İSTANBUL BİLGİ ÜNİVERSİTESİ

LİSANSÜSTÜ PROGRAMLAR ENSTİTÜSÜ

HUKUK YÜKSEK LİSANS PROGRAMI

AVRUPA BİRLİĞİ GENEL VERİ KORUMA TÜZÜĞÜ (GDPR) KAPSAMINDA AB DIŞINA KİŞİSEL VERİ AKTARIMI

Nadin SERTÇE

118615062

Dr. Ögr. Üyesi Nilgün BAŞALP YILDIRIM

İSTANBUL

2022

Avrupa Birliği Genel Veri Koruma Tüzüğü (GDPR) Kapsamında
AB Dışına Kişisel Veri Aktarımı

Transfer of Personal Data Outside the EU Under the European Union General Data Protection Regulation (GDPR)

Nadin SERTÇE
118615062

Tez Danışmanı : **Dr. Ögr. Üyesi Nilgün BAŞALP YILDIRIM** (İmza) .....
İstanbul Bilgi Üniversitesi

Jüri Üyeleri : **Dr. Öğr. Üyesi Pınar ARTIRAN** (İmza) .....
İstanbul Bilgi Üniversitesi

Doç. Dr. Selin SERT SÜTÇÜ (İmza) .....
Akdeniz Üniversitesi

Tezin Onaylandığı Tarih : 21.01.2022
Toplam Sayfa Sayısı : 191

Anahtar Kelimeler (Türkçe)	Anahtar Kelimeler (İngilizce)
1) Kişisel Veri	1) Personal Data
2) Genel Veri Koruma Tüzüğü	2) General Data Protection Regulation
3) Kişisel Verilerin Aktarımı	3) Transfer of Personal Data
4) Schrems II	4) Schrems II
5) Sınıraşan Kişisel Veri Aktarımı	5) Cross-Border Transfer of Personal Data

İÇİNDEKİLER

KISALTMALAR

108 Sayılı Sözleşme	:	108 sayılı Kişisel Verilerin Otomatik İşleme Tabi Tutulması Karşısında Bireylerin Korunması Sözleşmesi
181 Sayılı Ek Protokol		108 sayılı Kişisel Verilerin Otomatik İşleme Tabi Tutulması Karşısında Bireylerin Korunması Sözleşmesine Ek Denetleyici Makamlar ve Sınıraşan Veri Akışına İlişkin Protokol
182/2011 sayılı Tüzük	:	Üye Devletler tarafından Komisyonun uygulama yetkilerini kullanılması için kontrol mekanizmalarına ilişkin kurallar ve genel ilkelere dair 182/2011 Tüzüğü (Avrupa Birliği)
2016/680 sayılı Direktif	:	AB Polis ve Yargı Direktifi (Law Enforcement Directive)
95/46 sayılı Direktif	:	95/46/EC Kişisel Verilerin İşlenmesi ve Bu Tür Verilerin Serbest Dolaşımına Dair Bireylerin Korunması Direktifi
AB	:	Avrupa Birliği
ABAD	:	Avrupa Birliği Adalet Divanı
ABD	:	Amerika Birleşik Devletleri
AEA	:	Avrupa Ekonomik Alanı
APEC	:	Asia Pacific Economic Cooperation
BCR	:	Binding Corporate Rules (Bağlayıcı Şirket Kuralları)
Bilgi IT law Institute	:	Bilgi Information Technology Law Institute (Bilişim ve Teknoloji Hukuku Enstitüsü)
Bkz.	:	Bakınız
CBP	:	ABD Gümrük ve Sınır Koruma Bürosu (US Bureau of Customs and Border Protection)
dn.	:	Dipnot

DOC	:	United States Department of Commerce (ABD Ticaret Bakanlığı)
DOT	:	United States Department of Transportation (ABD Ulaştırma Bakanlığı)
DPA	:	Data Protection Authority (Veri Koruma Yetkilisi)
EC	:	European Commission (Komisyon)
EDPB	:	European Data Protection Board (Avrupa Veri Koruma Kurulu)
EDPS	:	European Data Protection Supervisor (Avrupa Veri Koruma Denetçisi)
ETS	:	European Treaty Series
EU	:	European Union
EUROJUST	:	European Union Agency for Criminal Justice Cooperation
EUROPOL	:	European Union Agency for Law Enforcement Cooperation
FISA	:	Foreign Intelligence Surveillance Act. (ABD Dış İstihbarat Gözetleme Yasası)
FTC	:	The Federal Trade Commission (Federal Ticaret Komisyonu)
GC	:	Grand Chamber
GDPR	:	General Data Protection Regulation (2016/679 sayılı Avrupa Birliği Genel Veri Koruma Tüzüğü)
ICO	:	Information Commisioner's Officer (Birleşik Krallık Bilgi Komiseri)
IT	:	Information Technology
Komisyon	:	Avrupa Komisyonu
Kurul	:	Kişisel Verileri Koruma Kurulu
Kurum	:	Kişisel Verileri Koruma Kurumu
KVKK	:	6698 sayılı Kişisel Verilerin Korunması Kanunu
m.	:	Madde

MLAT	:	Mutual Legal Assistance Treaty (Karşılıklı Adli Yardım Anlaşması)
NSA		US National Security Agency (ABD Ulusal Güvenlik Ajansı)
OECD	:	Organisation for Economic Co-operation and Development
Opinion 1/15	:	ABAD'ın 1/15 Sayılı Görüşü
para.	:	Paragraf
PNR	:	Passanger Name Record (Yolcu Adı Kaydı)
Sözleşme 108+		Kişisel Verilerin İşlenmesine İlişkin Olarak Bireylerin Korunması için Modernize Edilmiş Sözleşme (Convention 108+)
s.	:	Sayfa
Şart	:	Avrupa Birliği Temel Haklar Şartı
T.C.	:	Türkiye Cumhuriyeti
TFEU	:	Avrupa Birliği'nin İşleyişine İlişkin Antlaşma
WP29	:	Article 29 Working Party (Madde 29 Çalışma Grubu)

ŞEKİL LİSTESİ

TABLO LİSTESİ

ABSTRACT

Cross-border transfers of personal data have greatly increased due to the development of technology and the widespread use of the internet. With this increase, concerns about data protection have emerged and countries have made legal arrangements in their domestic laws to protect personal data based on these concerns. In the legal regulations made, it is seen that while some countries legislations provide data protection at an advanced level, some countries legislations cannot provide this level. These differences between the legislation of the countries regarding data protection may cause the data to remain unprotected in the place where it is transferred. For this reason, the cross-border transfer of personal data is regulated separately within the legal regulations for data protection. The personal data transfer mechanisms included in the European Union General Data Protection Regulation (“GDPR”) numbered 2016/679, which is the current data protection legislation of the European Union ("EU"), have been arranged in order to ensure the level of protection provided for personal data in the EU in third countries, taking into account the risks that the legal legislation of third countries may pose from being different from that of the EU.

The aim of this study is to examine the general framework of the transfer of personal data outside the EU regulated in GDPR and data transfer mechanisms in legislation and practice. In this context, first of all, the concept of "transfer to third countries" has been defined and general principles regarding the transfer have been mentioned in order to understand the transfer of personal data and to determine when the provisions regarding the transfers in the GDPR will be applied. Afterwards, the transfer mechanisms in the GDPR were examined in detail in terms of purpose, effectiveness and function. Then, the mentioned mechanisms were interpreted in the light of the current and past decisions of the Court of Justice of the European Union (“CJEU”), especially the Schrems I and Schrems II decisions, and the effects of the decisions on the transfer mechanisms were evaluated. The study is based on the documents of the Article 29 Working Party (“WP29”) and the European Data

Protection Board (“EDPB”), which show how the provisions of the GDPR regulating the transfer to third countries and international organizations will be applied in practice and interpret the said provisions.

In the last part of the study, the transfer of personal data abroad is examined in Turkish Law and the effects of the current decisions of the Personal Data Protection Board (“Board”) on data transfer are discussed. Finally, Law on Protection of Personal Data (“KVKK”) and GDPR were compared, and based on the comparison, suggestions were made regarding the issues needed for the development of KVKK.

Keywords: Personal Data, General Data Protection Regulation, Transfer of Personal Data, Schrems II, Cross-Border Transfer of Personal Data.

ÖZET

Kişisel verilerin sınır ötesi aktarımları, teknolojinin gelişmesine ve internet kullanımının yaygınlaşmasına bağlı olarak büyük oranda artış göstermiştir. Bu artışla birlikte veri korumasına ilişkin endişeler ortaya çıkmış ve bu endişelere istinaden ülkeler kişisel verileri korumak için iç hukuklarında yasal düzenlemeler yapmıştır. Yapılan yasal düzenlemelerde veri korumasını bazı ülke mevzuatları ileri düzeyde sağlarken bazı ülke mevzuatlarının bu düzeyde sağlayamadığı görülmektedir. Veri korumasına ilişkin ülkelerin mevzuatları arasındaki bu farklılıklar verilerin aktarıldığı yerde korumasız kalmasına sebep olabilmektedir. Bu nedenle kişisel verilerin sınır ötesi aktarımı, veri korumasına yönelik yasal mevzuatlar içerisinde ayrıca düzenlenmiştir. Avrupa Birliği'nin ("AB") güncel veri koruma mevzuatı olan 2016/679 sayılı Avrupa Birliği Genel Veri Koruma Tüzüğü'nde ("GDPR") yer alan kişisel veri aktarım mekanizmaları da, üçüncü ülkelerin yasal mevzuatlarının AB'ninkinden farklı olmasının meydana getireceği riskleri dikkate alarak, AB içinde kişisel veriler için sağlanan koruma seviyesinin üçüncü ülkelerde de aynı düzeyde sağlanması amacıyla düzenlenmiştir.

Bu çalışmanın amacı, GDPR'da düzenlenen kişisel verilerin AB dışına aktarımının genel çerçevesini ve veri aktarım mekanizmalarını mevzuat ve uygulamada incelemektir. Bu kapsamda, öncelikle kişisel verilerin aktarılması konusunun anlaşılabilmesi ve GDPR'da yer alan aktarımlara ilişkin hükümlerin ne zaman uygulanacağının belirlenebilmesi açısından "üçüncü ülkelere aktarım" kavramı tanımlanarak aktarıma ilişkin genel ilkelerden bahsedilmiştir. Sonrasında GDPR'da yer alan aktarım mekanizmaları, amaç, etkinlik ve işleyiş açısından detaylı olarak incelenmiştir. Ardından söz konusu mekanizmalar, başta Schrems I ve Schrems II kararları olmak üzere Avrupa Birliği Adalet Divanı'nın ("ABAD") güncel ve geçmiş kararları ışığında yorumlanarak, kararların aktarım mekanizmalarına etkisi değerlendirilmiştir. Çalışmada, Madde 29 Çalışma Grubu (Article 29 Working Party – "WP29") ve Avrupa Veri Koruma Kurulu'nun ("EDPB") GDPR'ın üçüncü ülkelere ve uluslararası kuruluşlara transferini düzenleyen hükümlerinin pratikte

nasıl uygulanacağını gösteren ve söz konusu hükümleri yorumlayan belgeleri esas alınmıştır.

Çalışmanın son bölümünde, yurtdışına kişisel veri aktarımı Türk Hukuku'nda incelenmiş ve Kişisel Verileri Koruma Kurulunun ("Kurul") güncel kararlarının veri aktarımına etkileri ele alınmıştır. Son olarak, Kişisel Verileri Koruma Kanunu ("KVKK") ile GDPR'ın karşılaştırması yapılmış ve yapılan karşılaştırmaya istinaden, KVKK'nın gelişimi için ihtiyaç duyduğu hususlara ilişkin önerilerde bulunulmuştur.

Anahtar Kelimeler: Kişisel Veri, Genel Veri Koruma Tüzüğü, Kişisel Verilerin Aktarımı, Schrems II, Sınıraşan Kişisel Veri Aktarımı.

GİRİŞ

Teknolojik gelişme ve dijitalleşme ile birlikte internet kullanımının hızla arttığı bir dünyada, kişisel verilerin[1] sınır ötesine aktarılması ekonomik, ticari ve teknolojik büyüme ve sosyal etkileşim açısından oldukça önemli bir hale gelirken, sınır ötesine aktarılan kişisel verilerin nasıl korunabileceğine dair endişeler de her geçen gün artmaktadır. Kişisel verileri ülke içinde muhafaza etmek veri odaklı ekonomilerde gittikçe daha zor hale gelmekte, dijitalleşmenin ve gelişen teknolojinin etkisiyle verilerin dünya üzerinde dolaşımı hızlı ve kolay bir şekilde gerçekleşmektedir. Söz konusu endişelerin bir sonucu olarak veri korumasına ilişkin yasal düzenlemeler oluşturan ülkeler, ilgili düzenlemelerde aktarılan veriler açısından kişisel verilerin korunmasına ayrı bir önem vermektedir.

Farklı ülkelerde bulunmalarından dolayı, kişisel veri aktarımlarında taraf olan veri aktaran[2] ve veri aktarılanların[3] tabi oldukları ülkelerin veri korumasına ilişkin yasal düzenlemelerinde doğal olarak farklılıklar bulunmaktadır. Bu farklılıkların bir sonucu olarak her iki tarafın kişisel veriler için sağladığı koruma düzeyi de eşit olmamaktadır. Dolayısıyla verilerin aktarıldığı ülkede veri korumasının zayıflaması, verilerin bulunduğu ülkelerde veri korumasına ilişkin yapılan yasal düzenlemelerde veri aktarımlarına ilişkin özel hükümlere yer verilerek kişisel verilerin serbest akışının kısıtlanması ve bazı şartlara tabi tutulması sonucunu doğurmuştur. Yapılan bu düzenlemeler ile kişisel verilerin kontrolsüz akışının ve korumasız kalmasının önüne geçilmeye çalışılmıştır. AB özelinde ise aktarılan veriler için AB'de sağlanan korumaya eşdeğer bir korumanın verilerin aktarıldığı ülkede de sağlanması amaçlanmıştır. Bu bağlamda kişisel verilerin korunması veri

[1] GDPR m.4(1), "kişisel veriyi" tanımlanmış veya tanımlanabilir bir gerçek kişiye ilişkin her türlü bilgi olarak tanımlamıştır.

[2] "Veri Aktaran" kavramı GDPR'da tanımlanmamış olup kavram kişisel verilerin sınır ötesi aktarımı bağlamında kullanılmakta ve kişisel verileri bulunduğu ülkeden bir başka ülkeye aktaran veri sorumlusu veya veri işleyen olarak tanımlanmaktadır. Veri aktaranlar, gerçek veya tüzel kişi/kişiler, kamu otoritesi/kuruluşları veya kurum/kuruluşlar olabilir.

[3] "Veri Aktarılan" kavramı GDPR'da tanımlanmamış olup kavram kişisel verilerin sınır ötesi aktarımı bağlamında kullanılmakta ve üçüncü bir ülkede bulunan ve veri aktarandan kişisel verileri alan veya bu verilere erişim sağlayan bir veri sorumlusu veya veri işleyen olarak tanımlanmaktadır.

akışını engellemeyi değil, veri akışlarının artmasından dolayı oluşan endişeleri gidermek için veri akışlarının kişisel verilerin zarar görmeyeceği şekilde gerçekleşmesini amaçlamaktadır[4]. Bu sebepledir ki kişisel verilerin sınır ötesine aktarımı mutlak olarak yasaklanamaz[5].

Geçmişten günümüze kadar uluslararası veri akışlarına ilişkin önemli düzenlemeler, dünya genelinde Ekonomik İşbirliği ve Kalkınma Teşkilatı'nın Mahremiyetin Korunması ve Kişisel Verilerin Sınır Ötesi Akışlarına İlişkin Kılavuz İlkeleri (OECD Gizlilik İlkeleri), Kişisel Verilerin Otomatik İşleme Tabi Tutulması Karşısında Bireylerin Korunması Sözleşmesi ("108 Sayılı Sözleşme") ve Asya-Pasifik Ekonomik İşbirliği (APEC) Gizlilik Çerçevesi (APEC Gizlilik Çerçevesi) olmakla beraber Avrupa özelinde 95/46/EC Kişisel Verilerin İşlenmesi ve Bu Tür Verilerin Serbest Dolaşımına Dair Bireylerin Korunması Direktifi[6] (The Data Protection Directive - "95/46 sayılı Direktif") ve Avrupa Birliği Genel Veri Koruma Tüzüğü'dür[7] (General Data Protection Regulation – "GDPR").

[4] Oğulcan Özkan, "Kişisel Verilerin Korunması", Yüksek Lisans Tezi, Ankara Üniversitesi, 2019, s.161.
[5] Elif Küzeci, *Kişisel Verilerin Korunması*, 3. Baskı, Ankara: Oniki Levha Yayınları, 2019, s.357.
[6] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (1995) OJ L281/31 ("95/46/EC Sayılı Kişisel Verilerin İşlenmesi ve Serbest Dolaşımı Bakımından Bireylerin Korunmasına İlişkin Avrupa Parlamentosu ve Avrupa Konseyi Direktifi") (Bundan sonra "95/46 sayılı Direktif" olarak anılacaktır.), https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A31995L0046, Erişim Tarihi: 04.01.2022.
[7] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (2016) L 119/1 (bundan sonra "GDPR" olarak anılacaktır), https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679, Erişim Tarihi: 14.10.2021.

AB'de veri korumasına ilişkin güncel mevzuat olan ve Mayıs 2018 de yürürlüğe giren GDPR[8], 1995 yılında kabul edilen 95/46 sayılı Direktif[9]ten bu yana AB veri koruma mevzuatındaki en önemli yasal gelişme olarak görülmektedir[10]. GDPR, AB'nin birincil hukuku olan Avrupa Birliği'nin İşleyişine İlişkin Antlaşma[11] (The Treaty on the Functioning of European Union – "TFEU") ve Avrupa Birliği Temel Haklar Şartı'nın[12] (Charter of Fundamental Rights of the European Union – "Şart") gerektirdiği özel hayata saygı ve mahremiyet ilkeleri esas alınarak oluşturulmuştur. Bu noktada GDPR'ın, aktarılan kişisel verilerin yasal güvenceler yoluyla korunması amacıyla temel hak ve özgürlükleri esas alarak hazırlandığı görülmektedir. GDPR, AB içinde kişisel verilerin serbest akışına izin vererek temel hakları korumayı amaçlamıştır[13]. GDPR m.1(3)'de yer alan kişisel verilerin Birlik içinde serbest dolaşımının kısıtlanamayacağı ve yasaklanamayacağına ilişkin hüküm ile Birlik içinde aynı veri koruma seviyesinin sağlanması amaçlanmıştır. Bu amaç doğrultusunda GDPR, AB vatandaşlarının kişisel verilerine Birlik içinde sağladığı bu korumayı AB sınırları dışında da sürdürebilmek için daha düşük veri koruma seviyesi ile verilerin aktarılmasına izin vermeyecek şekilde düzenlenmiştir.

[8] 27 Nisan 2016 tarihinde AB Parlamentosu tarafından kabul edilen ve iki yıllık bir uyum sürecinin ardından 25 Mayıs 2018 tarihinde yürürlüğe giren GDPR, 95/46/EC sayılı Direktif'i yürürlükten kaldırmıştır. Tüzük statüsünde olduğundan dolayı GDPR, AB çatısı altındaki tüm üye ülkelerde direkt bağlayıcı olmuş ve üye ülkelerde herhangi bir yasal düzenleme gerektirmeden uygulanması mümkün olmuştur. Bu çerçevede veri koruma hukuku açısından AB üyesi ülkelerde farklı yasal düzenlemelerin yarattığı sorunların önüne geçilmesi ve veri koruma hukukunun AB çatısı altında uyumlaştırılması amaçlanmıştır.

[9] AB üye ülkelerinin 108 Sayılı Sözleşme ve OECD Rehber İlkelerini dikkate alarak hazırladıkları kendi iç veri koruma mevzuatları, her üye ülkede farklı uygulamalara sahipti. Bu farklılıkların AB'nin ortak pazar amacına hizmet etmediği düşüncesiyle ve AB içinde yeknesaklık sağlamak amacıyla AB Komisyonu, kişisel verilerin işlenmesi ve serbest dolaşımı hakkında 1990 yılında bir taslak yönerge hazırlamıştır. Söz konusu taslak yönergenin eleştirilere maruz kalması sebebiyle 1992 yılında tekrar bir taslak yönergesi hazırlanmış ve 95/46/EC Sayılı Kişisel Verilerin İşlenmesi ve Bu Tür Verilerin Serbest Dolaşımına Dair Bireylerin Korunması Direktifi olarak 24 Ekim 1995 tarihinde kabul edilip 25 Ekim 1998 tarihinde yürürlüğe girmiştir.

[10] Nikolaos I. Theodorakis, "Cross Border Data Transfers Under the GDPR: The Example of Transferring Data from the EU to the US", *TTLF Working Papers*, 39/1 (2018), s.2.

[11] Bkz. Consolidated version of the Treaty on the Functioning of the European Union, (2012), OJ C 326/47.

[12] European Union, "Charter of Fundamental Rights of the European Union", OJ 2012 / C 326.

[13] 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*, 8/4 (2018) , s.320.

Gerek 95/46 sayılı Direktif gerekse GDPR, üçüncü ülkelere veri aktarımı kavramını tanımlamamasına rağmen kişisel verilerin üçüncü ülkelere aktarılmasına ilişkin hükümler içermektedir. Ayrıca GDPR, tıpkı 95/46 sayılı Direktifte olduğu gibi AB dışına[14] veri[15] aktarımını kısıtlamakta ve üçüncü ülkelere veri aktarımı için bir takım aktarım mekanizmaları öngörmektedir. GDPR, veri aktaran ve veri aktarılanların verilerin AB standardı ile eşdeğer seviyede korunmasını taahhüt etmeleri şartıyla, kişisel verilerin üçüncü bir ülkeye veya uluslararası bir kuruluşa aktarılmasına ilişkin mekanizmaları 5. Bölümde düzenlemektedir.

