, Oxford, 2020.
- Kuner, Christopher: **Transborder Data Flows and Data Privacy Law**, Oxford, Oxford University Press, 2013, (Data Flows).
- Küzeci, Elif: **Kişisel Verilerin Korunması**, 4. bs., İstanbul, On İki Levha, 2020.
- Lee, Phillip: “The Updated Standard Contractual Clauses - A New Hope?”, 07.06.2021, (çevrimiçi), <https://iapp.org/news/a/the-updated-standard-contractual-clauses-a-new-hope/>, 12.06.2022.

Levine, Robert: “Behind the European Privacy Ruling That’s Confounding Silicon Valley”, 09.10.2015, (çevrimiçi), <https://www.nytimes.com/2015/10/11/business/international/behind-the-european-privacy-ruling-thats-confounding-silicon-valley.html>, 12.06.2022.

Lloyd, Ian J.: **Information Technology Law**, 6. bs., New York, Oxford University Press, 2011.

Moerel, Lokke: **Binding Corporate Rules: Corporate Self-Regulation of Global Data Transfers**, Oxford University Press, 2012.

Oğuzman, M. Kemal/
Seliçi, Özer/
Oktay Özdemir, Saibe: **Kişiler Hukuku (Gerçek ve Tüzel Kişiler)**, 19. bs., İstanbul, Filiz Kitabevi, 2020.

Özcan, Göknil: **Bankacılık İş ve İşlemlerinde Kişisel Verilerin Korunması**, İstanbul, On İki Leva, 2020.

Özcan, Mehmet/
Yılmaz, Fatma: “Pendulum Swings in between Civil Rights and Security: EU Policies against Terrorism in the Light of the PNR Case”, **Uluslararası Hukuk ve Politika Dergisi**, C. 3, S. 12, 2007, s. 99-118.

Özçetin, Selvi/
Balaban, Murat: **Sağlık hukuku**, 2. bs., Ankara, Seçkin, 2015.

- Özdemir, Hayrunnisa: “Teşhis ve Tedavi Sözleşmesinde Kayda Geçirme ve Sır Saklama Yükümlülüğü”, **Ankara Barosu Sağlık Hukuku Digestası**, C. 1, S. 1, 2009, s. 148-163, (Teşhis ve Tedavi).
- Özdemir, Hayrunnisa: **Elektronik Haberleşme Alanında Kişisel Verilerin Özel Hukuk Hükümlerine Göre Korunması**, Ankara, Seçkin, 2009, (Elektronik Haberleşme).
- Özkan, Oğulcan: **Kişisel Verilerin Korunması**, Ankara, Yetkin, 2020.
- Öztan, Bilge: **Medeni Hukukun Temel Kavramları**, 43. bs., Ankara, Turan Kitabevi, 2019.
- Öztürk, Bahri/
Altınok Çalışkan, Elif/
Seyhan, Serkan: **Kişisel Verilerin Korunması Hukuku: Teorik ve Pratik Çalışma Kitabı**, Ankara, Seçkin, 2021.
- Pelen, Sevde: “AB’de Kişisel Verilerin Üçüncü Ülke ve Uluslararası Kuruluşlara Aktarılması”, **Bahçeşehir Üniversitesi Hukuk Fakültesi Dergisi**, C. 16, S. 205, 2021, s. 1711-1748.
- Peter, Laurence: “Ireland delays EU deal with Israel on data transfers”, 03.09.2010, (çevrimiçi), <https://www.bbc.com/news/world-europe-11176926>, 12.06.2022.
- Poullet, Yves/ “Data Protection and Privacy in Global Networks:

- Louveaux, Sophie/
Perez Asinari, Maria
Veronica:
Room, Stewart: a European Approach”, **Electronic Data Interchange Law Review**, C. 8, S. 2-3, 2001, s. 147-182.
- Data Protection and Compliance in Context**,
Edinburgh, British Informatics Society Limited,
2007.
- Roth, Paul: “Adequate Level of Data Protection in Third Countries Post-Schrems and under the General Data Protection Regulation”, **Journal of Law, Information and Science**, C. 25, S. 1, 2017, s. 49-67.
- Schwartz, Paul M.: “The EU-U.S. Privacy Collision: A Turn to Institutions and Procedures”, **Harvard Law Review**, C. 126, S. 7, 2013, s. 1966-2009.
- Selek, Ozan: “Genel Veri Koruma Tüzüğü Işığında Kişisel Verilerin İşlenmesinde Rıza Açıklaması”, **Dokuz Eylül Üniversitesi Hukuk Fakültes Dergisi**, C. 21, S. 2, 2019, s. 911-951.
- Sertçe, Nadin: “Avrupa Birliği Genel Veri Koruma Tüzüğü (GDPR) Kapsamında AB Dışına Kişisel Veri Aktarımı”, Yüksek Lisans Tezi, İstanbul Bilgi Üniversitesi, 2022.
- Sharma, Sanjay/
Menon, Pranav: **Data Privacy and GDPR Handbook**, New Jersey, John Wiley & Sons Inc., 2020.
- Svantesson, Dan Jerker B.: “Privacy, The Internet and Transborder Data