GDPR 5. Bölümde yer alan aktarım mekanizmaları, AB Hukukunun gerektirdiği veri korumasını verilerle birlikte üçüncü ülkelere aktararak kişisel veriler için AB içinde sağlanan koruma seviyesini üçüncü ülkelerde de sağlamayı amaçlamaktadır. Dünyanın geldiği noktada, birçok işlem sınır ötesi işbirliği ve yurtdışı hizmetlerin kullanımını gerektirmektedir. AB'de bulunan birçok şirket maliyet avantajı sağlamasından dolayı işledikleri verileri AB dışında bulunan bulut depolama sistemlerinde depolamayı tercih etmekte ve bu da AB'den üçüncü ülkelere veri aktarımını kaçınılmaz hale getirmektedir. Dolayısıyla GDPR 5. Bölümün anılan amaç doğrultusunda düzenlenmesi de, kaçınılmaz hale gelen veri aktarımları için önemli bir ihtiyaçtır. Bu doğrultuda bu çalışmanın amacı GDPR kapsamında AB dışına veri aktarımını analiz etmek olacaktır. Bu çerçevede çalışmada, GDPR'da yer alan kişisel verilerin aktarımı hususu uzun yıllardır AB Hukukunda oluşan mahkeme içtihatları ışığında incelenecek ve Türk Hukuku ile karşılaştırılacaktır. Çalışmanın sonucunda da, hem GDPR özelinde AB Hukukunun kişisel verilerin aktarımına ilişkin bakış açısı değerlendirilecek hem de Türk Hukukunun konuyla ilgili ihtiyaç duyduğu hususlara ilişkin önerilerde bulunulacaktır. AB ile Türkiye siyasi, ekonomik ve ticari gibi birçok alanda işbirliği içinde olduğundan

[14] AB serbest veri akış alanına, Avrupa Ekonomi Alanı (AEA) Anlaşması ile AB yasasını benimseyen İzlanda, Norveç ve Lihtenştayn da dâhil edilmiştir. Bu çerçevede AB veri koruma ilkelerinin uygulama alanı bu üç ülkeyi de kapsayacak şekilde genişlemiştir. Bu nedenle bu çalışmada kullanılan "AB dışına/AB içinde/AB ülkeleri" ifadeleri ile sırasıyla "AEA dışına/AEA içinde/AEA ülkeleri" ifadeleri kastedilmektedir.

[15] Bu çalışmada bahsedilen AB dışına aktarımlara konu olan veriler, tanımlanmış veya tanımlanabilir bir gerçek kişiye ait olan kişisel verileri ifade etmektedir.

Türkiye'nin AB'de yer alan regülasyonlara uyum sağlaması önem arz etmektedir. Bu sebeple, bu çalışmada AB Hukuku temel alınmış olsa da Türk Hukukunda kişisel verilerin aktarımına ilişkin hususlar, GDPR'a ve dolayısıyla da AB'ye uyum sağlanması açısından incelenecektir.

Çalışmada, Avrupa ve Türk Hukukunda kişisel verilerin korunmasının tarihsel gelişimine, literatürde bu konuyu detaylı olarak ele alan birçok kaynak bulunduğu için değinilmemiştir[16]. Bu kapsamda çalışmada, tarihsel gelişimden ziyade çalışmanın ana konusu olan kişisel verilerin AB dışına aktarımı konusu detaylı olarak ele alınacaktır.

[16] Kişisel verilerin korunması hukukunun Avrupa ve Türk Hukukundaki tarihsel gelişim için bkz. Küzeci, *Kişisel Verilerin Korunması*; Murat Volkan Dülger, *Kişisel Verilerin Korunması Hukuku*, İstanbul: Hukuk Akademisi, 2020.

1 KİŞİSEL VERİLERİN ÜÇÜNCÜ ÜLKELERE AKTARILMASINA İLİŞKİN GENEL HUSUSLAR

1.1 Üçüncü Ülkelere Aktarım Kavramı

GDPR ve 95/46 sayılı Direktif'te kişisel verilerin "üçüncü ülkelere veya uluslararası bir kuruluşa aktarılması" kavramının tanımı yapılmamıştır. Bu kavramın netliğe kavuşturulması, AB'de veri sorumlusu[17] veya veri işleyen[18] tarafından gerçekleştirilen veri işlemenin üçüncü bir ülkeye veya uluslararası bir kuruluşa aktarım oluşturup oluşturmayacağının ve buna bağlı olarak veri sorumlusu ve veri işleyenin GDPR 5. Bölümde yer alan hükümlere uymalarına gerek olup olmadığının belirlenmesi açısından gerekli ve önemlidir[19]. ABAD'ın "üçüncü ülkelere aktarım" kavramını tartıştığı tek ve bu konuyu ele aldığı ilk içtihadı olan Lindqvist davası[20] ise üçüncü ülkelere aktarım kavramını tanımlamada sınırlı bir kapsama sahiptir[21].

Lindqvist davasında ABAD diğer şeylerin yanı sıra, kişisel verilerin üye devletteki bir kişi (söz konusu davada Bodil Lindqvist) tarafından o devlette veya başka bir üye devlette yerleşik bir sağlayıcı tarafından depolanan bir internet sayfasına yüklenmesinin 95/46 sayılı Direktif m.25 uyarınca bir aktarım olup olmadığını analiz eder[22]. ABAD Lindqvist kararında AB'de bulunan bir sunucuda depolanan

[17] "Veri Sorumlusu" GDPR m.4(7)'de kişisel verilerin işlenmesinin amacını ve araçlarını (tek başına veya birlikte) belirleyen herhangi bir gerçek veya tüzel kişiyi, kamu kuruluşu, kurumu veya diğer herhangi bir organdır.
[18] "Veri işleyen" GDPR m.4(8)'de veri sorumlusu adına kişisel verileri işleyen bir gerçek veya tüzel kişi, kamu kuruluşu, kurumu veya diğer herhangi bir organdır.
[19] European Data Protection Board (EDPB), "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, s.4, https://edpb.europa.eu/our-work-tools/documents/public-consultations/2021/guidelines-052021-interplay-between-application_en, Erişim tarihi: 22.12.2021.
[20] Court of Justice of the European Union (CJEU), Case C-101/01, *Bodil Lindqvist*, 2003 E.C.R. I-12971.
[21] Paul Van den Bulck, "Transfers of Personal Data to Third Countries", *ERA Forum*, 18/2 (2017), https://doi.org/10.1007/s12027-017-0482-3. s.230.
[22] 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*, Ankara: Ocak 2009, s.21.

ve internet üzerinden dünya çapında erişilebilen bir web sitesinde veri paylaşmanın 95/46 sayılı Direktif m.25'e göre üçüncü bir ülkeye veri aktarımı teşkil etmediğini tespit etmiştir[23]. Söz konusu davada ABAD, yalnızca verilerin pasif bir eylem ile üçüncü bir ülkedeki kişiler de dâhil olmak üzere internete bağlanan herkes tarafından erişilebilir hale getirilmesinin yeterli olmadığı, aktarımın gerçekleşmesi için veri aktaranın verileri doğrudan göndermesi, kullanıcılarında bu bilgiye erişmek için aktif bir eylemde bulunması gerektiğini belirtmiştir[24]. Lindqvist davasında ABAD, davadaki sonuca asıl yargılamadaki koşulları esas alarak vardığından dolayı uluslararası aktarım kavramına ilişkin varmış olduğu sonucun aktarım ile ilgili farklı koşullara sahip davalara otomatik olarak uygulanmayacağını belirtmiştir[25].

Avrupa Veri Koruma Denetçisi[26] (European Data Protection Supervisor – "EDPS"), 2014 yılında yayınladığı bir durum belgesinde kişisel veri aktarımına ilişkin bazı önemli unsurlara dikkat çekmiş ve bu çerçevede kişisel veri aktarımı kavramını "(…) *Tüzük'e tabi bir göndericinin, alıcının/alıcıların erişime sahip olacağı bilgisi veya niyetiyle gerçekleştirilen kişisel verilerin iletilmesi, ifşa edilmesi veya başka bir şekilde kullanıma sunulması"* şeklinde tanımlamıştır[27]. Bu belge kapsamında kişisel veri aktarımı kavramı, alıcılar tarafından erişilen veriler açısından hem kasıtlı aktarımları hem de izin verilen erişimleri ifade eder. Bu kapsamda söz konusu belgede EDPS, verilerin AB'deki bir veri sorumlusu tarafından AB dışındaki bir alıcıya posta veya e-posta ile gönderilmesi, veri sorumlusu tarafından kişisel verilerin internette yayınlanması, verilerin veri sorumlusunun veri tabanından AB dışı bir alıcıya iletilmesi, AB dışındaki bir

[23] Case C-101/01, *Bodil Lindqvist*, para.69-70.
[24] Case C-101/01, *Bodil Lindqvist*, para.61-62.
[25] European Data Protection Supervisor (EDPS), "The transfer of personal data to third countries and international organisations by EU institutions and bodies", Position Paper, 14.07.2014, s.7, https://edps.europa.eu/sites/edp/files/publication/14-07-14_transfer_third_countries_en.pdf, Erişim Tarihi: 11.10.2021.
[26] Avrupa Veri Koruma Denetçisi (European Data Protection Supervisor-"EDPS"), 2004 yılında kurulmuştur. EDPS, Avrupa kurum ve kuruluşlarının, kişisel verileri işlerken ve yeni politikalar geliştirirken gizlilik ve veri koruma hakkına saygı duyulmasını sağlamayı amaçlayan bağımsız bir denetim makamıdır.
[27] EDPS,"The transfer of personal data", s.7.

alıcıya bir AB veri denetleyicisinin veri tabanına erişim izni verilmesi gibi durumları kişisel verilerin uluslararası aktarımına örnek olarak vermiştir[28].

ABAD Schrems I[29] kararında uluslararası veri aktarımı kavramını belirli bir tanım ile açıklamak yerine Şart'ın gerektirdiği veri koruma seviyesi ile ilişkilendirmiş ve bu çerçevede kavramı üçüncü ülkelere gönderilen veya erişilebilir hale getirilen kişisel verilerin AB standartlarına uygun olarak yüksek düzeyde koruma gerektirmesi açısından ele almıştır[30].

EDPB[31], 2021 yılında yayınladığı bir tavsiye raporunda kişisel verileri AB dışında bulunan bir bulutta depolamanın veya üçüncü bir ülkeden kişisel verilere uzaktan erişimin aktarım olarak kabul edildiğini tespit etmiştir[32]. Bu örnekler çerçevesinde kişisel verilerin üçüncü ülkelere aktarılması ile sonuçlanacak bu aktarımların GDPR 5. Bölümde yer alan hükümlere uygun olarak yapılması gerektiği açıktır. Ayrıca aktarım kavramı "yayma veya kullanıma sunma", "iletim yoluyla açıklama" gibi GDPR m. 4(2)'de belirtilen işleme faaliyetlerini de içereceğinden kişisel veri aktarımlarının GDPR'ın veri işlemeye ilişkin diğer ilgili tüm hükümlerine de uygun olarak gerçekleştirilmesi gerekecektir. Burada değinilmesi gereken bir önemli hususta aktarımın "transit aktarım" kavramı ile aynı anlama gelmediği ve bu noktada kişisel verilerin bir AB ülkesinden başka bir AB ülkesine üçüncü bir ülke

[28] EDPS,"The transfer of personal data, s.7.
[29] Court of Justice of the European Union (CJEU), C-362/14, *Maximilian Schrems v. Data Protection Commissioner [GC] ("Schrems I"*), 6 October 2015.
[30] Christopher Kuner, Lee Bygrave ve Christopher Docksey, *The EU General Data Protection Regulation (GDPR): A Commentary*, Oxford University Press, 2020, s.763.
[31] Avrupa Veri Koruma Kurulu (European Data Protection Board-"EDPB"), GDPR'ın tutarlı bir şekilde uygulanmasını sağlamak ve AB'nin ulusal denetim makamları arasında işbirliğini teşvik etmek amacıyla oluşturulan bağımsız bir kuruluştur. EDPB, GDPR'ın yürürlüğe girmesiyle birlikte 25 Mayıs 2018'de WP29'un yerini almıştır. GDPR'ın 68. maddesiyle oluşturulan EDPB, AB üyesi ülkelerin ulusal denetim makamı başkanları ve temsilcileri ile Avrupa Veri Koruma Denetçiliği (EDPS) temsilcilerinden oluşmaktadır. EDPB, GDPR'ın temel kavramlarının yorumlanmasına ilişkin yönergeler yayınlamaktadır.; Bkz. https://edpb.europa.eu/about-edpb/about-edpb_en, Erişim Tarihi: 17.12.2021.
[32] EDPB, " Recommendations 01/2020 on measures that supplement transfer tools to ensure complaince with the EU level of protection of personel data " (18 June 2021). s.11.

üzerinden yönlendirilerek aktarılmasının uluslararası bir aktarım teşkil etmeyeceğidir[33].

GDPR 5. Bölümde yer alan hükümlerin ne zaman uygulanacağının belirlenmesi açısından önemli bir gelişme ise EDPB'nin 18 Kasım 2021 tarihinde yayınladığı ve 31 Ocak 2022 tarihine kadar istişareye açtığı Yönerge[34] olmuştur. Söz konusu Yönerge'de EDPB belirlemiş olduğu üç kriterin tümünün karşılanması durumunda işlemenin aktarım olarak nitelendirilebileceğini belirtmiştir. Bu kriterlere göre, kişisel verilerin m.3 uyarınca GDPR'a tabi olan veri aktaran (veri sorumlusu ve veri işleyen) tarafından verilen işleme ile ilgili olarak GDPR m.3'e tabi olup olmadığına bakılmaksızın üçüncü bir ülkedeki veri aktarılana (veri sorumlusu veya veri işleyen) gönderilmesi veya kullanıma sunulması üçüncü bir ülkeye aktarım teşkil edecektir. Yani EDPB tarafından belirlenen kriterlerin tümünün karşılanmaması durumunda veri sorumlusu veya veri işleyen için bir aktarımdan bahsedilemeyecek ve GDPR 5. Bölümde yer alan hükümler uygulanamayacaktır. Kişisel verileri üçüncü ülkelere veya uluslararası kuruluşlara aktaran bir veri sorumlusu veya işleyenin ise GDPR 5. Bölümdeki koşullara uyması ve aktarımlarını bu bölümde yer alan aktarım mekanizmaları çerçevesinde yapması gerekmektedir. Bu anlamda GDPR 5. Bölümde yer alan hükümler, kişisel veriler AB dışındaki üçüncü ülkelere aktarıldığında GDPR tarafından kişisel verilere sağlanan korumanın veri aktarılanın tabi olduğu yasal mevzuat tarafından engellenmemesini amaçlar ve bu anlamda 3. maddede tanımlanan GDPR'ın bölgesel kapsamını tamamlayıcı hükümlerdir[35].

Bu çalışmada kullanılacak olan "üçüncü ülkelere aktarım" kavramı ile GDPR 5. Bölümde yer alan hükümlerin uygulanacağı aktarımlar kastedilmektedir. 5. Bölümde yer alan söz konusu hükümler, kişisel verilerin Avrupa Ekonomik Alanı[36]

[33] Information Commissioner's Office's (ICO), "International Transfers", https://ico.org.uk/media/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr-1-1.pdf, Erişim Tarihi: 28.11.2021.
[34] EDPB, "Guidelines 05/2021".
[35] EDPB, "Guidelines 05/2021", s.4.
[36] Bkz. Decision of the Council and the Commission of 13 December 1993 on the conclusion of the Agreement on the European Economic Area between the European Communities, their Member

("AEA") (AB Üye Devletlerine ek olarak Norveç, İzlanda ve Lihtenştayn'dan oluşur) içinden AEA dışındaki bir ülkeye aktarımları için geçerli olacaktır.

1.2 Kişisel Verilerin Aktarılmasına İlişkin Genel İlkeler

AB Hukuku kişisel verilerin üye devletler arasında serbest dolaşımına izin vermektedir. GDPR m.1(3) uyarınca üye devletler arasında serbest dolaşım, gerçek kişilerin kişisel verilerinin işlenmesi kapsamında korunması ile bağlantılı nedenlerle kısıtlanamayacak veya yasaklanamayacaktır. AB serbest veri akış alanına, AEA Anlaşması ile AB yasasını benimseyen İzlanda, Norveç ve Lihtenştayn da dâhil edilmiştir[37]. Bu çerçevede AB veri koruma ilkelerinin uygulama alanı bu üç ülkeyi de kapsayacak şekilde genişlemiştir. Temmuz 2018'de değiştirilen AEA Anlaşması, GDPR'ı eklerine dâhil etmiş ve bu kapsamda AEA Ortak Komitesi GDPR'ın uygulanmasına ilişkin bir karar almıştır[38]. Kişisel verilerin cezai suçların önlenmesi, soruşturulması, tespiti ve kovuşturulması amacıyla AEA içindeki serbest dolaşımı ise GDPR kapsamında değil, 2016/680 sayılı Direktif[39] kapsamında gerçekleşmektedir.

Kişisel verilerin AB'den üçüncü ülkelere veya uluslararası kuruluşlara[40] aktarılmasına ilişkin hükümler GDPR 5. Bölümde (m.44 - m.49) düzenlenmiştir.

States and the Republic of Austria, the Republic of Finland, the Republic of Iceland, the Principality of Liechtenstein, the Kingdom of Norway, the Kingdom of Sweden and the Swiss Confederation, OJ 1994 L 1.

[37] Christos Giakoumopoulos, Giovanni Buttarelli ve Michael O'Flaherty, *Handbook on European Data Protection Law*, Luxembourg: Publications Office of the European Union, 2018, s.252.

[38] Bkz. Decision of the EEA Joint Committee No 154/2018 of 6 July 2018 amending Annex XI (Electronic communication, audiovisual services and information society) and Protocol 37 (containing the list provided for in Article 101) to the EEA Agreement [2018/1022].

[39] Bkz. Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA, OJ 2016 L119, (Bundan sonra" 2016/680 sayılı Direktif" olarak anılacaktır).

[40] GDPR m.4(26) "Uluslararası Kuruluş" terimini, uluslararası kamu hukuku veya iki veya daha fazla ülke arasındaki bir anlaşma tarafından ya da bu anlaşmaya dayalı olarak kurulan herhangi bir başka kuruluş tarafından yönetilen bir kuruluş ve alt organları olarak tanımlamıştır.

Aktarımlara ilişkin genel ilkeleri düzenleyen GDPR m.44'de kişisel verilerin işleneceği veya işlenmesinin amaçlandığı üçüncü ülkelere aktarılabilmesi için iki aşamalı bir yaklaşım benimsenmiştir[41]. Bu yaklaşıma göre kişisel verilerin, GDPR ile gerçek kişilere yönelik sağlanan koruma düzeyi zarar görmeden AB dışına aktarılabilmesi için, aktarımın hem GDPR 5. Bölümdeki hükümlere hem de GDPR'ın diğer tüm hükümlerine uygun olarak yapılması gerekmektedir.

44. maddede yer alan söz konusu "Genel Aktarım İlkeleri" GDPR Gerekçe 101'de de açıklanmıştır. Gerekçe 101'de, Gerekçe 6'da da belirtildiği üzere uluslararası ticaret ve işbirliğinin geliştirilmesi açısından birlik dışındaki ülkelere ve uluslararası kuruluşlara kişisel veri aktarımının önemli olduğu vurgulanmakla birlikte, veri aktarımlarındaki artışa bağlı olarak kişisel verilerin korunması yönündeki risklerin ve endişelerin de arttığı belirtilmiştir. Bu nedenle söz konusu gerekçe ileriye dönük aktarımlarda dâhil olmak üzere kişisel verilerin üçüncü bir ülkede bulunan veri sorumluları, veri işleyenlere veya diğer alıcılara aktarılmasının, AB de bulunan bireylerin veri koruma düzeyini zayıflatmaması gerektiğini de düzenlemiştir. Bu bağlamda veri koruma düzeyinin zayıflatılmaması hükmü, kişisel verilerin üçüncü ülkelere aktarılması yoluyla AB'de yaşayan bireyler açısından temel bir hak olan ve Şartla güvence altına alınan kişisel verilerin korunması hakkı çerçevesinde GDPR başta olmak üzere AB Veri Koruma Hukukunda sağlanan korumaların atlatılmaması olarak yorumlanmaktadır[42]. Bu durumda GDPR 5. Bölümle uyumlu ancak GDPR'ın diğer hükümleri veya Şart tarafından istenen gerçek kişiler için koruma düzeyini garanti etmeyen aktarımların gerçekleşmesinin mümkün olmadığı görülmektedir.

GDPR'ın 5. Bölümü, kişisel verilerin üçüncü ülkelere veya uluslararası kuruluşlara hukuka uygun olarak aktarılabilmesi için aralarında hiyerarşi bulunan ve en üstte yeterlilik kararlarının, ortada uygun güvencelerin ve altta istisnaların olduğu "üç

[41] Kuner, Bygrave ve Docksey, *GDPR: A Commentary*, s.757.
[42] Kuner, Bygrave ve Docksey, *GDPR: A Commentary*, s.757.

katmanlı bir yapı" oluşturur[43]. Bir yeterlilik kararı (a*dequacy decision*) en yüksek koruma seviyesini temsil eder. Kişisel verilerin yeterlilik kararı kapsamında aktarılabilmesi için üçüncü bir ülke veya uluslararası kuruluşun hukuki sisteminin temelde en yüksek koruma standardını temsil eden AB Veri Koruma Hukukunda mevcut olan standarda "esasen eşdeğer" *(essentially equivalent)* olması gerekir[44]. Yeterlilik kararının olmaması durumunda uygun güvenceler kullanılabilir. Uygun güvencelerinde, yeterlilik kararı gibi "esasen eşdeğer" seviyede veri koruması sağlaması gerektiği ABAD'ın Schrems II[45] kararında belirtilmiştir[46]. Son olarak, bir yeterlilik kararının olmadığı ve uygun güvencelerin kullanılamadığı belirli durumlarda istisnalar kullanılabilecektir.

Şekil 1.1 GDPR 5. Bölümün Hiyerarşik Yapısı

Kaynak: https://tietosuoja.fi/en/transfers-of-personal-data-out-of-the-eea, Erişim Tarihi: 12.01.2022.

Çalışmamın bir sonraki bölümünde GDPR kapsamında kişisel verilerin AB dışına aktarılmasına ilişkin meşru aktarım mekanizmaları ve ABAD kararları güncel gelişmeler ışığında detaylı olarak incelenecektir.

[43] Kuner, Bygrave ve Docksey, *GDPR: A Commentary*, s.774.
[44] Case C-362/14, *Schrems I*, para 73: *"(...) the term 'adequate level of protection' must be understood as requiring the third country in fact to ensure, by reason of its domestic law or its international commitments, a level of protection of fundamental rights and freedoms that is 'essentially equivalent' to that guaranteed within the European Union by virtue of Directive 95/46 read in the light of the Charter".*
[45] Court of Justice of the European Union (CJEU), Case C-311/18, *Data Protection Commissioner v. Facebook Ireland Limited and Maximilian Schrems [GC]* ('*Schrems II*'), 16 July 2020.
[46] Case C-311/18, *Schrems II*, para. 105.

2 KİŞİSEL VERİ AKTARIM MEKANİZMALARI

2.1 Yeterlilik Kararına Dayalı Aktarımlar

GDPR kapsamında, kişisel verilerin üçüncü bir ülkeye veya uluslararası kuruluşa aktarılmasında dikkate alınması gereken ilk şey, Avrupa Komisyonu (European Commission – "Komisyon") tarafından alınan ve AB dışındaki üçüncü bir ülkenin veri koruma düzeyine ve koruma düzeyinin Avrupa yasal rejimindeki koruma düzeyine kıyasla yeterli olup olmayacağına dayanan bir yeterlilik kararının olup olmadığıdır. Yeterlilik kararı, Komisyonu'nun üçüncü bir ülkenin veya uluslararası bir kuruluşun "yeterli düzeyde veri koruması" (*adequate level of protection)* sağladığına karar verdiği anlamına gelir[47]. GDPR m.45'de, Avrupa Komisyonu'nun üçüncü bir ülkenin (bu ülkelerdeki bölgeler veya bir veya daha fazla belirli sektör dâhil) ya da uluslararası bir kuruluşun yeterli bir koruma seviyesi sağladığına karar verdiği hallerde, kişisel verilerin bu ülke veya uluslararası kuruluşa aktarımının gerçekleşebileceği yer almaktadır.

Yeterlilik kararları, AB'ye taraf olmayan herhangi bir ülke için verilebilir. Ayrıca GDPR, 95/46 sayılı Direktiften farklı olarak AB dışında ki bir yargı alanına aktarılacak kişisel veriler için yeterlilik kararı alma yetkisini yalnızca Komisyona vermiştir[48]. Yeterlilik kararları, AB'ye üye ülkelerin tümü için yasal olarak bağlayıcıdır ve kişisel verilerin Komisyonun bu karar yoluyla "yeterli" olarak belirlediği üçüncü ülkeye veya uluslararası kuruluşa, başka bir onay alınmasına gerek kalmaksızın aktarımına izin verir[49]. Yeterlilik kararları sayesinde kişisel verilerin herhangi bir ek izin veya güvence gerekmeden üçüncü ülkelere veya uluslararası kuruluşlara aktarılması kararın etkisi ve önemini ortaya koymaktadır.

[47] Data Protection Commission, "Transfers of Personal Data to Third Countries or International Organisations", https://www.dataprotection.ie/en/organisations/international-transfers/transfers-personal-data-third-countries-or-international-organisations, Erişim Tarihi: 20.11.2021.
[48] GDPR m.45 (1); 95/46 sayılı Direktif m. 25 (1); 95/46 sayılı Direktifte Avrupa Komisyonu'na ek olarak AB üye devletleri de "yeterlilik kararı" alma yetkisine sahipti.
[49] GDPR m. 45(1); GDPR Gerekçe 103; Bu yeterlilik kararları, 2016/680 sayılı Direktif tarafından yönetilen veri alışverişlerini kapsamamaktadır. Bkz. 2016/680 sayılı Direktif m.36.

Komisyonun almış olduğu bu yeterlilik kararları ile kişisel verilerin herhangi bir kısıtlama ve sınırlama olmadan aktarılabilmesi adına bir "beyaz liste" oluşmuştur[50].

Öte yandan ABAD Schrems I kararında, yeterli koruma seviyesini, üçüncü ülkenin temel hak ve özgürlükler için sağladığı koruma seviyesinin AB'de yasalarla garanti edilen koruma seviyesine "esasen eşdeğer" olarak tanımlamıştır[51]. Üçüncü bir ülkenin yeterli bir koruma düzeyi sağlamak amacıyla başvurduğu yöntemler AB'ninkilerden farklı olabilir, kullanılan yöntemlerin birebir aynı olması gerekmemektedir[52]. Yeterlilik kavramı üçüncü ülkelerdeki veya uluslararası kuruluşlardaki veri koruma kurallarının içeriğinin AB Hukuku standartlarına uygun olmasını gerektirdiği gibi aynı zamanda söz konusu kuralların uygulamada da etkili olmasını gerektirmektedir[53]. Buradaki amaç, veri aktarımlarına ilişkin AB mevzuatının temel gerekliklerini üçüncü ülkelerde de oluşturabilmektir[54].

Yeterlilik kararı tam yeterlilik kararı (*full adequacy decision*) ve kısmi yeterlilik kararı (*partial adequacy decision*) olmak üzere iki şekilde verilebilmektedir. Tam yeterlilik kararı Komisyonun üçüncü bir ülkenin yeterli korumayı tamamen sağladığına dair vermiş olduğu karardır. Bu karar çerçevesinde tam yeterli olarak kabul edilen ülkelere yapılan aktarımlar AB ülkelerine yapılan aktarımlar gibi değerlendirilir[55]. Tam yeterlilik kararı, kişisel verilerin AB'den üçüncü bir ülkeye,

---

[50]Theodorakis, s.7.

[51] 95/46 Sayılı Direktif m.25(1)'de yer alan "yeterli koruma seviyesi" kavramı, ABAD tarafından daha da geliştirilmiştir; Article 29 Working Party, "Adequacy Referential", 06.02.2018, ("WP254", Rev.1), s.3, https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=614108, Erişim Tarihi: 02.01.2022; Case C-362/14, *Schrems I*, para.96.

[52] Case C-362/14, *Schrems I*, para 73-74; Bkz. European Commission, "Communication from the Commission to the European Parliament and the Council "Exchanging and Protection Personal Data in a Globalised World", COM(2017) 7 final, 10.01.2017, s.6, http://ec.europa.eu/newsroom/document.cfm?doc_id=41157, Erişim Tarihi: 23.12.2021.

[53] Kuner, Bygrave ve Docksey, *GDPR: A Commentary*, s.775.

[54] WP254*, "*Adequacy Referantial", s.3.

[55] Bilgi Information Technology Law Institute ("Bilgi IT Law Institute"), " Kişisel Verilerin Korunmasına İlişkin Düzenlemeler Çerçevesinde Uluslararası Veri Aktarımı Yeni Gelişmeler ve Uygulamaya İlişkin Hukuki Değerlendirmeler", İstanbul: 2020, s.18, https://IT Law.bilgi.edu.tr/media/2020/3/30/Final%20Veri_Aktarimi_Raporu_30.03.2020.pdf, Erişim Tarihi: 15.11.2021; Bkz. https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en, Erişim Tarihi: 15.12.2021.

aktarım AB içinde yapılıyormuş gibi başka herhangi bir koruma önlemi gerekmeden yapılabilmesini sağlamaktadır[56]. Kore Cumhuriyeti için verilen yeterlilik kararı bu şekilde verilmiş en güncel yeterlilik kararıdır[57]. Kısmi Yeterlilik kararında ise, Komisyon tarafından yalnızca üçüncü ülkedeki belirli bir sektör, bölge veya uluslararası kuruluşun yeterli korumayı sağladığına dair bir karar verilmektedir. Örneğin, Kanada için verilmiş yeterlilik kararı ticari kuruluşlar için verilmiş bir yeterlilik kararı olduğundan kısmi yeterlilik kararıdır[58]. Ayrıca transatlantik ticareti desteklemek amacıyla kişisel verilerin AB'den ABD'ye aktarılması için hazırlanan ve Komisyonun veri aktarımlarını sağlamak için yeterli bulduğu *Safe Harbour* ("Güvenli Liman") ve *Privacy Shield* ("Gizlilik Kalkanı") Anlaşmaları kapsamında aldığı yeterlilik kararları da kısmi yeterlilik kararlarına örnek olarak verilebilir[59]. ABAD'ın kararları ile geçersiz kılınan Güvenli Liman ve Gizlilik Kalkanı ile ilgili ayrıntılara Bölüm 2.1.5'te yer verilecektir.

GDPR, 95/46 sayılı Direktiften farklı olarak Avrupa Komisyonu'nun, üçüncü bir ülkedeki belirli bir bölge veya sektörün yeterli düzeyde koruma sağladığına ilişkin kısmı yeterlilik kararları vermesine izin vermekte ve böylece Komisyonun yeterlilik kararına ilişkin yetkisini genişletmiş olmaktadır. Ancak sağlık sektörü gibi sektörel sınırların net olarak çizilemediği ve sektördeki oyuncuların birbirine bağlı olduğu durumlar için böyle bir kararın alınmasının zor olacağı değerlendirilmektedir[60].

[56] Data Protection Commission, "Transfers of Personal Data".
[57] Güncel yeterlilik kararları için bkz. https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en, Erişim Tarihi: 24.12.2021.
[58] European Comission, "Commission Decision 2002/2/EC of 20 December 2001 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequate protection of personal data provided by the Canadian Personal Information Protection and Electronic Documents Ac, OJ 2001 L 2/13.
[59] Bkz Kuner, Bygrave ve Docksey, *GDPR: A Commentary*, s.776; Bilgi IT Law Institute, "Kişisel Verilerin Korunmasına İlişkin Düzenlemeler", s.18; Theodorakis, s.3.
[60] Theodorakis, s.8.

Komisyon tarafından verilen ve şu anda yürürlükte olan 15 (on beş) yeterlilik kararı mevcuttur[61]. Komisyon şu ana kadar GDPR m.45(3) kapsamında Andorra, Arjantin, Birleşik Krallık[62], Kanada (ticari kuruluşlar), Faroe Adaları, Guernsey, Man Adası, İsrail, Jersey, Yeni Zelanda, İsviçre, Uruguay, Japonya ve son olarak Kore Cumhuriyeti'ne yönelik aldığı yeterlilik kararlarıyla bu ülkelere aktarılan kişisel verilere ilişkin yeterli koruma sağlandığını kabul etmiştir. Daha önce geçerli olan üç yeterlilik kararı ise ABAD tarafından geçersiz kılındığı için yürürlükte değildir. Geçersiz kılınan söz konusu yeterlilik kararları, ABAD'ın yolcu adı kaydı (Passanger Name Record-"PNR") verilerinin ABD Gümrük ve Sınır Koruma Bürosu'na aktarılmasına ilişkin 2006 tarihli kararı[63] ile 2015 tarihli Schrems I kararı ile geçersiz kıldığı AB-ABD Güvenli Liman ve 2020 tarihli Schrems II kararı ile geçersiz kıldığı AB-ABD Gizlilik Kalkanı Anlaşmaları kapsamında alınan yeterlilik kararlarıdır[64]. Bu yeterlilik kararları 2016/680 sayılı Direktif tarafından yönetilen veri aktarımlarını kapsamamaktadır.

Birleşik Krallık, Avrupa Birliği Antlaşması'nın (Treaty on European Union) 50. maddesine başvurarak AB'den çıkmak istemiş (Brexit) ve bunun neticesinde 31 Aralık 2020 tarihinde AB'den ayrılmıştır. Birleşik Krallık'ın AB'den ayrılması ile birlikte, AB'den Birleşik Krallık'a yapılacak kişisel veri aktarımlarında Birleşik Krallık AB için üçüncü bir ülke konumuna gelmiştir. Bu duruma istinaden AB'den Birleşik Krallık'a Brexit sonrası kişisel veri aktarımlarının kolaylaştırılabilmesi ve aktarımlara ilişkin belirsizliklerin giderilebilmesi için EDPB ve Birleşik Krallık Bilgi Komiseri (Information Commisioner's Officer - "ICO") tarafından Kılavuz[65] yayınlanmış ve Birleşik Krallık için GDPR m.45 kapsamında bir yeterlilik kararı

[61] Yeterlilik kararına sahip ülkelerin güncel listesi için bkz. https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en, Erişim Tarihi: 24.12.2021.
[62] Birleşik Krallık kapsamında GDPR ve 2016/680 sayılı Direktif uyarınca alınan iki yeterlilik kararı mevcuttur.
[63] Joined Cases C-317/04 and C-318/04, European Parliament v Council and Commission, EU:C:2006:346.
[64] Kuner, Bygrave ve Docksey, *GDPR: A Commentary*, s.776.
[65] Information Commissioner's Office's (ICO), "Guide to the General Data Protection Regulation (GDPR)", https://ico.org.uk/media/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr-1-1.pdf, Erişim Tarihi: 28.11.2021.

alınması gündeme gelmiştir. Avrupa Komisyonu 19 Şubat 2021 tarihinde Birleşik Krallık'a aktarılan kişisel verilerin yeterli düzeyde korunduğuna dair GDPR ve 2016/680 Sayılı Direktif uyarınca yayınlamış olduğu taslak düzeyindeki iki yeterlilik kararı ile Birleşik Krallık'a yönelik yeterlilik kararının kabul edilmesi prosedürünü başlatmıştır. 28 Haziran 2021'de taslak iki yeterlilik kararı Komisyon tarafından onaylanmıştır[66].

Öte yandan Avrupa Komisyonu tarafından 14 Haziran 2021'de yayınlanan taslak karar ile GDPR kapsamında kişisel verilerin Kore Cumhuriyeti'ne aktarılması için bir yeterlilik kararının kabul edilmesi prosedürü başlatılmıştır. Bu kapsamda 17 Aralık 2021 tarihinde AB'den Kore Cumhuriyeti'ne kişisel veri aktarımlarına ilişkin yeterlilik kararı Komisyon tarafından onaylanmıştır[67]. Yeterlilik kararlarının kabulüne ilişkin süreç aşağıda "Yeterlilik Kararları Prosedürü" başlığı altında anlatılacaktır.

2.1.1 Yeterlilik Değerlendirme Kriterleri

Avrupa Komisyonu'nun üçüncü bir ülke veya uluslararası kuruluştaki veri koruma düzeyinin yeterliliğini değerlendirirken hangi kriterleri dikkate alması gerektiği GDPR m.45(2)'de ele alınmıştır. Madde 45(2)'de yer alan, Komisyon tarafından yapılacak koruma düzeyinin yeterliliğine ilişkin değerlendirmede ilgili hususların "özellikle" dikkate alınması gerektiği ifadesinden, Komisyonun yapacağı değerlendirmenin söz konusu kriterlerler ile sınırlı olmadığı anlaşılmaktadır[68]. Ayrıca, GDPR m.45(2)'de düzenlenen yeterlilik kriterlerinin ABAD'ın Schrems I

[66] Bkz. European Commission, "Commission Implementing Decision of 28.6.2021 pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council on the adequate protection of personal data by the United Kingdom", 28.06.2021; European Commission, "Commission Implementing Decision of 28.6.2021 pursuant to Directive (EU) 2016/680 of the European Parliament and of the Council on the adequate protection of personal data by the United Kingdom".
[67] Bkz. https://ec.europa.eu/info/sites/default/files/1_1_180366_dec_ade_kor_new_en.pdf, Erişim Tarihi: 24.12.2021.
[68] Bulck, s.235.

kararının etkisiyle 95/46 sayılı Direktif m.25(2)'de yer alan kriterlerden çok daha kapsamlı ve ayrıntılı bir liste içerdiği görülmektedir[69].

GDPR m.45(2)(a), Komisyon'un koruma düzeyinin yeterliliğine ilişkin değerlendirmesini gerçekleştirirken dikkate alması gereken üçüncü ülke mevzuatının ve içtihatlarının kapsamını tanımlamaktadır[70]. Bu bağlamda Komisyon üçüncü ülkede yürürlükte olan ulusal mevzuat, insan hakları ve temel hak ve özgürlüklere saygı, veri koruma kuralları, mesleki kurallar, genel ve sektörel hukuk kuralları, bağımsız denetleyici otorite veya bu tür bir veri koruma kuruluşunun varlığı gibi birçok hususu dikkate almaktadır[71]. GDPR Gerekçe 104'e göre üçüncü ülkenin mevzuatına ilişkin değerlendirme ulusal güvenlik, kamu güvenliği, savunma, kamu düzenine ilişkin mevzuat ile ceza hukukunu da içerecek şekilde geniş ve kapsamlı bir şekilde yapılmalıdır.

Ayrıca değerlendirmenin üçüncü ülkenin kamu makamlarının kanunun uygulanması *(law enforcement)*, kamu yararı veya ulusal güvenlik amaçlarıyla kişisel verilere erişim sistemini de içerecek şekilde kapsamlı olması gerekmektedir[72]. Bu hüküm, Komisyon'un söz konusu değerlendirmeyi yaparken üçüncü ülkenin kamu makamları tarafından kişisel verilere erişim izni verilmesi imkânına özellikle dikkat edilmesi gerektiğini vurgular[73]. GDPR m.45(2)(a), ABAD'ın Schrems I kararının etkisiyle ulusal mevzuatların yanında içtihat hukukunun da değerlendirilmesini gerektirir[74].

GDPR m.45(2)(c)'ye göre Komisyon, yeterliliğe ilişkin değerlendirmesinde söz konusu üçüncü ülkenin veya uluslararası kuruluşun üstlendiği uluslararası taahhütler ve yasal olarak bağlayıcı sözleşmelerden ve belgelerden kaynaklanan diğer yükümlülükleri ve özellikle kişisel verilerin korunmasına ilişkin çok taraflı

[69] Kuner, Bygrave ve Docksey, *GDPR: A Commentary*, s.775.
[70] Wagner, s.321.
[71] GDPR m.45(2).
[72] European Commission, "Exchanging and Protection Personal Data", s.6.
[73] Wagner, s.321.
[74] Case C-362/14, *Schrems I*, para 75; Wagner, s.323.

veya bölgesel sistemlere katılımından kaynaklanan yükümlülükleri de dikkate alacaktır[75]. Bu çerçevede GDPR'ın 105. Gerekçesi, yeterliliğe ilişkin değerlendirmede ilgili ülkenin 108 Sayılı Sözleşme ve 181 Sayılı Ek Protokole katılımının özellikle dikkate alınması gerektiğini düzenlemiştir.

Komisyon, yapmış olduğu değerlendirme neticesinde söz konusu üçüncü ülkenin AB içinde sağlanan koruma düzeyine "esasen eşdeğer" bir koruma düzeyini garanti edip etmediğini belirlemelidir. Yeterlilik kararı tüm AB ülkeleri için bağlayıcı olup, yeterlilik kararının kabul edilmesi ile birlikte kişisel veriler AB'den yeterlilik kararı alınan üçüncü bir ülkeye, AB içindeki veri aktarımında olduğu gibi, ek bir izin veya güvenlik önlemi almadan aktarılabilmektedir[76]. Yeterlilik kararın önemi ve etkisi bu çerçevede değerlendirildiğinde yeterliliğe ilişkin değerlendirmede Komisyonun kişisel veri aktarımını etkileyebilecek tüm koşulları dikkate alması gerektiği açıktır.

WP29[77] 1998 yılında, yeterliliği değerlendirme yaklaşımı ile ilgili olarak üçüncü ülkelerdeki veya uluslararası kuruluşlardaki korumanın yeterli sayılabilmesi için asgari bir gereklilik olarak uyulması gereken temel ilkeleri belirlemiştir[78]. Bu ilkeler, amaç sınırlama, veri kalitesi ve orantılılık, güvenlik, şeffaflık, erişim, düzeltme ve itiraz hakkı ile ileriye dönük aktarımlara ilişkin kısıtlamalardır[79]. Üçüncü ülkeler tarafından uyulması gereken söz konusu temel ilkeler Komisyon tarafından yeterlilik kararının verilmesinde yararlı bir başlangıç noktası olarak

[75] GDPR Gerekçe 105.
[76] GDPR m.45(1); Data Protection Commission, "Transfers of Personal Data".
[77] Madde 29 Çalışma Grubu (Article 29 Working Party-"WP29"), 95/46 sayılı Direktif'in 29. maddesi kapsamında kurulmuştur. Avrupa Komisyonuna veri koruma konularında tavsiyelerde bulunmak, AB üye devletlerinde veri koruma için uyumlu politikaların geliştirilmesinde yardımcı olmak, veri koruma alanında ortaya çıkan sorunların çözümü ve güncel konularda görüş hazırlamak amacıyla bağımsız bir çalışma grubu olarak kurulmuştur. WP29, AB üyesi ülkelerin ulusal denetim makamları, Avrupa Veri Koruma Denetçiliği (EDPS) ve Avrupa Komisyonu temsilcilerinden oluşmaktadır. GDPR'ın yürürlüğe girmesiyle birlikte 25 Mayıs 2018'de WP29'un yerine EDPB kurulmuştur.
[78] Article 29 Working Party (WP29), "Transfers of Personal Data to Third Countries; Applying Articles 25 and 26 of the EU data protection directive", 24.07.1998, s.5, "WP12", https://ec.europa.eu/justice/article-29/documentation/opinionrecommendation/files/1998/wp12_en.pdf, Erişim Tarihi: 1.10.2021.
[79] WP12, "Transfers of Personal Data to Third Countries", s.5-8.

kabul edilse de, kesin gerekliklerin belirlenmesinde aktarımın ilgili kişiye[80] getirdiği risk derecesinin değerlendirmesi önemli bir faktör olacaktır[81].

2017 yılında WP29 tarafından yayınlanan ve EDPB tarafından onaylanan bir bildiride GDPR'da yer alan yeterlilik kriterleri yorumlanmış ve yeterliliğe ilişkin bir takım içerik, prosedür ve uygulamaya yönelik ilke ve mekanizmalar belirlenmiştir. Söz konusu çalışmada üçüncü ülke veya uluslararası kuruluşun yeterli sayılabilmesi için 1998'de belirlenen içeriğe ilişkin ilkelere, temel veri koruma, meşru amaçlarla yasal ve adil işleme, veri saklama ve gizlilik ilkeleri de eklenmiştir. Bununla beraber WP29 tarafından hazırlanan bu belgelerin rehberlik sağlama amacı taşıdığını ve bağlayıcı olmadığını belirtmek gerekir[82].