- Flows an Australian Perspective”, **Masaryk University Journal of Law and Technology**, C. 4, S. 1, 2010, s. 1-20, (Data Flows).
- Svantesson, Dan Jerker B.: “The Regulation of Cross-Border Data Flow”, **International Data Privacy Law**, C. 1, S. 3, 2011, s. 180-198, (Cross-Border Data Flow).
- Sveinbjarnardóttir, Þorgerður Jóhanna: “The Concept of “Transfer” of Data under European Data Protection Law: In the Context of Transborder Data Flows”, Master Thesis, University of Oslo, 2015.
- Şimşek, Oğuz: **Anayasa Hukukunda Kişisel Verilerin Korunması**, İstanbul, Beta Basım, 2008.
- Taştan, Furkan Güven: **Türk Sözleşme Hukukunda Kişisel Verilerin Korunması**, İstanbul, On İki Levha, 2017.
- Tepe, Esra: **Kişisel Verilerin Korunması: Özel Hukuk Açısından Avrupa İnsan Hakları Mahkemesi İçtihatları Işığında**, Ankara, Adalet, 2021.
- Theodorakis, Nikolaos I.: “Cross Border Data Transfers Under the GDPR: The Example of Transferring Data from the EU to the US”, Transatlantic Technology Law Forum Working Papers №39, Ed.: Siegfried Fina, Mark Lemley, and Roland Vogl, 2018.
- Toparlak, Rüya Tuna: **Veri Koruması Hukukunda Bağlayıcı Şirket Kuralları: 2016/679 sayılı Genel Veri Koruma**

Tüzüğü ve 6698 sayılı Kişisel Verilerin Korunması Kanunu Karşılaştırılması, İstanbul, On İki Levha, 2021.

Tunçer, Polat: **Sağlık Hukuku Temel Bilgileri**, 2. bs, Ankara, Adalet, 2017.

Ustaran, Eduardo: “International Data Transfers”, **Data Protection: A Practical Guide to UK and EU Law** içinde, Ed.: Peter Carey, 5. bs., Oxford, Oxford University Press, 2018, s. 105-121.

Ünsal Özden, Sevgi/
Uz, İdil/
Karamustafaoğlu, Mert: “Kişisel Veri Aktarımı ve Bankacılık Kanunu Madde 73 Değişikliği”, **Kişisel Verileri Koruma Dergisi**, C. 3, S. 1, 2020, s. 17-39.

van den Bulck, Paul: “Transfers of Personal Data to Third Countries”, **ERA Forum**, C. 18, S. 2, 2017, s. 229-247.

Voigt, Paul/ von dem Bussche, Axel: **The EU General Data Protection Regulation (GDPR): A Practical Guide**, Berlin, Springer International Publishing, 2017.

Voss, W. Gregory: “Cross-Border Data Flows, the GDPR, and Data Governance”, **International Law Journal**, C. 29, S. 3, 2020, s. 485-532.

Wagner, Julian: “The Transfer of Personal Data to Third Countries under the GDPR: When Does a Recipient Country Provide an Adequate Level of Protection?”, **International Data Privacy Law**, C. 8, S. 4, 2018, s. 318-337.

- Weber, Rolf H.: “Transborder Data Transfers: Concepts, Regulatory Approaches and New Legislative Initiatives”, **International Data Privacy Law**, C. 3, S. 2, 2013, s. 117-130.
- White House: “Fact Sheet: United States and European Commission Announce Trans-Atlantic Data Privacy Framework”, 25.03.2022, (çevrimiçi), [whitehouse.gov/briefing-room/statements-releases/2022/03/25/fact-sheet-united-states-and-european-commission-announce-trans-atlantic-data-privacy-framework/](https://www.whitehouse.gov/briefing-room/statements-releases/2022/03/25/fact-sheet-united-states-and-european-commission-announce-trans-atlantic-data-privacy-framework/), 12.06.2022.
- Wolf, Christian: “Delusions of Adequacy? Examining the Case for Finding the United States Adequate for Cross-Border EU-U.S. Data Transfers”, **Washington University Journal of Law & Policy**, C. 43, S. 227, 2014, s. 227-257.
- World Health Organization: “Health Systems Financing”, Haziran 2008, (çevrimiçi) [who.int/healthinfo/statistics/toolkit_hss/en_pdf_toolkit_hss_financing.pdf](https://www.who.int/healthinfo/statistics/toolkit_hss/en_pdf_toolkit_hss_financing.pdf), 12.06.2022.
- Yılmaz, Sabire Sanem: **Tıp Alanında Kişisel Verilerin Korunması**, 5. bs., Ankara, Seçkin, 2021.
- Yılmaz, Süleyman/
Çavuşoğlu, Gökçe Filiz: **Kişisel Verileri Koruma Hukuku**, Ankara, Yetkin, 2020.

Yücedağ, Nafiye: “Kişisel Verilerin Korunması Kanunu Kapsamında Genel İlkeler”, **Kişisel Verileri Koruma Dergisi**, C. 1, S. 1, 2019, s. 47-63, (Genel İlkeler).

Yücedağ, Nafiye: “Medeni Hukuk Açısından Kişisel Verilerin Korunması Kanunu’nun Uygulama Alanı ve Genel Hukuka Uygunluk Sebepleri”, **İstanbul Üniversitesi Hukuk Fakültesi Mecmuası**, C. 75, S. 2, 2017, s. 765-786, (Hukuka Uygunluk Sebepleri).

Zor, Abdülhamid: **Veri Sorumlusunun Yükümlülükleri ve Bu Yükümlülüklerin İhlalinden Doğan Özel Hukuk Sorumluluğu**, İstanbul, On İki Levha, 2020.