2.1.2 Yeterlilik Kararının Kabul Edilmesi Prosedürü

GDPR m.45, Komisyon tarafından üçüncü ülkelerin (bu ülkelerdeki bir veya daha fazla belirli sektör dahil) veya uluslararası kuruluşların yeterliliğine ilişkin kararların verilebilmesi için prosedür ve standartları ortaya koymaktadır[83]. Yeterlilik kararları, 182/2011 Sayılı Komitoloji Tüzüğünün[84] 5. maddesinde belirtilen inceleme prosedürüne uygun olarak kabul edilen ve GDPR m.93(2)'de detaylı olarak ele alınan bir uygulama tasarrufudur[85]. Komisyon tarafından alınacak yeterlilik kararları, kararın bölgesel ve sektörel uygulamasını içermeli, kararın periyodik olarak incelenmesi için gerekli mekanizmayı sağlamalı ve GDPR

[80] "İlgili Kişi" GDPR'da doğrudan tanımlanmasa da dolaylı olarak kişisel veri tanımı içinde ifade edilmiştir. Bu kapsamda ilgili kişi, kişisel verileri işlenen tanımlanmış veya tanımlanabilir gerçek kişidir.
[81] WP12, "Transfers of Personal Data to Third Countries", s.5.
[82] Wagner, s.326.
[83] GDPR Gerekçe 105.
[84] GDPR m.97(4)'e göre Avrupa Komisyonu yeterlilik kararına ilişkin değerlendirme ile ilgili Avrupa Parlamentosunun, Avrupa Konseyinin ve diğer ilgili organ veya kaynakların pozisyonlarını ve görüşlerini dikkate almalıdır; Regulation (EU) No.182/2011 of the European Parliament of the Council of 16 February 2011 Laying down the rules and general principles concerning mechanism for control by Member States of the Commissions exercise of implementing Powers, OJ 2011 L 55/13, (Bundan sonra "182/2011 sayılı Tüzük" olarak anılacaktır).
[85] GDPR m.93(2)'ye göre Avrupa Komisyonu'na yeterlilik kararlarını yürürlüğe koyarken üye devlet temsilcilerinden oluşan ve Komitoloji Tüzüğü'nün 5. maddesi ile sağlanan inceleme prosedürüne uygun olarak kararları onaylaması gereken komite yardımcı olmaktadır.

m.45(2)(b)'de belirtilen ve veri koruma kurallarına uyumu sağlamakla sorumlu denetim makamları ve yetkililerini belirlemelidir[86]. Bununla birlikte bir yeterlilik kararının alınabilmesi süreci sırasıyla Komisyon tarafından bir teklif sunulmasını (taslak kararın yayınlanması), EDPB'nin görüşünün alınmasını, AB ülkelerinin temsilcilerinin onayını ve son olarak da kararın Komisyon tarafından kabulünü gerektirir[87].

GDPR Gerekçe 105'e göre Komisyon, üçüncü ülkelerdeki veya uluslararası kuruluşlardaki koruma düzeyini değerlendirirken EDPB'ye danışmalıdır. GDPR m.70(1)(s) hükmü uyarınca Komisyon'a tavsiye verme görevini yerine getirebilmek ve üçüncü ülkedeki veri koruma seviyesine ilişkin değerlendirmesini yapabilmek için Komisyon tarafından EDPB'ye üçüncü ülke ya da uluslararası kuruluşla ilgili gerekli tüm belgeler sağlanır[88]. EDPB, yapmış olduğu değerlendirme neticesinde yeterlilik çerçevesinde Komisyonun bulguları hakkında görüş sunacak, varsa yetersizlikleri belirleyecek ve bu yetersizlikleri giderebilmek için önerilerde bulunacaktır[89]. Ancak burada EDPB'nin görüşünün bağlayıcı olmadığını ve GDPR'ın EDPB'ye Komisyonun yeterliliğe ilişkin kararını onaylama yetkisi vermediğini belirtmek gerekir[90]. Komisyon, yeterlilik kararına ilişkin diğer kurumlar tarafından verilen özellikle Avrupa Parlamentosu tarafından verilen görüşleri de dikkate alacaktır[91].

Komisyonun yeterlilik kararlarını veya yeterli koruma düzeyinin artık mevcut olmadığını tespit eden kararları, AB'nin Resmi Gazetesi ve web sitesinde

[86] GDPR m.45(3); GDPR m.45(2)(b).
[87] Bkz. https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en, Erişim tarihi: 24.08.2021.
[88] GDPR m.70 (1)(s).
[89] WP254, "Adequacy Referantial", s.4.
[90] Kuner, Bygrave ve Docksey, *GDPR: A Commentary*, s.774, s.785 dn. 91.; Nitekim Avrupa Komisyonu EDPB'nin karara ilişkin görüşü eleştiri içermesine rağmen, Japonya'ya yönelik yeterlilik kararını onaylamıştır.
[91]GDPR m.97(4), Komisyonun GDPR m.97(2)'de atıfta bulunulan ve m.45(3) uyarınca alınan yeterlilik kararlarına ilişkin yapılan değerlendirmeler ve gözden geçirmeleri gerçekleştirirken, Avrupa Parlamentosu, Konsey ve diğer ilgili organlar veya kaynakların görüşleri ve bulgularını dikkate alması gerektiğini belirtir.

yayınlanması gerekir[92]. Yeterlilik kararlarının ve karara ilişkin kriterlerin kamuya açıklanması, üçüncü ülkelerin AB'nin veri koruma standartlarını anlamaları ve yasa ve uygulamalarını bu çerçevede uyarlamaları açısından oldukça önemlidir[93].

2.1.3 Yeterlilik Kararlarının Periyodik Olarak Gözden Geçirilmesi

Komisyon, GDPR m.45(3) uyarınca yeterlilik kararlarını üçüncü ülke veya uluslararası kuruluştaki tüm ilgili gelişmeleri dikkate alarak en az dört yılda bir periyodik olarak gözden geçirmelidir. Ancak belirtilen dört yıllık zaman diliminin genel bir zaman dilimi olduğu, mevcut ve özel koşullara bağlı olarak söz konusu dört yıllık periyodik gözden geçirme süresinin bundan daha kısa olabileceği belirtilmektedir[94]. Ayrıca, yeterlilik kararına sahip üçüncü ülke veya uluslararası kuruluşta yasal çerçevede meydana gelen değişiklikler, planlanandan önce bir inceleme ihtiyacını ortaya çıkarabilir[95]. GDPR, periyodik inceleme prosedürünün söz konusu üçüncü ülke veya uluslararası kuruluşla istişare içinde yürütülmesi ve bu süreçte Komisyon'un Avrupa Parlamentosu ve Avrupa Konseyi ile birlikte diğer ilgili kurum ve kaynakların görüşlerini dikkate alması gerektiğini belirtmektedir[96].

Komisyona yeterlilik kararları için dört yılda bir periyodik gözden geçirme mekanizması sağlama yükümlülüğü getirilmesi Schrems I Kararının bir sonucudur[97]. Söz konusu kararda Başsavcı Bot görüşünde, Güvenli Liman kapsamında alınan yeterlilik kararının on beş yıllık bir süre içinde bir incelemeye tabi tutulmadığını belirtmiştir[98]. Bu çerçevede ABAD, Komisyon'un söz konusu ülkeyi veya uluslararası kuruluşu yeterliliğe ilişkin olarak periyodik olarak gözden

[92] GDPR m.45(8).
[93] Wagner, s.320.
[94] GDPR m.45(3); Bkz.WP254, "Adequacy Referantial", s.4; Kuner, Bygrave ve Docksey, *GDPR: A Commentary* s.790.
[95] WP254, "Adequacy Referantial", s.4.
[96] GDPR m.45(5).
[97] Bulck,s.236.
[98] CJEU, *Opinion of Advocate General Bot in Case C- 362/ 14 Schrems I,* EU:C:2015:627, para. 232-236.

geçirmesi gerektiğini[99] ve söz konusu inceleme prosedürünün titiz ve kapsamlı olarak yürütülmesi gerektiğini belirtmiştir[100]. Ayrıca EDPB, üçüncü ülkedeki veya uluslararası kuruluştaki herhangi bir inceleme süreci hakkında bilgilendirilmeyi ve sürece katılmayı beklediğini belirtmiştir[101].

95/46 sayılı Direktif kapsamında kabul edilen yeterlilik kararları, GDPR m.45(9) hükmüne dayanarak bir Komisyon kararı ile yürürlükten kaldırılana, değiştirilene veya yenilenene kadar yürürlükte kalmaktadır. Ancak GDPR m.45(3) uyarınca söz konusu kararların da periyodik olarak gözden geçirilmeleri gerekir. 95/46 sayılı Direktif döneminde alınan kararların çoğu GDPR m.45' te yer alan yeterlilik gerekliklerini tam anlamıyla karşılayamayacağından bu durum Komisyon'un bu kararları gelecek dönemde değiştirmek zorunda kalabileceği şeklinde yorumlanabilir[102]. Nitekim ABAD'ın Schrems II Kararı ile geçersiz kıldığı Gizlilik Kalkanı Anlaşması GDPR'ın gerekliliklerini tam anlamıyla karşılamıyordu.

2.1.4 Yeterlilik Kararlarının Yürürlükten Kaldırılması, Değiştirilmesi veya Askıya Alınması

GDPR m.45(4) ile m.45(6) arasındaki hükümlerle Komisyona getirilen yükümlülükler, Schrems I davasının GDPR'a sağladığı önemli başka bir katkı olmuştur[103]. GDPR m.45(4)'e göre Komisyon, GDPR m.45(3) ve 95/46 sayılı Direktif m.25(6) uyarınca alınan bir yeterlilik kararının işleyişini olumsuz etkileyebilecek gelişmeleri sürekli olarak izlemelidir. GDPR m.45(5)'e göre Komisyon, üçüncü ülke veya uluslararası kuruluş artık yeterli düzeyde koruma sağlamıyorsa yeterlilik kararını almada kullandığı ve m.93(2)'de atıfta bulunulan prosedüre göre yeterlilik kararını yürürlükten kaldırabilir, değiştirebilir ya da askıya alabilir. Söz konusu maddede ayrıca, Komisyon'un uygun şekilde

[99] Case C-362/14, *Schrems I*, para 76.
[100] Case C-362/14, *Schrems I, para* 78.
[101] WP254, "Adequacy Referantial", s.4.
[102] Kuner, Bygrave ve Docksey, *GDPR: A Commentary*, s.791.
[103] Bu hükümler 95/46 sayılı Direktif'in m.25(3)-25(5) hükümlerini esas alarak detaylandırmış ve açık hale getirmiştir; Bulck, s.237.

gerekçelendirilmiş zorunlu acil nedenlerle m.93(3)'te atıfta bulunulan prosedüre uygun olarak uygulanabilir uygulama tasarruflarını derhal kabul etmesi gerektiği de belirtilmektedir. Bir yeterlilik kararının yürürlükten kaldırılması, değiştirilmesi veya askıya alınması geriye etkili olarak hüküm doğurmayacaktır. Bunun yanında Avrupa Parlamento'su ve Avrupa Konseyi dilediği zaman Komisyon'dan yeterlilik kararını GDPR'da öngörülen uygulama yetkilerini aştığı gerekçesiyle değiştirmesini veya geri çekmesini talep edebilir[104].

Komisyon, yeterlilik kararının yürürlükten kaldırılması, değiştirilmesi veya askıya alınması kararına sebebiyet veren durumların düzeltilmesi için üçüncü ülke veya uluslararası kuruluşlarla istişarelerde bulunmalıdır[105]. Yeterlilikle ilgili alınan tüm kararlar AB'nin resmi gazetesinde ve web sitesinde yayınlanmalıdır[106]. Bir yeterlilik kararı yürürlükten kaldırılsa bile bu durum kişisel verilerin söz konusu üçüncü ülkeye veya uluslararası kuruluşa 46. maddede belirtilen uygun güvenceler ve 49. maddede belirtilen istisnalara dayanarak aktarılmasına halel getirmeyeceği özellikle belirtilmelidir[107].

2.1.5 ABAD Kararlarının Yeterlilik Kararları Üzerindeki Etkisi

2.1.5.1 Güvenli Liman ve Schrems I Kararı

Kişisel verilerin korunmasına yönelik, AB ve ABD'nin farklı yaklaşımları bulunmaktadır. AB gizlilik ve kişisel verilerin korunması konusuna temel haklar çerçevesinde yaklaşmaktadır. ABD Yüksek Mahkemesi ise Anayasa'yı bireylere mahremiyet hakkı sağlayacak şekilde yorumlasa da, bu hak genellikle hükümetin müdahalelerine karşı koruma sağlamaktadır[108]. AB'de kişisel verilerin korunması

[104] Bkz. https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en, Erişim Tarihi: 22.10.2021.
[105] GDPR m.45(6).
[106] GDPR m.45(8).
[107] GDPR m.45(7).
[108] Congressional Research Service, "U.S.-EU Privacy Shield and Transatlantic Data Flows", September 22,2021, s.3.

hakkı AB'nin birincil hukuku olan Şart kapsamında garanti altına alınırken, ABD'de ise hiçbir federal yasa tüketicilerin kişisel verilerinin işlenmesini kapsamlı bir şekilde düzenlememektedir[109].

1995 yılında AB'de veri korumasına yönelik 95/46 sayılı Direktifin kabul edilmesinin ardından bu farklılıklar AB ve ABD arasındaki kişisel verilerin aktarımına ilişkin birçok işletme ve endüstrinin olumsuzluklarla karşılaşacağına dair endişeler oluşturdu. Oluşan bu olumsuz durumun önüne geçmek amacıyla yapılan görüşmeler neticesinde ABD Ticaret Bakanlığı (United States Department of Commerce – "DOC") ve Avrupa Komisyonu, ABD'li şirketlerin Direktifte yer alan kişisel verilerin AB'den üçüncü bir ülkeye veri aktarımı için gerekli olan "yeterli koruma seviyesi**"** gerekliliğini yerine getirmesini sağlayacak bir sistem üzerinde anlaştı. Bu çerçevede Avrupa Komisyonu 2000 yılında, AB'den ABD'ye yapılacak kişisel veri aktarımlarının 95/46 sayılı Direktifin 25. maddesi uyarınca yeterli koruma sağladığını tespit eden Güvenli Liman Gizlilik İlkeleri[110] kararını yayınladı. Ancak Avrupa Komisyonu'nun kararında, Güvenli Liman ilkelerinin kamu yararı, ulusal güvenlik veya kanunun uygulanması söz konusu olduğunda gerekli ölçüde sınırlandırılabileceği de yer almaktaydı[111].

AB Veri Koruma Hukukuna dayalı ilkelerden oluşan Güvenli Liman, merkezi ABD'de yer alan şirketlerin, AB'den ABD'ye aktarılan kişisel verilerin korunmasını temin etmek üzere uymayı taahhüt ettikleri bir öz denetim mekanizmasıydı[112]. Bu ilkelere uyan ABD'li şirketlerin AB'den kişisel verilerin aktarılması için AB'nin gerekliliklerini karşıladığı Komisyon tarafından kabul edilmekteydi. Bir şirketin Güvenli Limana dâhil olabilmesi için Federal Ticaret Komisyonu (The Federal

[109] Congressional Research Service, "U.S.-EU Privacy Shield", s.3.
[110] Bkz. "Commission Decision 2000/520 of 26 July 2000 Pursuant to Directive 95/46 of the European Parliament and of the Council on the Adequacy of the Protection Provided by the Safe Harbour Privacy Principles and Related Frequently Asked Questions Issued by the US Department of Commerce", 2000 OJ/L 215.
[111] Bkz. Commission Decision 2000/520, Frequently Asked Questions.
[112] Christopher Kuner, "Reality and Illusion in EU Data Transfer Regulation Post Schrems," *German Law Journal,* 18/4 (2017), s.886.

Trade Commission - "FTC") ve ABD Ulaştırma Bakanlığı (United States Department of Transportation – "DOT")'nın yetki alanına girmesi gerekliydi. Şirketlerin yeterlilik kazanmak için her yıl DOC'a bir mektup göndererek Güvenli Liman gizlilik ilkelerine ve gerekliliklerine uyduklarını kendi kendilerine onaylamaları gerekiyordu. Ayrıca FTC, AB üye ülke makamlarının herhangi bir ihlale ilişkin bildirimlerini gözden geçirmeyi taahhüt ediyordu. Güvenli Liman, FTC ve DOT tarafından denetleniyordu.

15 yıl kullanılmasının ardından Güvenli Liman, ABAD'ın 6 Ekim 2015 tarihli "Schrems I" kararı ile geçersiz kılınmıştır. ABAD'ın "Schrems I " kararı, AB Veri Koruma Hukukunda veri aktarımı ile ilgili dönüm noktası sayılabilecek bir karar olmuştur[113]. Dava, 25.06.2013 tarihinde Avusturya vatandaşı olan Maximillian Schrems'ın İrlanda ulusal denetim makamına yapmış olduğu şikâyet ile başladı. Facebook kullanıcısı olan Schrems, Snowden'ın ABD gözetim faaliyetlerine ilişkin ifşaatlarına dayanarak, Facebook'a kayıtlı kişisel verilerinin bir kısmının veya tamamının Facebook İrlanda'daki AB merkezli sunuculardan ABD'deki sunuculara Facebook tarafından aktarıldığını ve Amerikan Ulusal Güvenlik Ajansı'nın ("US National Security Agency -NSA") bu verilere erişimi olduğunu iddia etti. Schrems, ABD'nin veri koruma hukuku ve istihbarat gözetimine ilişkin uygulamalarda yeterli bir korumaya sahip olmadığını iddia ederek İrlanda ulusal denetim makamının Güvenli Liman ilkelerinin ABD'ye aktarılan kişisel veriler açısından yeterli bir koruma sağlayıp sağlamadığını incelemesi ve Facebook'a ABD'ye veri aktarımını durdurma talimatı vermesi gerektiğini ileri sürmüştür. İrlanda ulusal denetim makamı, Facebook'un Güvenli Limana bağlı kaldığını ve denetim makamının Avrupa Komisyonu tarafından, 95/46 Sayılı Direktif m.25(6) uyarınca oluşturulan Güvenli Liman Gizlilik İlkeleri kapsamında alınan yeterlilik kararının "yeterli koruma" sağlayıp saylamadığını sorgulayamayacağını ileri sürerek söz konusu şikâyeti değerlendirmek için herhangi bir dayanağının olmadığı gerekçesiyle davayı ve Facebook aleyhine işlem yapmayı reddetmiştir. İrlanda ulusal denetim

[113] Kuner, "Reality and illusion", s.884.

makamının ret kararına karşı Schrems, davayı İrlanda Yüksek Mahkemesine taşımıştır. İrlanda Yüksek Mahkemesi ise 18 Haziran 2014 tarihinde davayı ön karar için ABAD'a havale etmiştir.

ABAD'ın 6 Ekim 2015 tarihinde vermiş olduğu Schrems I kararının önemi odaklandığı dört ana konuya dayanmaktadır[114]. ABAD vermiş olduğu kararda ilk olarak, kişisel verilerin korunması hakkının AB Hukuku kapsamındaki temel haklardan biri olduğunu onaylamış ve AB Hukukunda temel haklara verilen önem çerçevesinde Avrupa Komisyonu'nun üçüncü ülkelerdeki veri korumanın yeterliliğini değerlendirirken, 95/46 sayılı Direktifin 25. maddesinden kaynaklanan gereklilikleri Şart kapsamında okumasını ve buna istinaden yeterlilik değerlendirmesinin "katı" olması gerektiğini vurgulamıştır[115].

ABAD'ın Schrems I kararında ele aldığı ikinci konu ise, AB Hukukunun veri aktarım mekanizmaları aracılığıyla üçüncü ülkelerde gerçekleşen veri işleme faaliyetlerine dolaylı olarak uygulanmasıdır[116]. ABAD, AB Hukukunun üçüncü ülkelerde doğrudan uygulanmadığını[117] ancak kişisel verilerin 95/46 sayılı Direktif m.2(b)[118] hükmüne dayanarak bir üye devletten üçüncü bir ülkeye aktarılmasının bir veri işleme faaliyeti oluşturduğunu, bu nedenle Güvenli Liman kapsamındaki veri aktarımları açısından AB Hukukunun geçerli olduğunu belirtmiştir[119].

ABAD'ın vermiş olduğu kararda odaklandığı üçüncü konu ise ulusal denetim makamlarının rolünün güçlendirilmesi olmuştur[120]. Karara göre, Komisyon

[114] Kuner, "Reality and illusion", s.892.
[115] Case C-362/14, *Schrems I*, para 78.
[116] Christopher Kuner, *Transborder Data Flows and Data Privacy Law*, Oxford Scholarship Online, September 2013, s.125-126.
[117] Case C-362/14, *Schrems I*, para 44.
[118] 95/46 sayılı Direktif m.2(b) kişisel verilerin işlenmesini *"silme veya tahrip etme, engelleme, birleştirme veya sıralama, sağlama ya da dağıtma, iletmeyle açıklama, toplama, kaydetme, organizasyon, depolama, adaptasyon veya değiştirme, kurtarma, danışma gibi otomatik ya da otomatik olmayan araçlarla kişisel veriler üzerinde yapılan herhangi bir faaliyet veya faaliyet dizisi*" olarak tanımlamaktadır.
[119] Case C-362/14, *Schrems I*, para 45.
[120] Kuner, "Reality and illusion", s.894.

tarafından üçüncü ülkelere veri aktarımı için verilen bir yeterlilik kararı, ulusal denetim makamlarının Şart ve 95/46 Sayılı Direktif tarafından sunulan yetkilerini azaltmayacak veya engellemeyecektir[121]. Bu çerçevede Komisyon tarafından kabul edilen bir yeterlilik kararı mevcut olsa bile, ulusal denetim makamları, bir yeterlilik kararına dayanarak yapılan aktarımlarda üçüncü ülkelerdeki korumanın yeterliliğine ve temel hak ve özgürlüklerinin korunmasına yönelik bireylerin iddiasını tam bir bağımsızlıkla[122] ve "tüm gerekli özeni" göstererek incelemelidir[123]. Bir Komisyon kararının geçerli olup olmadığına karar verme görevi nihai olarak ABAD'a aittir[124].

ABAD'ın Schrems I davasına ilişkin kararda ele aldığı son konu ise, önemi itibariyle çalışma kapsamında da tartışılması gereken, üçüncü ülkelere veri aktarımı için gerekli olan "yeterli veri koruma seviyesinin" tanımlanması olmuştur[125]. ABAD'ın söz konusu kararda yeterli veri koruma seviyesi olarak tanımladığı koruma, Şart ışığında belirlenen yüksek düzeyde koruma olup bu koruma AB Hukuku kapsamındaki korumayla birebir aynı değil "esasen eşdeğer" bir korumadır[126]. ABAD, AB dışına veri aktarımı için üçüncü bir ülkenin karşılaması gereken yeterli veri koruma standardını yüksek düzeyde veri koruma standardı olarak tanımlayarak küresel veri koruma çıtasını da yükseltmiştir[127].

ABAD Schrems I kararında, Komisyonun 95/46 sayılı Direktif m.25'e göre verilerin aktarılması kapsamında bir yeterlilik kararı verirken üçüncü ülkenin yerel yasalarını veya uluslararası taahhütlerini incelemesi gerektiğini belirtmiş ancak Güvenli Limanı bir yeterlilik kararı olarak tanıyan Komisyonun 2000 tarihli kararında bu yönde bir tespit yer almadığını belirlemiştir. Ek olarak ABAD, ABD ulusal

[121] Case C-362/14, *Schrems I*, para 53-58.
[122] Case C-362/14, *Schrems I*, para 40-41.
[123] Case C-362/14, *Schrems I*, para 63.
[124] Case C-362/14, *Schrems I*, para 61.
[125] Kuner, "Reality and illusion", s.895.
[126] Case C-362/14, *Schrems I*, para 73: *"(...) the term 'adequate level of protection' must be understood as requiring the third country in fact to ensure, by reason of its domestic law or its international commitments, a level of protection of fundamental rights and freedoms that is essentially equivalent to that guaranteed within the European Union by virtue of Directive 95/46 read in the light of the Charter".*
[127] Kuner, "Reality and illusion", s.893.

güvenliği, kamu yararı ve kanun uygulama gerekliliklerinin Güvenli Liman ilkelerinden daha öncelikli olduğuna ve ABD şirketlerinin bu gerekliliklerin çatışması durumunda Güvenli Liman tarafından belirlenen koruyucu ilkeleri herhangi bir sınırlama olmadan göz ardı etmekle yükümlü olduğuna karar vermiştir[128].

Sonuç olarak ABAD, Güvenli Liman ilkelerinin ABD yetkililerinin kişisel verileri AB'den ABD'ye aktarılan veya aktarılabilecek bireylerin temel haklarına müdahale etmesine imkân verdiği sonucuna varmıştır. Ayrıca ABAD, Komisyonun Güvenli Liman ilkelerinin yeterli veri koruması sağladığını tespit ederken, bu tür bir müdahaleyi sınırlamaya yönelik kuralların veya müdahaleye karşı etkili yasal korumanın var olup olmadığını dikkate almadığını belirtmiştir.

Tüm bu nedenlerle ABAD, Güvenli Liman Gizlilik İlkelerini geçersiz saymıştır. Karardan sonra AB ve ABD arasında veri aktarımı için standart sözleşme maddeleri ve Bağlayıcı Şirket Kuralları (Binding Corporate Rules – "BCR") kullanılabilir olsa da Güvenli Liman kapsamında alınan yeterlilik kararı aktarımlar için artık yasal bir dayanak olmaktan çıkmıştır. Komisyon Aralık 2016'da Schrems I kararının gerekliliklerini dikkate almak için o tarihte yürürlükte olan Andorra, Arjantin, Kanada, Faroe Adaları, Guernsey, Man Adası, İsrail, Jersey, Yeni Zelanda, İsviçre ve Uruguay'ı kapsayan on bir yeterlilik kararını değiştiren bir karar yayınlamıştır[129]. ABAD'ın Schrems I kararı ile Güvenli Limanı geçersiz kılmasının ardından Güvenli Liman'a katılan yaklaşık 4.500 ABD'li şirket, söz konusu kararın AB ve ABD arasındaki ticari ilişkiler için olumsuz etkileri olacağından endişe etmişlerdir. Ancak, kararın dört aylık bir geçiş sürecinden sonra devreye girmesinin yanında AB

[128] Case C-362/14, *Schrems I*, para 86-87.
[129] Bkz. 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, OJ L 34; Kuner, Bygrave, Docksey, *GDPR: A Commentary*, s.776.

ve ABD yetkilileri arasında yapılan müzakereler neticesinde Temmuz 2016'da Gizlilik Kalkanı Anlaşması yürürlüğe girmiştir.

2.1.5.2 Gizlilik Kalkanı ve Schrems II Kararı

Güvenli Liman 2000 yılında yürürlüğe girdiğinde kişisel verilerin aktarılması da dâhil verilerin işlenmesi bugünkünden çok daha sınırlı seviyedeydi. Güvenli Limanı daha güvenli hale getirmek için AB ve ABD arasındaki görüşmeler aslında, ABD gözetim uygulamalarının ifşa edilmesiyle birlikte 2013 yılında başlamıştı ve ABAD'ın Schrems I kararı ile de bu görüşmeler hız ve önem kazanmış oldu[130]. Ayrıca, yeni anlaşma için yapılan görüşmelerde o tarihte henüz yürürlüğe girmemiş olan GDPR'ın öngördüğü değişiklikler ve yeniliklerde dikkate alınmıştı[131].

ABAD'ın 6 Ekim 2015 tarihli Schrems I kararı ile Güvenli Limanın geçersiz kılınmasının ardından Komisyon ve DOC kişisel verilerin ticari amaçla AB'den ABD'ye aktarılması için geçerli bir mekanizma olan Gizlilik Kalkanı sistemi üzerinde anlaştılar. Komisyon tarafından 12 Temmuz 2016 tarihinde Gizlilik Kalkanı Anlaşmasının yeterli bir koruma düzeyi sağladığı resmi bir karar ile yayınlandı. Gizlilik Kalkanı tüm AB üyeleri tarafından kabul edilerek 1 Ağustos 2016 tarihinde yürürlüğe girdi. Bu çerçevede AB'den ABD'ye veri aktarılabilmesi için gönüllü olarak ABD'li şirketin Gizlilik Kalkanı ilkelerine uymayı taahhüt etmesi ve DOC tarafından sertifikalandırılması gerekmekteydi. Gizlilik Kalkanı Schrems II kararı ile geçersiz kılındığında, anlaşmaya kayıtlı %75'i küçük ve orta büyüklükte işletme olan 5.380 ABD'li şirket bulunuyordu[132].

Gizlilik Kalkanı Anlaşması, 16.07.2020 tarihinde ABAD'ın "Schrems II" olarak adlandırılan kararı ile geçersiz kılınmıştır. Gizlilik Kalkanı Anlaşması, halefi olduğu Güvenli Limanın geçersiz kılınmasından sonra daha fazla veri güvenliği

[130] European Commission, "European Commission Calls on the U.S. To Restore Trust in EU-U.S. Data Flows," Press Release, 27.11.2013.
[131] Congressional Research Service, "U.S.-EU Privacy Shield", s.8.
[132] Congressional Research Service, "U.S.-EU Privacy Shield", s.14.

sağlamak amacıyla düzenlenmesine rağmen yalnızca 4 yıl gibi kısa bir süre yürürlükte kalabilmiştir.

Gizlilik Kalkanı Anlaşması, halefi olduğu Güvenli Limanda yer alan yedi temel gizlilik ilkesini içermekle beraber, ABAD'ın Schrems I kararında belirttiği endişelere de yer vermekteydi. Gizlilik Kalkanı özellikle, ABD ulusal güvenlik yetkililerinin kişisel verilere olası erişimlerine ilişkin şikâyetleri ele alan Gizlilik Kalkanı Ombudsmanı dâhil tazminat mekanizması ve kişisel verilere erişimin sınırlı olacağına dair ABD yetkililerinin yazılı taahhüt ve güvencelerini içeriyordu. Bunun bir göstergesi olarak ABD Kongresi Şubat 2016'da, 1974 tarihli ABD Gizlilik Yasası'ndaki bazı yargısal tazminat hükümlerini AB vatandaşlarını da kapsayacak şekilde genişleten ABD Adli Tazminat Yasasını kabul etti.

AB ve ABD tarafı, Güvenli Liman ile karşılaştırıldığında Gizlilik Kalkanının, önemli ölçüde daha güçlü gizlilik korumaları, gözetim mekanizmaları, tazminat hakları ve ABD makamlarının kişisel verilere erişimiyle ilgili yeni güvenceler içerdiğini ifade ediyordu[133]. Kişisel verilerinin ABD makamları tarafından ele geçirildiğini düşünen ilgili kişi, doğrudan ABD'li şirketlere veya FTC'ye iletmesi için AB ulusal denetim makamlarına şikâyette bulunabilmekteydi.

Gizlilik Kalkanının çıkış noktasında, ABD makamlarının kişisel verilerine yetkisiz eriştiğini veya kişisel verilerini kötüye kullandığını düşündüğü durumlarda ilgili kişilere ABD mahkemelerine başvurma hakkı da dâhil olacak şekilde yeni güvenlik tedbirlerinin sağlanması, ilgili kişilere bilgilerinin nasıl işlendiği konusunda daha çok kontrol imkânı sağlanması ve ABD makamlarının yeterli bir sebep olmadan verilere erişemeyeceğine dair taahhütte bulunulması hedefleniyordu. Ancak ABAD, nihayetinde Gizlilik Kalkanı Anlaşmasını Schrems II kararı ile geçersiz kılarak uygulamada bu hedeflerin sağlanamadığı kanaatine varmıştır[134]. Gizlilik

[133] Congressional Research Service,"U.S.- EU Privacy Shield", s.10.
[134]Deniz Güngör, "Avrupa Birliği'nden ABD'ye Yapılacak Veri Aktarımlarına İlişkin Gizlilik Kalkanı Anlaşmasının İptali", *Mondaq,* September 30,2020,

Kalkanı Anlaşması, ABD kamu makamlarının AB'den aktarılan kişisel verilere ülkenin iç hukukuna dayanarak yetkisiz erişim sağlaması ve bu verileri kullanması yönündeki uygulamaların orantılı olmadığı ve anlaşmanın AB'nin veri korumaya ilişkin yüksek standartları ile uyum sağlamadığı gerekçeleri ile geçersiz kılınmıştır.

Schrems I kararından sonra Maximilian Schrems, İrlanda ulusal denetim makamına, Facebook'un AB'den ABD'ye veri aktarımları için standart sözleşme maddelerini kullanmasına ilişkin başka bir şikâyette bulundu. Şikâyet, Facebook'un kullanıcılarının kişisel verilerini ABD gözetim programları kapsamında ABD hükümet yetkililerinin erişimine açmak zorunda olduğu için standart sözleşme maddelerinin ABD'ye kişisel verilerin aktarılması için geçerli yasal dayanak olamayacağı şeklindeydi. İrlanda ulusal denetim makamı davayı, iddiaları araştırdıktan ve ABAD'ın standart sözleşme maddelerinin geçerli olup olmadığını inceleyene kadar bu hususta karar veremeyeceğini tespit ettikten sonra İrlanda Yüksek Mahkemesine taşıdı. Ayrıca şikâyet, Facebook'un ABD'ye veri aktarımları için kullandığı ve Komisyon tarafından yeterli koruma sağladığı belirlenen Gizlilik Kalkanının sağladığı koruma düzeyine ilişkin sorular içermekteydi.

İrlanda Yüksek Mahkemesi 2018 yılında yargılamayı durdurarak, standart sözleşme maddelerinin geçerliliği ile ilgili ABAD'a birkaç soru iletmiştir[135]. Başsavcı görüşünde, hem Direktif hem de o tarihte tam anlamıyla yürürlüğe girmiş olan GDPR kapsamında ABAD'a iletilen soruları incelemiştir. Başsavcı, standart sözleşme maddelerini onaylamış[136] ve yeterli koruma sağladığı hususunda şüpheleri olmasına rağmen ABAD'ın Gizlilik Kalkanının geçerliliğini incelemesinin gerekli olmadığını tespit etmiştir[137].

---

https://www.mondaq.com/turkey/privacy-protection/989728/avrupa-birli287i39nden-abd39ye-yapilacak-veri-aktarimlarina-304li351kin-gizlilik-kalkani-anla351masinin-304ptali, Erişim Tarihi: 7.10.2021.

[135] Irish High Court, Data Protection Commissioner v. Facebook Ireland Limited and Maximilian Schrems.

[136] Court of Justice of European Union (CJEU), "Opinion of Advocate General Saugmandsgaard Øe in Case C-311/18", Data Protection Commissioner v. Facebook Ireland Limited and Maximilian Schrems, delivered on 19 December 2019, ECLI:EU:C:2019:1145, para. 343.

[137] Case C-311/18, "Opinion of Advocate General Saugmandsgaard Øe", para. 342.

İrlanda Yüksek Mahkemesi tarafından ABAD'a iletilen sorular, Mahkemenin Schrems II kararında beş başlıkta özetlenmiş olup bunlar, kişisel verilerin kanunun uygulanması ve kamu güvenliği amacıyla üçüncü bir ülkede işlenmesi durumunda ekonomik operatörler *(economic operator)* arasındaki aktarımlar için GDPR'ın geçerli olup olmadığı[138], standart sözleşme maddeleri kapsamındaki koruma seviyesinin ne olduğu[139]; ulusal denetim makamlarının, ilgili maddelere uyum gösterilmez veya yeterli koruma düzeyi sağlanamazsa, standart sözleşme maddeleri kapsamındaki aktarımları askıya almalarının veya yasaklamalarının gerekli olup olmadığı[140]; standart sözleşme maddelerinin Şart kapsamında geçerli olup olmadığı[141] ve Gizlilik Kalkanı Anlaşmasının GDPR kapsamında yeterli seviyede koruma sağlayıp sağlamadığı[142] şeklindedir.

ABAD'ın kararına göre Gizlilik Kalkanı, AB'den ABD'ye kişisel verilerin aktarılması için yeterli bir mekanizma değildir. ABAD, Komisyonun Gizlilik Kalkanı kapsamında aktarılan veriler için yeterli düzeyde koruma sağladığına ilişkin kararını, ABD gözetim yasalarına istinaden ABD'nin veri toplama yetkilerinin genişliğini ve AB'de ki ilgili kişiler için tazminat mekanizmasının eksik olmasını dikkate alarak geçersiz kılmıştır. ABAD'a göre ABD Dış İstihbarat Gözetleme Yasası 702. Bölümü (Foreign Intelligence Surveillance Act - "FISA 702) ABD istihbarat kurumlarının ABD vatandaşı olmayan kişilerin kesinlikle gerekli olandan daha fazla bilgisini toplamaya izin vermektedir. Ayrıca ABAD, Gizlilik Kalkanı Ombudsman sisteminin bağımsızlığını ele alarak, Ombudsmanın ABD istihbarat kurumları üzerinde bağlayıcı bir karar alma yetkisinin olup olmadığının net olmaması sebebiyle söz konusu sistemin yeterli bir tazminat sağlayamayacağına karar verdi.

[138] Case C-311/18, *Schrems II*, para. 80.
[139] Case C-311/18, *Schrems II*, para. 90.
[140] Case C-311/18, *Schrems II*, para. 106.
[141] Case C-311/18, *Schrems II*, para. 122.
[142] Case C-311/18, *Schrems II*, para. 160.

ABAD Gizlilik Kalkanı Anlaşmasını dört ana sebebe dayanarak geçersiz kılmıştır. Bu sebepler, ABD yasalarının Gizlilik Kalkanı gerekliliklerine göre öncelikli olması[143], özellikle orantılılık gereklilikleri kapsamında ABD hukuku uyarınca yetkililerin sahip oldukları yetkilere yönelik gerekli sınırlama ve güvencelerin mevcut olmaması[144], AB'de ki ilgili kişiler için ABD'de etkili bir hukuki yolun bulunmaması[145] ve Gizlilik Kalkanının sahip olduğu Ombudsman sistemindeki eksikliklerdi[146]. ABAD, Şart'ın 7, 8 ve 47. maddeleri çerçevesinde bu konuları değerlendirmiş ve bu eksikliklerle birlikte Gizlilik Kalkanı Anlaşmasını, kararın verilmesi ile birlikte yürürlüğü girmek üzere geçersiz kılmıştır[147].

Schrems II kararının, GDPR m.45 kapsamındaki yeterlilik kararları açısından ilk önemi, bir yeterlilik kararı alınması için gerekli olan yüksek koruma standardına ilişkin Schrems I kararında varılan sonuçları ve söz konusu standardın Şart ışığında okunması gerektiği gerçeğini sağlamlaştırmış olmasıdır[148]. İrlanda Yüksek Mahkemesi, ABD'nin gizlilik ve istihbarat toplama konularına ilişkin uzmanlarının detaylı ifadelerine de başvurmuştur[149]. Bu durum, kararın, ABD yasa ve uygulamalarının dikkate alınarak yapılan değerlendirme ile verildiğini ve bunun da ABAD'ın ABD özelinde üçüncü ülkelere veri aktarımlarında olmasını istediği yüksek standardı pekiştirdiği görülmektedir[150].

ABAD Schrems II kararında AB Hukukunun ihlal edilmesinin önüne geçmek ve GDPR m.44 uyarınca güvence altına alınan gerçek kişilerin koruma düzeyinin zedelenmemesini sağlamak için kişisel verilerin üçüncü bir ülkeye aktarımının gerçekleştirilmesine dayanan GDPR 5. Bölümün hükmüne bakılmaksızın 44. maddede yer alan koruma düzeyinin garanti edilmesi gerektiğine karar vermiştir[151].

[143] Case C-311/18, *Schrems II*, para. 164.
[144] Case C-311/18, *Schrems II*, para. 168-185.
[145] Case C-311/18, *Schrems II*, para. 191-192.
[146] Case C-311/18, *Schrems II*, para. 193-197.
[147] Case C-311/18, *Schrems II*, para. 201-202.
[148] Kuner, Bygrave ve Docksey, *GDPR: Update of Selected Articles*, s.162.
[149] Case C-311/18, "Opinion of Advocate General Saugmandsgaard Øe ", para. 342.
[150] Kuner, Bygrave ve Docksey, *GDPR: Update of Selected Articles*, s.162.
[151] Case C-311/18, *Schrems II*, para. 92 and 105.

Bu durum ABAD'ın, bir yeterlilik kararının sağladığı esasen eşdeğerlilik standardını GDPR 5. Bölümün temel gerekçesi olarak kabul ettiğini göstermektedir[152].

TFEU m.288 gereğince, Komisyonun almış olduğu bir yeterlilik kararı ABAD tarafından yasallığı incelenecek bir karardır ve ulusal denetim makamları da dâhil üye ülkelerin tüm organları için bağlayıcıdır[153]. Bu hükmün anlamı, ABAD tarafından bir yeterlilik kararı geçersiz kılınıncaya kadar, üye ülkeler ve organları bu kararın uygulanmasına mani olamaz[154].

ABAD'ın Schrems II kararının ardından EDPB, veri aktaran ve veri aktarılanların AB veri koruma gerekliliklerini sağladığından emin olmaları için alabilecekleri ilave önlemleri açıkladığı ve standart sözleşme maddelerinin kullanımına ilişkin rehberlik sağlayacak tavsiyeler yayınladı. Ayrıca Komisyon, GDPR'ın ve Schrems II kararının gerekliliklerini içeren yeni standart sözleşme maddeleri yayınladı. AB tarafındaki bu gelişmelere karşın ABD tarafından, şirketlerin aktarımlarının ABAD kararına uygun olarak veri koruması sağlayıp sağlamadığını değerlendirmelerine yardımcı olması için bir teknik inceleme belgesi yayınlandı. Belgede ABD şirketlerin çoğunun, ABD istihbarat teşkilatlarını ilgilendiren verilerle ilgilenmediği ifade edilerek, şirketlerin ABAD'ı ilgilendiren ve Schrems II de ki mahremiyete yönelik belirlenen riskleri içeren veri aktarımlarıyla meşgul olmadıkları belirtilmiştir[155].

ABAD verdiği kararda ayrıca, verileri ABD gözetimine dâhil olabilecek Avrupa vatandaşları için ABD'nin yeterli bir tazminat mekanizmasına sahip olmadığını tespit etti. Tazminat ilkesi uyarınca, Avrupa vatandaşları NSA gibi ABD kurumlarının verilerini gereklilik ve orantılılık ilkelerini ihlal edecek şekilde toplayıp toplamadığını veya işleyip işlemediğini öğrenebilmeli ve ABD

[152] See Case C-362/14, *Schrems I*, para. 73.
[153] Case C-311/18, *Schrems II*, para. 117.
[154] Case C-311/18, *Schrems II*, para. 118.
[155] Congressional Research Service, "U.S.-EU Privacy Shield", s.14 dn. 56.

mahkemelerinde yasal yollara başvurabilmelidir. Bu nedenle Schrems II, ABD gözetim yasasında önemli değişikliklerin yanı sıra yeni bir tazminat mekanizmasının kurulmasını gerektirir.

2.1.5.3 AB ve ABD Arasında Veri Aktarımının Geleceği

ABAD'ın Temmuz 2020'de verdiği Schrems II kararının ardından Gizlilik Kalkanı Anlaşmasını revize etmek veya yerine yeni bir anlaşma yapmak için Avrupa Komisyonu ve DOC arasında müzakereler başladı. Bu çalışmanın hazırlandığı sırada müzakereler devam etmekle birlikte 25 Mart 2021 tarihinde Komisyon ve DOC yetkilileri tarafından yapılan ortak basın açıklamasında, veri koruma ve mahremiyet bağlamında kıtalar arası veri akışının ekonomi ve kişiler açısından önemi vurgulandı[156]. Ayrıca, müzakereler sırasında ABD'nin daha fazla güvence sağlayarak AB vatandaşlarının kişisel verilerinin korunmasına yönelik endişelerini gidermeye çalıştığı görülmektedir[157].

ABAD'ın veri korumasına ilişkin endişelerini dikkate almak ve AB ve ABD arasındaki yaklaşık 6 trilyon dolarlık ticaret ilişkisini korumak adına, ABD'nin gizlilik ve güvenlik önlemlerine ilişkin yasa ve uygulamalarını geliştirmesi, kişisel verilerin AB'den ABD'ye aktarılması kapsamında kritik bir öneme sahip görünüyor[158]. Nitekim ABAD'ın kararı, ABD tarafından gözetim yasasında değişiklikler yapılmasını, tazminat mekanizmasının kurulmasını ve ticari gizlilik yasasının çıkarılmasını gerektirmektedir. Öyle ki Gizlilik Kalkanı Anlaşmasının yerini alacak yeni anlaşmaya ilişkin yapılan görüşmelerin süresi, ABD'nin ABAD'ın gözetim endişelerini yeteri kadar dikkate alıp almayacağına bağlı olacak

[156] Bkz. European Commission, "Intensifying Negotiations on Transatlantic Data Privacy Flows: A Joint Press Statement by European Commissioner for Justice Didier Reynders and U.S. Secretary of Commerce Gina Raimondo", 25.03.2021, https://ec.europa.eu/commission/presscorner/detail/en/STATEMENT_21_1443, Erişim Tarihi: 26.11.2021.
[157] Congressional Research Service, "U.S.-EU Privacy Shield", s.17.
[158] Bkz. Emily Skahill, "Trans-Atlantic Data Flows: What's Next After the EU-U.S. Privacy Shield?", July 29, 2021, https://www.brookings.edu/events/transatlantic-data-flows-whats-next-after-the-eu-u-s-privacy-shield/, Erişim Tarihi: 24.11.2021.

ve bu dikkatin gereği olarak ABD'nin yeterli bir tazminat mekanizmasını kurması ve gözetim uygulamalarına ilişkin yenilikler yapması da müzakerelerin önemli görüşme konuları arasında olacaktır[159].

ABAD'ın Schrems II kararı ile AB'den ABD'ye kişisel veri aktarımlarında 2016'dan itibaren yürürlükte olan Gizlilik Kalkanı Anlaşmasının geçersiz kılınması AB ve ABD işletmelerini veri aktarımları için alternatif yöntemler arayışına zorladı. Gizlilik Kalkanının geçersiz kılınmasıyla AB'den ABD'ye veri aktarımları için yasal dayanak olarak artık geçerli bir yeterlilik kararının mevcut olmaması ve aktarım için diğer mekanizmaların kullanılması gerekliliği küçük ve orta büyüklükteki şirketler için büyük maliyetlere sebep olmaktadır. Büyük çaplı işletmeler, yine ABAD'ın kararı ile aktarım koşulları ağırlaşan ve ayrıca Komisyon tarafından güncellenerek yeni gerekliliklere sahip olan standart sözleşme maddeleri yoluyla aktarımların yüksek maliyetlerine katlanabilirken, küçük ve orta büyüklükteki şirketler için maliyetler bu şirketlerin maddi sınırlarını zorlamaktadır[160]. Bu bakımdan Gizlilik Kalkanının halefi olacak bir anlaşmanın müzakere edilmesi ve görüşmelerin olumlu sonuçlanması AB'den ABD'ye veri aktarımının sürekliliği açısından önem arz etmektedir.

ABD'nin, tüketici mahremiyetine ilişkin şirketlerin veri toplama ve saklamalarına yönelik kısıtlamaların olduğu bir yasayı yürürlüğe koyarak kamu yetkililerinin verilere erişim riskini en aza indirmesi, ABD'nin kişisel verileri AB'nin veri koruma standardına uygun koruyacağına ilişkin güven oluşturacak ve söz konusu müzakerelerin AB tarafında tatmin edici olarak sonuçlanması ile veri aktarımının kolaylaşmasına yardımcı olacaktır[161].

Nihayetinde, Gizlilik Kalkanının yerini alacak yeni bir anlaşma için AB ve ABD arasında yapılan müzakereler ve bu müzakerelerin süresi, ABD'nin gözetim

[159] Skahill, "Trans-Atlantic Data".
[160] Skahill, "Trans-Atlantic Data".
[161] Skahill, "Trans-Atlantic Data".

uygulamalarında yapacağı modernizasyon ve ticari gizlilik yasasını çıkarmasına ve bu gelişmelerin ne kadar sürede gerçekleşeceğine göre neticelenecektir.

2.2 Uygun Güvencelere Tabi Aktarımlar

95/46 sayılı Direktif yürürlüğe girdiğinde, çoğu ülkenin yeterlilik kararından faydalanamayacağı düşünülüyordu ve bu durum, uygun güvenceler olarak bilinen yöntemlerle AB dışına kişisel veri aktarımı yapılması ihtimalini ortaya çıkardı[162]. Uygun güvenceler, hem ilgili kişiler hem de ulusal denetim makamları için hukuki çözümlerle desteklenen, kişisel veriler üzerinde yeterli seviyede koruma sağlamak için şirketlerin hukuki olarak bağlayıcı taahhütlerde bulunduğu yöntemlerdir.

GDPR'da yer alan uygun güvenceler, 95/46 sayılı Direktif m.26 kapsamındaki hükümlerin temel alınması ve genişletilmesiyle oluşturulmuştur[163]. GDPR m.46(1) ve Gerekçe 108, bir yeterlilik kararının mevcut olmaması durumunda veri sorumlusu ve veri işleyenin üçüncü ülkelerde kişisel verilerin korunmasına ilişkin eksiklikleri uygun güvenceler ile telafi etmeye yönelik önlem almasını gerektirir[164]. Bu kapsamda, söz konusu uygun güvencelerin sağlanması ve GDPR'da yer alan ilgili diğer hükümlere uyulması durumunda GDPR m.46(2)'de yer alan aktarım araçları kullanılarak üçüncü ülkelere ve uluslararası kuruluşlara kişisel veri aktarımı gerçekleştirebilecektir[165]. Söz konusu uygun güvenceler ile veri sorumlusu ve veri işleyen tarafından ilgili kişinin kişisel verilerine ilişkin temel hak ve özgürlüklerinin korunması amaçlanmaktadır. Bu aktarım yöntemleri genellikle alternatif aktarım araçları/mekanizmaları olarak isimlendirilir[166]. Nitekim GDPR 5. Bölüm, öncelikle yeterlilik kararının bulunması durumunda bu yeterlilik kararına istinaden aktarım yapılmasını, yeterlilik kararının bulunmadığı durumlarda alternatif olarak uygun güvencelerin kullanılmasını gerektirir.

---

[162] Theodorakis, s.26.
[163] Kuner, Bygrave ve Docksey, *GDPR: A Commentary*, s.799.
[164] EDPB, " Recommendations 01/2020", s.8.
[165] EDPB, " Recommendations 01/2020", s.7.
[166] Theodorakis, s.27.

GDPR m.46(2)'de yer alan uygun güvenceler için, Direktiften farklı olarak bir denetim makamından özel bir izin alınmasına gerek olmamakta fakat BCR, davranış kuralları ve sertifikasyon mekanizmaları için denetim makamı onayı gerekmektedir. Yalnız, onay alındıktan sonra bu yöntemler veri aktaranların sorumluluğu altında kullanılabilir. GDPR m.46(3)'e göre özel sözleşme maddeleri *(ad hoc contractual clauses)* ve kamu makamları veya organları arasındaki idari düzenlemeler *(administrative arrangements between public authorities or bodies)* ulusal denetim makamından izin gerektirir.

Uygun güvenceler sadece belirli aktarım veya aktarım türlerine koruma sağladığından GDPR m.45(2) kapsamında bir yeterlilik kararı alınırken göz önünde bulundurulması gereken belirli veri koruma risklerine karşı koruma sağlayamazlar[167]. Yeterlilik kararı verilmesi değerlendirmesinde verilerin aktarılacağı üçüncü ülkenin veya uluslararası kuruluşun hukuk sistemi dikkate alınır. Ancak uygun güvencelere dayalı aktarımlarda üçüncü ülke veya uluslararası kuruluşta aktarılan veri için geçerli bir korumanın varlığı aranmaktadır[168].

Uygun güvenceler, GDPR m.46 ve m.47'de düzenlenmiş sekiz ana yöntemden oluşmaktadır. 95/46 sayılı Direktifte yer almayan kamu makamları veya organları arasında yasal olarak bağlayıcı ve uygulanabilir belgeler, onaylanmış davranış kuralları, onaylanmış sertifika mekanizması ve idari düzenlemelere eklenen hükümler GDPR'ın getirdiği uygun güvencelere tabi yeni aktarım mekanizmalarıdır.

ABAD Schrems II Kararında, GDPR m.46 kapsamındaki "uygulanabilir haklar" *(enforceable rights)*, "etkili yasal yollar" *(effective legal remedies)* ve "uygun güvencelere" *(appropriate safeguards)* ilişkin kavramların, aktarımlara ilişkin genel ilkeleri düzenleyen ve GDPR'ın 5. Bölümünde yer alan tüm hükümlerin GDPR tarafından garanti edilen gerçek kişilerin koruma düzeyinin zayıflatılmaması

[167] Kuner, Bygrave ve Docksey, *GDPR: A Commentary*, s.802.
[168] Kuner, Bygrave ve Docksey, *GDPR: A Commentary*, s.799.

için uygulanacağını belirten GDPR'ın 44. maddesi ışığında yorumlanması gerektiğini belirtmiştir[169]. Ayrıca, GDPR Gerekçe 108 herhangi bir uygun güvencenin GPDR m.5 kapsamında düzenlenen kişisel veri işlemeye ilişkin genel ilkelerle uyumlu olması gerektiğini belirtir.

2.2.1 Yasal Olarak Bağlayıcı ve Uygulanabilir Belgeler

GDPR m.46'da yer alan uygun güvencelerden ilki, "kamu kuruluşları ve organları arasında hukuki olarak bağlayıcı ve uygulanabilir olan belgeler" başlığı ile m.46(2)(a)'da düzenlenmiştir. Bu uygun güvence yöntemi ile AB'deki kamu kuruluşları veya organları ile üçüncü ülkelerde bulunan kamu kuruluşları arasında uygulanabilir hukuki belgelere dayanarak veri aktarımı yapılabilir. Örneğin, AB'de yer alan bir kamu makamı ile üçüncü ülkede bulunan bir kamu makamı arasında veri aktarımı için uluslararası bir sözleşmenin varlığı bu güvence kapsamında düşünülebilir[170]. GDPR m.46(2)'ye göre bu yöntemin kullanılabilmesi için ulusal denetim makamından onay alınması gerekliliği bulunmamaktadır. Eğer taraflardan birinin yasal olarak bağlayıcı ve uygulanabilir belge düzenleme yetkisi bulunmuyorsa m.46(3)(b)'de yer alan idarî düzenlemelere eklenen hükümler yöntemi kullanılır[171]. EDPB tarafından 15 Aralık 2020 tarihinde, GDPR m.46(2)(a) ve m.46(3)(b) uyarınca AB'de yer alan kamu kuruluşları ve organlarından üçüncü ülkelerdeki kamu kuruluşlarına veya uluslararası kuruluşlara kişisel verilerin aktarılmasına ilişkin rehber yayınlanmıştır[172].

2.2.2 Bağlayıcı Şirket Kuralları

BCR'ler çok uluslu grup şirketlerinin kendi aralarında yaptıkları veri aktarımları için hukuki olarak bağlayıcı kurallar ve politikalardır. AB Hukukunda 95/46 Sayılı

[169] Case C-311/18, *Schrems II*, para. 92.
[170] Kuner, Bygrave ve Docksey, *GDPR: A Commentary*, s. 806.
[171] Bkz. Bölüm 2.2.7.
[172] Bkz. https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-22020-articles-46-2-and-46-3-b-regulation_en, Erişim Tarihi: 10.10.2021.

Direktifte yazılı bir şekilde yer almayan BCR'ler, WP29 çalışma belgeleri ile gündeme gelmiştir. WP29, çok uluslu şirketlerin 95/46 sayılı Direktif doğrultusunda kendi oluşturdukları fakat kişisel verileri korumada eksik kalan gizlilik politikalarında yer alması gereken bazı kriterler belirlemiştir[173]. Bu kriterlerden en önemlisi, bu politikaların hem şirket içinde yani şirket ve şirkete bağlı grup şirketlerinde hem de şirket dışında, ilgili kişilerin menfaatleri doğrultusunda şirketler için bağlayıcı olmasıydı[174]. Bahse konu bağlayıcılığa atıf yapmak amacıyla WP29 tarafından bu politikalar Bağlayıcı Şirket Kuralları olarak adlandırılmıştır.

Çok uluslu şirket gruplarının farklı ülkelerde yer alan şirketlerden oluşması sebebiyle grup şirketleri içindeki kişisel veri aktarımları, farklı hukuki düzenlemelere tabi olabilir. Gruba dâhil şirketler arasında kişisel veri aktarımlarını düzenlemek ve uygulamada meydana gelen ihtiyaçları gidermek amacıyla 95/46 sayılı Direktif m.26 ve m.29'a istinaden WP29 tarafından oluşturulan BCR'ler ile farklı ülkelerde farklı kurallar yerine tüm grup şirketlerini kapsayacak şekilde geçerli tek bir veri koruma kuralı meydana getirilmiştir[175].

WP29 tarafından BCR'ler için rehber niteliğinde olan çok sayıda belge yayınlanmıştır. BCR'ler için temel gereklilikleri ve onay süreçlerinin temelini bu belgeler oluşturmuştur. WP29'un hazırladığı belgelerin büyük çoğunluğu, WP29 yerine kurulan EDPB tarafından uygun görülmüş ve halen rehber olarak

---

[173] Murat Volkan Dülger, Cansu Ceren Kahraman, "KVKK'dan Kişisel Verilerin Yurt Dışına Aktarımında Önemli Bir Adım: Bağlayıcı Şirket Kuralları", 24 Şubat 2021, s.2, https://ssrn.com/abstract=3792375, Erişim Tarihi: 11.10.2021; Murat Volkan Dülger, Cansu Ceren Kahraman, "GDPR ve KVKK Ekseninde Bağlayıcı Şirket Kuralları", *Hukuk ve Daha Fazlası*, 26 Mayıs 2021, s.62, https://ssrn.com/abstract=3853724, Erişim Tarihi: 11.10.2021.

[174] Dülger ve Kahraman, "KVKK'dan Kişisel Verilerin Yurt Dışına", s.2; Dülger ve Kahraman, "GDPR ve KVKK Ekseninde Bağlayıcı Şirket Kuralları", s.62.

[175] 95/46 sayılı Direktif zamanında, AB üye ülkelerin ulusal denetim makamlarının BCR'lere bakış açılarında farklılıklar bulunmaktaydı. Bazı denetim makamları BCR'leri 95/46 sayılı Direktif m.25 kapsamında verilerin aktarıldığı ülkede yeterli koruma oluşturan belgeler olarak görmüşler ve bu madde kapsamda bir aktarımın yapılabilmesi için denetim makamının onayı gerekmediğinden onay alınması denetim makamları tarafından isteğe bağlı hale getirilmiştir. Bazı denetim makamları ise BCR'leri Direktif m.26(2) kapsamında sözleşme maddelerine benzer olarak değerlendirmiş ve onaylanması gerektiğini belirterek uygun güvence olarak onaylamışlardır.

kullanılmaktadır. WP29 tarafından 95/46 sayılı Direktif zamanında düzenlenen BCR'ler daha sonra geliştirilerek GDPR'da detaylı bir şekilde yer almıştır. Bu kapsamda GDPR'da yer alan BCR'ler için temel gereklilikler çoğunlukla WP29 belgelerinden alınmış ve sadeleştirilmiştir. Hâlihazırda BCR'lere ilişkin WP29 tarafından oluşturulmuş ve EDPB tarafından onaylanan ve halen faydalanılan beş güncel belge bulunmaktadır[176].

GDPR, 95/46 sayılı Direktifin aksine BCR'leri kişisel verilerin çok uluslu bir şirket grubu içerisinde aktarılmasına ilişkin hukuki bir dayanak olarak açıkça tanımaktadır. BCR'ler GDPR m.46(2)(b)'de bir yeterlilik kararının olmadığı durumlarda kişisel verilerin aktarılmasına yasal dayanak olabilecek bir uygun güvence aktarım mekanizması olarak düzenlenmiştir. Diğer uygun güvenceler gibi BCR'ler de ilgili kişilerin kişisel verilerine ilişkin hak ve özgürlüklerin korunmasını amaçlamaktadır. BCR'lerin GDPR'da yer almasının amaçlarından birisi de, Birlik genelinde daha uyumlu standartların olması ve BCR'lerin onaylanması için daha güncel bir prosedür oluşturmaktır[177].

BCR'lerin tanımı GDPR m.4(20)[178]'de yapılmıştır. BCR'lerin kişisel verilerin aktarılmasında kullanılması için temel koşullar ise GDPR m.47'de düzenlenmiştir. BCR'lerin onay süreçlerine dair hükümler ise m.57, m.63 ve m.64'de yer almaktadır. GDPR Gerekçe 110, bir grup şirketin veya ortak ekonomik işbirliği içinde bulunulan teşebbüslerin AB'den, aynı grupta yer alan AB dışındaki şirketlere yaptıkları uluslararası veri aktarımları için onaylanmış bir BCR kullanabileceklerini belirtir. Söz konusu gerekçede, ilgili BCR'lerin kişisel veri işleme ilkelerini içermesi ve ilgili kişilerin haklarını mutlaka taahhüt etmesi gerektiği de

[176] WP29 tarafından oluşturulan ve halen faydalanılan güncel belgeler için bkz. https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/binding-corporate-rules-bcr_en#howistheleadauthoritychosen, Erişim Tarihi: 8.10.2021.
[177] Kuner, Bygrave ve Docksey, *GDPR: A Commentary*, s. 816.
[178] GDPR m.4(20)'ye göre BCR'ler " *ortak bir ekonomik faaliyette bulunan bir işletmeler grubu veya teşebbüsler grubu içinde bir veya daha çok sayıda üçüncü ülkede yer alan bir veri sorumlusu veya veri işleyeni, kişisel verileri aktarılmasına ilişkin AB üye ülkelerinden birinin sınırları içinde kurulmuş olan veri sorumlusu veya veri işleyen tarafından uyulması gereken kişisel veri koruma politikaları*" olarak tanımlanmıştır.

belirtilmiştir. Gerek GDPR m.4(20)'de yer alan tanımda gerekse GDPR Gerekçe 110'da, veri sorumlusu ve veri işleyen olarak bir ayrım yapılmamış ancak işletmeler grubu ve ortak bir ekonomik iş birliği içerisindeki teşebbüsler olarak sınırlama getirilmiştir.

95/46 Sayılı Direktif'te yazılı olarak yer almayan BCR'ler, GDPR'da grup şirketleri veya ortak bir faaliyet içinde bulunan teşebbüslerin BCR'ler ile veri aktarımı yapabileceği şeklinde düzenlenmiştir. BCR'ler, çok uluslu şirket grupları, teşebbüs grupları veya bayilikler, ortak girişimler veya profesyonel ortaklıklar gibi ortak bir ekonomik faaliyette bulunan her türlü yapı tarafından kullanılmak üzere tasarlanmıştır[179]. GDPR'ın ifadesinden anlaşılan, BCR düzenleyebilmek için hukuki olarak bir grup şirket yapısı olması zorunlu olmadığıdır[180]. Teşebbüs gruplarının neler olduğu GDPR'da açıkça belirtilmemiş olsa da, sadakat programı kapsamında işbirliği içindeki havayolu şirketleri veya adi ortaklıklar teşebbüs grubu olarak düşünülebilir[181].

GDPR m.46(5)'e göre GDPR'dan önce Direktif döneminde yürürlüğe girmiş olan BCR'ler GDPR yürürlüğe girdikten sonra da ulusal denetim makamı tarafından iptal edilmediği takdirde hukuka uygun olmaya devam edecektir. Nitekim BCR'si GDPR öncesi dönemde onaylanan pek çok şirket, hala bu BCR'leri kullanmaya devam etmektedir.

WP29 tarafından hazırlanan ilk BCR taslağı sadece veri sorumluları için oluşturulmasına rağmen GDPR'a göre hem veri sorumluları hem de veri işleyenler BCR'leri kullanabilmektedir. Veri sorumlusu BCR'leri, AB'de bulunan veri sorumlusundan başka bir grup şirketi veri sorumlusuna veya AB dışında bulunan veri işleyenlere kişisel veri aktarımları için kullanılır. Ayrıca veri sorumlusu

[179] ICO, "International Transfers".
[180] Rüya Tuna Toparlak, "Veri Koruması Hukukunda Bağlayıcı Şirket Kuralları: 2016/679 Sayılı Genel Veri Koruma Tüzüğü ve 6698 Sayılı Kişisel Verilerin Korunması Kanunu Karşılaştırması", Yüksek Lisans Tezi, Türk Alman Üniversitesi, İstanbul: Şubat 2021,s.61.
[181] Theodorakis, s.33.

BCR'leri aynı grup içinde veri sorumlusu olarak faaliyet gösteren kuruluşlara ve dâhili veri işleyeni olarak faaliyet gösteren kuruluşlara karşı da uygulanır. Veri işleyen BCR'leri ise şirket grubunun içerisinde olmayan AB'de yerleşik bir veri sorumlusundan alınan ve sonrasında veri işleyen veya alt veri işleyen olarak hareket eden grup üyeleri tarafından işlenen kişisel veriler için geçerlidir. Bu yöntem standart sözleşme maddelerini veri sorumluları ile yapılan hizmet sözleşmelerine dâhil etmenin diğer bir yoludur[182].

BCR'lerin taşıması gereken kriterler GDPR m.47(1)'de düzenlenmiştir. GDPR m.47(1)(a)'ya göre BCR'ler, çalışanlarda dâhil olacak şekilde ortak bir ekonomik faaliyette bulunan işletmeler grubu veya teşebbüsler grubunun her üyesi için yasal olarak bağlayıcı olmalı ve her üye tarafından uygulanmalı ve yürütülmelidir. GDPR m.47(1)(b)'ye göre BCR'ler ilgili kişilere, kişisel verilerin işlenmesine dair uygulanabilir hakları vermelidir. BCR'ler GDPR m.47(1)(c)'ye göre GDPR m.47(2)'de yer alan minimum gereklilikleri içermelidir.

WP29 veri sorumlusu ve veri işleyen BCR'leri için bir takım önemli ilkelere dikkat çekmiş olup bu ilkeler; şikâyette bulunma hakkı, şeffaflık, uygulama kapsamı, veri koruma ilkeleri, hesap verilebilirlik, üçüncü ülke mevzuatı, üçüncü taraf lehtar hakları ve hizmet sözleşmesi ilkeleri şeklindedir[183].

GDPR m.5(2)'ye göre veri sorumlularının, m.5(1)'de yer alan veri işleme ilkelerine uygun davranmaları ve uygun davrandıklarını kanıtlamaları yani hesap verebilir olmaları gerekmektedir. BCR'lerin grup şirket dâhilinde hesap verilebilirliği sağlamayı ve bunu kanıtlamayı amaçlaması kanun ile uyumu göstermesi açısından en önemli avantajlarından biridir[184]. Öyle ki, BCR'ler hukuk muhakemesi kuralları

[182] PwC, "Binding Corporate Rules", s.1, https://www.pwc.com/m1/en/publications/documents/pwc-binding-corporate-rules-gdpr.pdf, Erişim Tarihi: 26.11.2021.
[183] WP29, "Working Document on Binding Corporate Rules for Controllers (WP256 rev.01)", 09.02.2018 https://ec.europa.eu/newsroom/article29/items/614109, Erişim Tarihi: 26.10.2021.
[184] Toparlak, s.46.

uyarınca veya idarî yargılamalarda geçerli bir kanıt aracı olarak görülmektedir[185]. BCR'lerde yer alması gereken hesap verilebilirlik ilkesi WP29 tarafından ilk oluşturulduğundan beri temel bir ilkedir.

GDPR'da BCR'ler için bir onay süreci yer almaktadır. GDPR m.47(1)'e göre BCR'ler ulusal denetim makamları tarafından, GDPR m.63'de yer alan tutarlılık mekanizması *(consistency mechanism)* kapsamında onaylanmaktadır. BCR'lerin değerlendirmesi ve onaylanması Komisyon'un yetkisinde değildir. BCR'lerin onaylanması için grup içinde yer alan şirketlerden birinin yerleşik olduğu AB üye ülkesinde bulunan ulusal denetim makamına başvuruda bulunması gerekmektedir. Birden çok AB üye ülkesinde kurulu şirketler için birkaç AB ülkesinin denetim makamına başvuru yapılabilir. Burada bahsedilen denetim makamlarından birisi "Baş Denetim Makamı" olmalıdır. GDPR m.47 uyarınca taslak BCR'leri ulusal denetim makamının onayına sunan şirket, BCR'leri onaylayacak baş denetleyici belirlenmesi için bir denetim makamı önermelidir. Şirket grubunun BCR'ler için önereceği baş denetleyiciyi seçme kriterleri WP29 tarafından hazırlanan "Bağlayıcı Şirket Kurallarının Onaylanmasına İlişkin İş Birliği Prosedürü Hakkında Çalışma Belgesi"nde belirlenmiştir[186]. Söz konusu belgede ilgili kriterler, grubun Avrupa genel merkezinin konumu, yetkilendirilmiş veri koruma sorumlulukları bakımından şirketin grup içindeki konumu, grupta BCR'leri uygulamak için en iyi konumda olan şirketin yeri, aktarımla ilgili çoğu kararın alındığı şirketin yeri ve üçüncü ülkelere aktarımların çoğunun veya tamamının yapılacağı AB üye ülkesi olarak belirlenmiştir. Bu kriterlerden grubun Avrupa genel merkezinin konumu baş denetçiyi belirlemede en önemli kriterdir.

BCR onayı için başvuran şirket ilk önce baş denetim makamına başvurmalıdır. Söz konusu ulusal denetim makamı GDPR m.56 kapsamında baş denetim makamı olarak BCR'leri onaylar. GDPR m.55 ve m.56'da uyarınca baş denetim makamı

[185] Toparlak, s.46.
[186] Bkz. WP29, "Working Document on the approval procedure of the Binding Corporate Rules for controllers and processors (WP 263 Rev.01)", 16.04.2018, https://ec.europa.eu/newsroom/article29/items/623056, Erişim Tarihi: 26.10.2021.

BCR'leri onaylamayı amaçlanması durumunda, EDPB'nin görüşünü almak üzere taslak kararı EDPB'ye iletir[187]. EDPB'den onay alındığı takdirde başka bir merciden onay almaya gerek olmamaktadır. Grup şirketine bağlı şirketlerin yerleşik olduğu diğer AB ülkelerinde bulunan ulusal denetim makamları da bu onay sürecine dâhil olmaktadır. Bu sebeple BCR'lerin onayı farklı ülkelerdeki ulusal denetim makamlarının karşılıklı işbirliği ve taahhütlerini gerektirmektedir. BCR'lerin onay süreçlerinin ve prosedürlerinin eskiye göre daha hızlı bir şekilde ilerlemesi BCR'leri sadece çok büyük çok uluslu şirketler için değil birçok şirket için kullanılabilir bir yöntem haline getirmektedir[188].

Burada hatırlatılması gereken önemli bir husus, Brexit sonucunda Birleşik Krallık'ın AB'den ayrılmasıyla ICO'nun artık EDPB'nin bir üyesi olmadığı ve bu çerçevede GDPR kapsamında BCR'ler için baş denetim makamı olamayacak olmasıdır[189]. Bu nedenle EDPB, ICO'nun baş denetim otoritesi olduğu şirket grupları ve teşebbüslerinin BCR'lerine ilişkin bir bilgi notu yayınlamış ve bir dizi gereklilikler belirlemiştir[190].

GDPR m.47(3)'de, veri sorumluları, veri işleyenler ve denetim makamları arasında BCR'lere ilişkin bilgi alışverişi için format ve prosedürlerin Komisyon tarafından belirlenebileceği yer almaktadır. Bu durum benimsenirse, bir takım model BCR hükümleri veya onay prosedürleri oluşturulması ile BCR onaylarının daha kolay hale gelmesi sağlanabilir ve denetim makamları üzerinde bağlayıcı olabilir[191]. Grup şirketinin AB'de sadece bir şirketi mevcutsa m.63'de yer alan tutarlılık mekanizmasının uygulanmasına gerek yoktur. Nitekim ulusal denetim makamları GDPR m.57(1)(s) ve m.58(3)(j) hükmüne dayanarak kendi bölgelerindeki BCR'leri onaylama yetkisine sahiptir.

---

[187] GDPR m.64(1)(f).
[188] Kuner, Bygrave ve Docksey, *GDPR: A Commentary*, s.821.
[189] EDPB, "Information Note on BCRs for Companies Which Have ICO as BCR Lead Supervisory Authority", 12.02.2019, https://edpb.europa.eu/sites/default/files/files/file1/edpb-2019-02-12-infonote-bcrs-brexit_en_0.pdf, Erişim Tarihi: 26.10.2021.
[190] EDPB, "Information Note on BCRs".
[191] Theodorakis, s.34.

Farklı ülkelerde yer alması sebebiyle farklı hukuki düzenlemelere tabi olan şirketler için yüksek seviyede veri koruması sağlayan BCR'ler[192], çok uluslu şirketlerin kişisel verilerini aynı şirket grubu içerisinde, GDPR'a uygun olarak kişisel veriler için yeterli düzeyde koruma bulunmayan üçüncü ülkelere aktarmasına imkân tanır. BCR'ler, grup şirketinin veri işleme süreçlerine istinaden ihtiyaçlara göre oluşturulmakta ve ulusal denetim makamı tarafından onaylanmaktadır. Bu anlamda BCR'ler çok uluslu bir şirketin içyapısına uygun oluşturulmuş özel nitelikli[193] kişisel veri koruma politikası araçlarıdır. Bu kurallar şirketin tüm üyelerinin veri işleme faaliyetinde kullandığı ve tabi olduğu bağlayıcı kurallardır. Bundan dolayıdır ki grup şirketi dâhilinde eşit ve GDPR'a uygun veri koruması taahhüt eden bu kurallar metni, grup şirketi üyeleri arasında veri aktarımı için uygun güvence sağlar ve verilere serbest dolaşma imkânı tanır[194]. Çok uluslu bir şirketin BCR'leri kullanması, şirketin veri koruma politikasının dünyanın diğer ülkelerinde yerleşik tüm grup şirketleri açısından standart hale gelmesi ve GDPR'da yer alan belli standartlara sahip olması açısından şirketlere büyük avantaj sağlamaktadır[195]. BCR'lerin şirketlere sağladığı faydaların yanında, BCR'leri sürdürebilmek ve güncel tutabilmek için daha fazla çaba sarf edilmesi gerekir[196].

BCR'ler bazı durumlarda daha sıkı kurallara sahip standart sözleşme maddelerine alternatif olarak kullanılabilmektedir. Çok uluslu bir şirket, standart sözleşme maddeleri yöntemini kullanarak üyeleri arasında birçok farklı kategoriye sahip kişisel veri aktarımı yaptığında BCR yöntemine göre daha zor bir prosedür ile karşılaşmaktadır. Bu iki yöntemin ikisi de sözleşmeye dayalı taahhüt özelliği taşımaktadır[197] Fakat BCR'ler ile yapılan aktarımlarda veri çeşidinde bir sınırlama

[192] Rolf H. Weber, Dominic Staiger, *Transatlantic Data Protection in Practice*, Springer, 2017, s.36.
[193] GDPR m.9(1)'de, kişinin ırksal veya etnik kökeni, siyasi görüşü, dini veya felsefi inancı, sendika üyeliğine ilişkin bilgiler ile genetik verileri, biometrik verileri ve sağlık veya cinsel yaşamına ilişkin bilgileri özel nitelikli kişisel veri olarak kabul edilmiştir.
[194] Daniela Fábián Masoch, "Why Should Companies Invest in Binding Corporate Rules?", *Data Protection 2019*, ICLG.com, 03.07.2019. s.12-13.
[195] Toparlak, s.37.
[196] Bulck, s.242.
[197] Toparlak, s.38.

yapılmamakta[198] ve BCR'ler tüm verilerin aktarımına uygun olarak hazırlanmaktadır. Standart sözleşme maddeleri ise veri aktaran ve veri aktarılan arasında aktarımı yapılacak verinin niteliğine göre oluşturulmaktadır.

Öte yandan ABAD'ın Schrems II kararının BCR'ler üzerinde de etkisi bulunmaktadır. ABAD Schrems II kararında uygun güvenceler mekanizması ile veri aktarımının, Şart ışığında okunan AB veri koruma yasası ile esasen eşdeğer bir koruma seviyesi gerektirdiğine karar vermiştir[199]. Bahse konu uygun güvencelerde ABAD, BCR'ler den bahsetmemiştir. Ancak EDPB, karardan sonra yayınladığı nihai tavsiyede, burada bahsedilen koruma seviyesinin GDPR m.46(2)'de yer alan ve sözleşmeye dayalı özellikte olan tüm uygun güvenceler için geçerli olduğunu belirtmiştir[200]. Bu tespit, Schrems II kararında ABAD'ın uygun güvenceler için belirlediği AB Hukuku ile eşdeğer koruma gerekliliğinin GDPR m.46(2)(b)'de yer alan ve sözleşmeye dayalı bir uygun güvence olan BCR'leri de etkilediği ve standart sözleşme maddeleri için gerekli olan ilave önlemlerin BCR'ler içinde kullanılabileceği anlamına gelmektedir[201].

Bu çerçevede özellikle üçüncü ülke mevzuatının temel haklara muhtemel müdahalesi göz önünde bulundurularak, BCR'ler tarafından sağlanan garantilerin uygulamada yerine getirilip getirilemeyeceğini belirlemek için ilgili üçüncü ülkede AB Hukukunun gerekliliklerine uyulması gerektiği belirtilmiştir[202]. BCR'ler ile ilgili olarak EDPB'nin vurguladığı bir diğer durum, standart sözleşme maddeleri veya BCR'lerin temin ettiği garantilere uygulamada uyulup uyulamayacağının belirlenmesi için üçüncü ülkede AB yasalarının gerektirdiği koruma seviyesine uyulup uyulmadığı değerlendirmesinin veri aktaran ve veri aktarılan tarafın sorumluluğunda olduğudur[203]. Durum bunun aksine ise, veri aktaran ve veri

[198] BCR'ler de genel olarak veri çeşidinde bir sınırlama yapılmamakla birlikte, aktarım yapılacak kişisel veri grubunun sınırlanması imkânı da vardır. (Örneğin: finansal veriler).
[199] Case C-311/18, *Schrems II*, para. 105.
[200] Case C-311/18, *Schrems II*, para. 132; EDPB, " Recommendations 01/2020", s.24.
[201] EDPB, " Recommendations 01/2020", s.24.
[202] EDPB, " Recommendations 01/2020", s.24.
[203] EDPB, " Recommendations 01/2020", s.24-25.

aktarılan, üçüncü ülkede AB'de öngörülen korumaya esasen eşdeğer seviyede bir korumayı temin etmek için ilave önlemler sağlayıp sağlayamayacağını ve üçüncü ülke yasa ve uygulamalarının bu ilave önlemlere etkilerini değerlendirmelidir[204]. Nitekim Schrems II kararında yer alan bu hususlar, Norveç yerel denetim makamı tarafından onaylanan Jotun Şirketine ait BCR[205] ve İsveç yerel denetim makamı tarafından onaylanan Tetra Pak şirketine ait BCR[206]'ler de yer almış ve söz konusu BCR'ler EDPB tarafından onaylanmıştır[207].

Ayrıca bu bağlamda ABAD'ın Schrems II davasında, AB'de yerleşik bir veri sorumlusu veya veri işleyenin GDPR'ın gerektirdiği esasen eşdeğer koruma seviyesini garanti altına almak için yeterli ilave önlemleri almadığı durumlarda ulusal denetim makamının aktarımı askıya alması veya sonlandırması gerektiğine ilişkin kararı[208] BCR'ler ile veri aktarımı için de geçerli olacaktır.

2.2.3 Standart Sözleşme Maddeleri

GDPR m.46'da yer alan bir diğer uygun güvence standart sözleşme maddeleridir. Diğer uygun güvenceler gibi standart sözleşme maddeleri de GDPR m.45(3) uyarınca verilen bir yeterlilik kararının bulunmadığı durumlarda üçüncü ülkelere veya uluslararası kuruluşlara kişisel veri aktarımı için hukuki dayanak sağlar.

---

[204] EDPB, " Recommendations 01/2020", s.25.
[205] Bkz. Norwegian Data Protection Authority, "Decision of the Norwegian Data Protection Authority Approving Binding Corporate Rules of Jotun Group",18 August 2020, https://edpb.europa.eu/sites/default/files/bcr_decision_sa/no_final_decision_bcr-c_jotun20200818.pdf, Erişim Tarihi: 12.10.2021.
[206] Bkz. Swedish Data Protection Authority,"Decision Approving the Binding Corporate Rules of Tetra Pak Group", 17.08.2020, https://edpb.europa.eu/sites/default/files/bcr_decision_sa/se_sa_final_decision_bcr-c_tetra-pak_2020081_7_en.pdf , Erişim Tarihi: 14.10.2021.
[207] EDPB, "Opinion 25/2020 on the draft decision of the Swedish Supervisory Authority regarding the Controller Binding Corporate Rules of Tetra Pak", 31.07.2020, https://edpb.europa.eu/sites/default/files/files/file1/edpb_opinion202025_bcr-c_tetrapak_en.pdf, Erişim Tarihi: 12.10.2021; EDPB, "Opinion 24/2020 on the draft decision of the Norwegian Supervisory Authority regarding the Controller Binding Corporate Rules of Jotun", 31.07.2020, https://edpb.europa.eu/sites/default/files/files/file1/edpb_opinion202024_bcrcontrollerjotun_en.pdf , Erişim Tarihi: 14.10.2021.
[208] Case C-311/18, *Schrems II*, para. 135.

Standart sözleşme maddeleri GDPR m.46(2)(c) ve m.46(2)(d)'de düzenlenmiştir. GDPR m.46(2)(c)'de yer alan standart sözleşme maddeleri Komisyon tarafından kabul edilen ve ilan edilen maddelerdir. GDPR m.46(2)(d)'de yer alan standart sözleşme maddeleri ise 95/46 sayılı Direktifte yer almayan ve GDPR'ın sunduğu yeni sözleşme maddeleridir. GDPR m.46(2)(d)'de yer alan standart sözleşme maddeleri ulusal denetim makamı tarafından kabul edilir ve Komisyon tarafından onaylanır. Ancak ulusal denetim makamı tarafından hazırlanan m.46(2)(d)'de yer alan standart sözleşme maddelerinin kabul edilebilmesi için EDPB'nin görüşü aranır[209]. GDPR'ın ulusal denetim makamlarına standart sözleşme maddelerini kabul etme yetkisi vermesi ulusal denetim makamlarının yetkisini genişleten bir uygulama olarak görülebilir.

Tablo 2.1 Standart Sözleşme Maddelerinin Özellikleri

İlgili Madde	**Yasal Dayanak**	**Kullanımı**	**Onay**	**Güncel Durum**
GDPR m.46(2)(c)	Komisyon tarafından kabul edilen ve yayınlanan standart sözleşme maddeleri	Komisyonun hazırlamış ve yayınlamış olduğu standart sözleşme maddeleridir. Bu maddeler, veri aktarımı sözleşmelerine değiştirilmeden eklenir.	Spesifik veri aktarımına yönelik otorite onayı aranmamaktadır.	Komisyon tarafından, 4 Haziran 2021 tarihinde yayınlanan yeni standart sözleşme maddesi bulunmaktadır.

[209] GDPR m.64(1)(e).

GDPR m.46(2)(d)	Denetim Makamı tarafından kabul edilen ve Komisyon tarafından onaylanan standart sözleşme maddeleri	İlgili ülkenin ulusal denetim makamı tarafından hazırlanır ve Komisyon tarafından onaylanır.	Spesifik veri aktarıma yönelik otorite onayı aranmamaktadır. Standart sözleşme maddelerinin denetim makamı tarafından kabul edilebilmesi için EDPB'nin görüşü aranır.	Hâlihazırda bir denetim makamı tarafından yayınlanan standart sözleşme maddeleri bulunmamaktadır.

Her iki madde de belirtilen standart sözleşme maddeleri GDPR m.93(2)[210]'de atıfta bulunulan inceleme usulüne tabidir. Ayrıca m.46(2) hükmü uyarınca standart sözleşme maddeleri kapsamındaki aktarımlar için ulusal denetim makamlarından özel bir izin alınmasına gerek olmamaktadır. Böylece GDPR, Direktifte bulunan ve bazı AB ülkelerinde geçerli olan bildirimde bulunma ve yetkilendirme yükümlülüklerini geçersiz kılarak uluslararası veri aktarımları için prosedürleri sadeleştirmiş ve bürokrasiyi azaltmıştır.

Model maddeler *(model contract clauses)* olarak da bilinen standart sözleşme maddeleri AB genelinde kişisel veri aktarımlarında kullanılan en yaygın ve etkili uygun güvence yöntemidir. Nitekim GDPR m.28(6)'da, veri sorumlusu ve veri işleyenler arasındaki işleme faaliyetine ilişkin düzenlenen bir sözleşmenin "tamamen veya kısmen" Komisyon veya yerel denetim makamı tarafından kabul edilen standart sözleşme maddelerine dayanabileceğinin ifade edilmesi, standart

[210] AB 182/2011 sayılı Tüzük m.5.

sözleşme maddelerinin veri aktarımında model alınması gereken bir araç olduğunu göstermektedir[211].

Standart sözleşme maddeleri yönteminde, kişisel verileri AB'den aktaran ile AB dışında verileri alan arasında standart sözleşme maddelerinin yer aldığı bir sözleşme imzalanır. Söz konusu sözleşmede tarafların sözleşmeden kaynaklanan yükümlülükleri ve ilgili kişinin hakları yer almalıdır. İlgili kişiler, veri aktaran ve veri aktarılandan bu hakları için talepte bulunabilmektedir. Ayrıca, standart sözleşme maddeleri kullanılarak yapılan aktarımlarda, veri aktarılan bir uyuşmazlık olması durumunda veri aktaranın tabi olduğu mahkemelere ve yerel denetim makamına uymayı kabul etmelidir[212].

95/46 sayılı Direktif doğrultusunda Komisyon tarafından kabul edilen, veri sorumlusundan veri sorumlusuna aktarımlar için iki set[213], veri sorumlusundan veri işleyenlere yapılan aktarımlar için bir set standart sözleşme maddesi mevcuttu[214]. Komisyon 2016 yılında, ABAD'ın Schrems I kararına istinaden, 2001 yılında onaylanan veri sorumlusundan veri sorumlusuna ve 2010 yılında onaylanan veri sorumlusundan veri işleyene sözleşme maddelerinde değişiklik yapılması kararı aldı[215].

---

[211] Theodorakis, s.29.

[212] Giakoumopoulos, Buttarelli ve O'Flaherty, *Handbook on European Data Protection Law*, s.252.

[213] European Commission, "Commission Decision 2001/497/EC of 15 June 2001 on standard contractual clauses for the transfer of personal data to third countries, under Directive 95/46", OJ 2001 / L 181; European Commission, "Commission Decision 2004/915/EC of 27 December 2004 amending Decision 2001/497/EC as regards the introduction of an alternative set of standard contractual clauses for the transfer of personal data to third countries", OJ 2004 / L 385; 2004 yılında kabul edilen veri sorumlusundan veri sorumlusuna standart sözleşme maddeleri, 2001'de kabul edilenlere ilaveten kullanıldı, böylece veri sorumlusundan veri sorumlusuna standart sözleşme maddeleri için kullanılabilir iki standart sözleşme maddeleri oluştu.

[214] European Commission, "Commission Decision 2010/87 of 5 February 2010 on standard contractual clauses for the transfer of personal data to processors established in third countries under Directive 95/46 of the European Parliament and of the Council", OJ 2010/ L 39.

[215] Commission Implementing Decision (EU) 2016/2297 of 16 December 2016 amending Decisions 2001/497/EC and 2010/87/EU on standard contractual clauses for the transfer of personal data to third countries and to processors established in such countries, under Directive 95/46 of the European Parliament and of the Council, OJ 2016/ L344 2016 yılında yapılan değişiklik, her iki grubun 4. maddelerini aşağıdaki şekilde değiştirmiştir;

"*(...)Üye Devlet yetkili makamı, kişisel verilerin işlenmesi kapsamında bireyleri korumak için üçüncü ülkelere veri aktarımını durdurma veya yasaklamaya yönelik yetkisini kullandığında, söz*

GDPR yürürlüğe girdikten sonra ise, Komisyon 4 Haziran 2021 tarihinde GDPR m.46(2)(c) uyarınca AB'de bulunan veri sorumluları veya veri işleyenlerden AB dışında bulunan veri sorumluları veya veri işleyenlere veri aktarımları için, 95/46 sayılı Direktif kapsamında kullanılan bu üç standart sözleşme maddelerinin yerini alacak, modernize edilmiş iki standart sözleşme maddeleri seti yayınladı[216].

GDPR Gerekçe 106'ya göre Komisyonun onayladığı standart sözleşme maddelerinin, yeterlilik kararlarında olduğu gibi düzenli olarak gözden geçirilmesi gerekmektedir. GDPR m.46(5)'de, 95/46 Sayılı Direktif m.26(2) hükmüne dayalı olarak bir üye devlet veya denetim makamı tarafından verilen yetkilerin, gerektiği durumda söz konusu denetim makamı tarafından değiştirilene, yenilenene veya yürürlükten kaldırılana kadar geçerliliğini koruyacağı belirtilmiştir. Aynı madde de devamla, Komisyonu'nun 95/46 sayılı Direktif m.26(4) kapsamında kabul ettiği kararların, yine Komisyon kararı ile değiştirilene, yenilenene veya yürürlükten kaldırılana kadar geçerli olduğu yer almaktadır. Nitekim 4 Haziran 2021 tarihinde Komisyon almış olduğu karar ile Direktif kapsamında kabul edilen üç standart sözleşme maddesi setinin yerini alacak iki yeni standart sözleşme maddesi setini yayınlamıştır.

Komisyon onaylı standart sözleşme maddeleri, eklerin doldurulması dışında üzerinde bir değişiklik yapılmadan aynen kullanılmalıdır. Bununla birlikte uygulamada, standart sözleşme maddelerinde bir değişiklik yapılırsa, bu değişiklik söz konusu standart sözleşme maddelerinin ulusal denetim makamının onayını gerektiren özel (ad hoc) maddeler olarak kabul edileceği anlamına gelir[217]. Ancak GDPR Gerekçe 109, sözleşme maddelerine ihtiyaçlar doğrultusunda asıl maddelerle ters düşmemek şartıyla ve ilgili kişilerin temel hak ve özgürlüklerini

---

konusu üye devlet, diğer üye ülkeleri bu konuda bilgilendirecek olan Komisyona bu bilgileri gecikmeksizin iletecektir"
Ancak bu değişiklik, 2004 yılında onaylanan veri sorumlusundan veri sorumlusuna olan sözleşme maddelerini (Komisyon Kararı 2004/915) kapsamamaktadır.

[216] Bkz. https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/standard-contractual-clauses-scc_en, Erişim Tarihi: 20.10.2021.

[217] Kuner, Bygrave ve Docksey, *GDPR: A Commentary*, s.806.

engellemeyecek şekilde ilgili taraflar tarafından ek maddeler veya ilave önlemler eklenebileceğini ve veri sorumluları ve veri işleyenlerin de bu yönde desteklenebileceğini düzenler. Pratikte de söz konusu ilave önlemlerin bu şartlar ile uyumsuz olmasının pek mümkün olmadığı, aksine bireylerin özgürlüklerini daha fazla koruyan ve standart sözleşme maddeleriyle ters düşmeyen bir uygulama ortaya çıkardığı da görülmektedir[218]. Özellikle verilerin hassasiyeti açısından yüksek bir riskin bulunduğu ve ayrıntılı veri güvenliği gereksinimlerinin olduğu durumlarda ek maddeler önem taşımaktadır[219]. Zira bu durumda ek maddeler, daha etkili bir uygun güvence sağlanmasına olanak tanır.

2.2.3.1 Schrems II Kararının Standart Sözleşme Maddelerine Etkisi

ABAD'ın Schrems II kararı bir veri aktarım mekanizması olan standart sözleşme maddelerinin yeterli koruma sağladığını onaylayan ilk karar olmuştur[220]. Öyle ki, kararın 148. Paragrafında standart sözleşme maddelerinin uygulamada, kararın ekinde yer alan standart sözleşme maddeleri uyarınca veri aktarılan tarafın bu maddelere uymadığı veya uyamadığı durumlarda üçüncü bir ülkeye kişisel veri aktarımının askıya alınmasını veya yasaklanmasını sağlayan etkili bir mekanizma olduğu belirtilmiştir. Ayrıca Schrems II kararında ABAD'ın tespitine göre, AB Hukukunun uygulanabilirliği Şart'ın uygulanabilirliğini gerektirdiği için GDPR m.46'da yer alan uygun güvencelere istinaden yapılan veri aktarımlarının Şart ışığında yorumlanması ve koruma düzeyine ilişkin standartların Şart'a dayanarak belirlenmesi gerekmektedir[221]. ABAD bu şartlar dâhilinde standart sözleşme maddelerini veri aktarım mekanizması olarak tek başına kullanılmasını onaylamıştır[222]. Mahkeme, Komisyon tarafından kabul edilen standart sözleşme maddelerinin AB'de yerleşik veri sorumlusu veya veri işleyenlere, tüm üçüncü ülkelerde her bir üçüncü ülkede sözleşmeye dayalı olarak garanti edilen koruma

[218] Theodorakis, s.29.
[219] EDPB, "Recommendations 01/2020", s.15 dn. 42.
[220] Kuner, Bygrave ve Docksey, *GDPR: Update of Selected Articles*, s.171-172.
[221] Case C-311/18, *Schrems II*, para. 99.
[222] Case C-311/18, *Schrems II*, para. 136.

seviyesinden bağımsız olarak aynı şekilde uygulanan garantiler sağlamayı amaçladığının altını çizmiştir[223].

Yalnızca belirli aktarım çeşitlerine uyarlanan bir veri aktarım mekanizması olan uygun güvenceler, bir diğer veri aktarım mekanizması olan yeterlilik kararına göre daha dar kapsamlıdır. Ancak ABAD Schrems II kararında, yeterlilik kararları için geçerli olan AB Hukukunda garanti edilene esasen eşdeğer düzeyde bir korumanın standart sözleşme maddelerine dayanarak yapılan aktarımlar için de geçerli olduğuna karar vermiştir[224]. Söz konusu kararda ABAD, m.46 kapsamındaki uygun güvencelere ilişkin dikkate alınması gereken kriterlerin m.45(2) kapsamındaki yeterlilik kararını belirlemede dikkate alınması gereken kriterler ile aynı olduğuna karar vermiştir[225]. Bu karar, Schrems II'nin GDPR kapsamında uluslararası veri aktarımlarına ilişkin gündeme getirdiği en önemli sonuçlardan birisidir. ABAD'ın Schrems II kararının, GDPR'ın lafzına ve ulusal denetim makamlarının uzun süredir var olan uygulamasına rağmen bu iki veri aktarım mekanizması arasındaki hiyerarşiyi görmezden geldiği şeklinde yorumlanmıştır[226]. Ayrıca ABAD'ın Schrems II kararının, sadece standart sözleşme maddeleri için değil, GDPR m.46(2)'de yer alan tüm uygun güvenceler için de geçerli olduğu da EDPB'nin kılavuzunda belirtilmiştir[227].

Schrems II kararında ABAD, standart sözleşme maddelerinin bir veri aktarım aracı olarak geçerliliğini onaylamıştır[228]. Bu bağlamda ABAD standart sözleşme maddelerinin geçerli bir veri aktarım mekanizması olarak kalabilmesi için, veri aktaranların üçüncü ülkelerde AB Hukuku ile esasen eşdeğer standartta bir veri koruma düzeyinin sağlanmasına ilişkin boşlukları giderebilmek adına uygun

[223] Case C-311/18, *Schrems II*, para. 133.
[224] Case C-311/18, *Schrems II*, para. 96.
[225] Case C-311/18, *Schrems II*, para. 104.
[226]Christopher Kuner, "Schrems II Re-Examined", 25.10.2020, https://verfassungsblog.de/schrems-ii-re-examined/, Erişim Tarihi: 19.10.2021.
[227] EDPB, " Recommendations 01/2020", s. 24.
[228] Case C-311/18, *Schrems II*, para. 136.

güvenceler sağlaması ve bu çerçevede gerekli olduğunda "ek önlemler" uygulaması gerektiğinin altını çizmiştir[229].

ABAD Schrems II davasında yapmış olduğu tespitte, standart sözleşme maddelerinin sözleşmeye dayalı olmaları sebebiyle sözleşmeye taraf olmayan üçüncü ülkelerdeki kamu makamları açısından bağlayıcı olmadığını ve bu kapsamda standart sözleşme maddeleri yoluyla yapılan aktarımlarda üçüncü ülkelerin kamu yetkililerinin kişisel verilere erişmesine engel olunamadığını belirtmiştir. Bu bağlamda ABAD, üçüncü ülkelerin yetkili makamların kişisel verilere ulaşmasına karşı koruma sağlamak için tarafların standart sözleşme maddeleri kapsamında sağlanan güvencelere ilave olarak "ek güvenceler" sağlamaları gerektiğine karar vermiş[230] ve bu noktada GDPR Gerekçe 109'a atıfta bulunmuştur[231]. Ayrıca ne GDPR'da, ne de Schrems II kararında ABAD ek güvenceleri tanımlamamış veya bu güvencelerin nasıl alınabileceğine dair detaylı bilgi vermemiştir. Ek güvenceler ile ilgili ayrıntılar, EDPB'nin veri aktaran olarak hareket eden veri sorumlusu ve veri işleyenlerin almaları gereken ek güvenceleri belirlemek için izleyebilecekleri sürece ilişkin tavsiyelerde bulunmak adına yayınladığı kılavuzunda yer almıştır[232]. Anılan belgeye göre EDPB'nin örnek olarak belirlediği başlıca ek güvenceler; şifreleme, takma isim kullanma ve veri işlemenin birden fazla yerde veya tarafça gerçekleştirilmesi gibi teknik önlemler; teknik önlemlerin uygulanma taahhütleri, kamu yetkililerinin verilere erişimine dair şeffaflık raporu ve belgelerin yayınlanması ve ileriye yönelik aktarımlar yapılmasının yasaklanması gibi sözleşmesel önlemler ve iç politikaların benimsenmesi ve veri erişim taleplerinin belgelenmesi gibi organizasyonel önlemlerdir. Ayrıca, EDPS, AB kurumlarının, organlarının, ofislerinin ve ajanslarının Schrems II kararına uyumunu sağlamayı ve izlemeyi amaçlayan bir belge yayınlamıştır[233].

---

[229] Case C-311/18, *Schrems II*, para. 103, 133, 134.
[230] Case C-311/18, *Schrems II*, para. 134; EDPB,"Recommendations 01/2020", s.8.
[231] EDPB, "Recommendations 01/2020", s.8; C-311/18, *Schrems II*, para 132 -133.
[232] EDPB, "Recommendations 01/2020", s.28.
[233] Bkz.European Data Protection Supervisor (EDPS) ,"Strategy for Union Institutions, Offices, Bodies and Agencies to Comply with the Schrems II Ruling", 29.10.2020,

ABAD Schrems II davasında, veri aktaran konumunda olan veri sorumlusu ve işleyenlere standart sözleşme maddeleriyle yapılan kişisel veri aktarımlarında üçüncü ülkelerde AB Hukukuna esasen eşdeğer standartta bir koruma sağlamayı birincil sorumluluk olarak yüklemiştir. Bu noktada ABAD, GDPR m.5(2)'de yer alan hesap verebilirlik ilkesini bir veri işleme biçimi olan üçüncü ülkelere veri aktarımlarına da uygulamıştır[234]. Mahkeme'ye göre, hesap verebilirlik ilkesinin gereği olarak, standart sözleşme maddeleri ile verileri aktaran, veri aktarılan ile işbirliği içerisinde gerektiğinde bu maddeler tarafından sunulanlara ek önlemler alarak ilgili üçüncü ülke yasalarının AB yasalarına nazaran yeterli koruma sağlayıp sağlamadığını[235] ve aktarımdan önce AB yasalarının sağladığı koruma düzeyine üçüncü ülkede uyulup uyulmadığını vaka bazında doğrulaması gerekmektedir[236].

Bu bağlamda ABAD, AB'de yerleşik bir veri sorumlusu veya veri işleyenin bu tür bir korumayı garanti altına almak için yeterli ilave önlemleri alamaması durumunda ilgili veri sorumlusunun veya işleyenin veya bunun olmaması durumunda ulusal denetim makamının verilerin üçüncü ülkelere aktarımını askıya alması veya sona erdirmesi gerektiğini belirtmiştir[237]. Bununla bağlantılı olarak ABAD, standart sözleşme maddelerinin Komisyon tarafından onaylanmasının, Komisyona ulusal denetim makamlarının GDPR m.58(2) kapsamındaki yetkilerine sınırlama yetkisi vermediğini ve böylece bir ulusal denetim makamının AB ve yerel yasaların ihlal edildiğini belirlemesi durumunda, veri aktarımlarını askıya alabileceğini ve yasaklayabileceğini belirtmiştir[238].

ABAD Schrems II kararında, Schrems I kararında belirtilen uygun güvencelerin uygulanmasıyla ilgili ilkeleri onaylamıştır[239]. Bu çerçevede ABAD, geçerli bir

https://edps.europa.eu/data-protection/our-work/publications/papers/strategy-union-institutions-offices-bodies-and_en, Erişim Tarihi: 23.10.2021.

[234] EDPB, "Recommendations 01/2020", s.10.

[235] Case C-311/18, *Schrems II*, para. 134.

[236] Case C-311/18, *Schrems II*, para. 142.

[237] Case C-311/18, *Schrems II, para*. 135.

[238] Case C-311/18, *Schrems II*, para. 115.

[239] Kuner, Bygrave ve Docksey, *GDPR: Update of Selected Articles*, s.181.

yeterlilik kararı mevcut olmadıkça, ulusal denetim makamının, söz konusu üçüncü ülkede bu maddelere uyulmadığı veya uyulamadığı, AB Hukukunun özellikle GDPR m.45, m.46 ve Şart'ın gerekli kıldığı aktarılan verilere ilişkin korumanın başka yolla sağlanamadığı ve veri sorumlusu veya veri işleyenin aktarımı askıya almadığı veya son vermediği durumlarda kendi görüşü ile ve aktarımın tüm koşullarını dikkate alarak standart sözleşme maddeleri kapsamında yapılan veri aktarımını askıya alması veya sona erdirmesi gerektiğini belirtir[240]. İlaveten, mevcut bir yeterlilik kararı bulunsa bile, bir kişi şikâyette bulunursa ulusal denetim makamı aktarımın GDPR gerekliliklerine uygun olup olmadığını inceleyebilmeli ve yeterlilik kararının geçerliliğine ilişkin şüpheleri olması halinde buna ilişkin bir ön karar için ulusal mahkemelere dava açabilmelidir[241].

2.2.3.2 Schrems II Kararı Sonrası Modernize Edilmiş Standart Sözleşme Maddeleri

Komisyon, 4 Haziran 2021 tarihinde, GDPR'ın gerekliliklerini içeren ve ABAD'ın Schrems II kararındaki yasal değerlendirmeyi dikkate alan iki yeni güncellenmiş standart sözleşme maddesi seti yayınladı[242]. Bu setlerden birincisi GDPR m.28(7) ve m.29(7) kapsamında, uluslararası aktarımları kapsamayan ve AB içindeki veri sorumluları ve veri işleyenler arasında kullanılmak üzere düzenlenmiştir[243]. İkinci standart sözleşme maddeleri seti ise GDPR m.46 kapsamında kişisel verilerin üçüncü ülkelere aktarılmasında uygun güvence sağlamak amacıyla oluşturulan standart sözleşme maddeleridir[244]. Modernize edilmiş bu yeni standart sözleşme maddeleri mevcut olan üç standart sözleşme maddesinin yerini almıştır.

---

[240] Case C-311/18, *Schrems II*, para. 121.
[241] Case C-311/18, *Schrems II*, para. 120.
[242] Bkz. European Commission (EC), "Standard Contractual Clauses for controllers and processors in the EU" 4 June 2021, https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/standard-contractual-clauses-scc_en, Erişim Tarihi: 21.10.2021.
[243] European Commission, "Standard Contractual Clause".
[244] Bkz. 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, https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/standard-contractual-clauses-scc/standard-contractual-clauses-international-transfers_en, Erişim Tarihi: 21.10.2021.

95/46 sayılı Direktif hükümlerine göre 2000'li yılların başında oluşturulmaya başlanan mevcut standart sözleşme maddeleri, 2018 yılında Direktif yerine yürürlüğe giren GDPR'ın getirdiği birçok yenilik ve değişikliği içermiyordu. Öte yandan, ABAD Schrems II kararında üçüncü ülke yasalarının aktarılan verilerin koruma düzeyini zayıflatabileceği ve kamu yetkililerinin aktarılan kişisel verilere yetkisiz erişebileceğini ifade etmiş ve buna bağlı olarak standart sözleşme maddelerinin GDPR tarafından sağlanan korumaya eşdeğer bir koruma düzeyi sağlamak için ilave önlemler içermesi gerektiğini belirtmiştir. Bu durum GDPR'ın getirdiği yeniliklerle birlikte mevcut standart sözleşme maddelerinin güncellenmesi ihtiyacını doğurmuştur. Yeni standart sözleşme maddeleri, mevcut olanlara göre önemli derecede geliştirilmiş güvenlik önlemleri, bildirim, raporlama ve kayıt yükümlülükleri gerektirmektedir.

Mevcut standart sözleşme maddeleri 27 Eylül 2021 tarihinde yürürlükten kaldırılmış olup bu tarihten sonra imzalanan veri aktarımına ilişkin sözleşmelerin yeni standart sözleşme maddelerine göre düzenlenmesi gerekmektedir. 27 Eylül 2021 tarihinden önce mevcut standart sözleşme maddeleri kullanılarak imzalanan sözleşmelerin ise sözleşme konusu işleme faaliyetlerinin değişmemesi şartı ile 15 ay boyunca (27 Aralık 2022'ye kadar) uygun güvence sağladığı kabul edilmektedir[245].

Yeni standart sözleşme maddeleri, mevcut standart sözleşme maddelerinde olan bazı hususları aynı şekilde içermeye devam etmektedir. Bunlar, yeterli düzeyde veri koruması sağlamak için GDPR'ın gerekliliklerine uymayı taahhüt etmesi, içerdiği standart maddelerin taraflar tarafından değiştirilememesi ve tarafların belirli veri aktarımlarına göre eklerini güncellemesi gerektiğidir. Ayrıca, mevcut olanlarda olduğu gibi yeni standart sözleşme maddelerine, standart maddelerle çelişmediği sürece ilave maddeler eklenebilir. Mevcut gereksinimlerin yanında şeffaflık, ilgili kişi hakları, veri ihlalleri gibi ilkeler GDPR ilkeleriyle uyumluluk adına yeni

[245] Bkz. https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/standard-contractual-clauses-scc_en, Erişim Tarihi: 21.10.2021.

standart sözleşme maddelerinin getirdiği önemli yeniliklerdir. Mevcut standart sözleşme maddeleri kısıtlı veri aktarımı sunmasına karşın yeni standart sözleşme maddeleri, oluşturulan yeni modüler (*modular*) yapısı sayesinde daha fazla esneklik sağlamaktadır[246]. Bu yapı sayesinde veri aktaranlar ve veri aktarılanlar aynı sözleşme ile ihtiyaçlarına en uygun olan seçeneği seçebilirler[247]. Bu modüller veri sorumlusundan veri sorumlusuna veya veri işleyene ve veri işleyenden veri işleyene veya veri sorumlusuna yapılan aktarımlar için olmak üzere dört tanedir. Mevcut standart sözleşme maddeleri ise sadece veri sorumlusundan veri sorumlusuna veya veri işleyene yapılan aktarımları kapsamaktaydı. AB'de yer alan ve veri işleyen konumunda olan bir bulut hizmet sağlayıcısının üçüncü ülkedeki bu hizmet sağlayıcısına alt yapı hizmeti sunan başka bir veri işleyene veri aktarması, veri işleyenden veri işleyene aktarıma örnek olarak verilebilir. Veri işleyenden veri sorumlusuna aktarım durumunda ise veriler veri sorumlusuna geri aktarılmış (aslına geri dönüş) olur ve bu ters aktarım olarak isimlendirilir[248].

Mevcut standart sözleşme maddeleri sadece AB içerisinde kurulu veri aktaranın sözleşmeye taraf olmasını içerirken, yeni standart sözleşme maddelerine göre veri aktaran AB dışında da yerleşik olabilir. Bu uygulama, modüler yapı ile birlikte yerleşik olduğu yere ve veri işleme rolüne bakılmaksızın veri aktaran ve veri aktarılan arasında her türlü verinin aktarılmasına imkân tanır[249].

---

[246] Philip Gordon, Zoe Argento ve Kwabena Appenteng, "The European Union's New Standardized Data Transfer Agreement: Implications for Multinational Employers", 9 June 2021, https://www.littler.com/publication-press/publication/european-unions-new-standardized-data-transfer-agreement-implications, Erişim Tarihi: 30.11.2021.

[247] Marcelo Corrales Compagnucci, Mateo Aboy, Timo Minssen, "Cross-Border Transfers of Personal Data after Schrems II: Supplementary Measures and New Standard Contractual Clauses (SCCs)", October 27, 2021, s.8, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3951085, Erişim Tarihi: 30.11.2021.

[248] Compagnucci, Aboy ve Minssen, "Cross-Border Transfers", s.8.

[249] Phillip Lee, "The Updated Standard Contractual Clauses:A New Hope?", June 7, 2021, https://iapp.org/news/a/the-updated-standard-contractual-clauses-a-new-hope/, Erişim Tarihi: 30.11.2021.

Tablo 2.2 Eski ve Yeni Standart Sözleşme Maddeleri Karşılaştırması

Standart Sözleşme Maddeleri	**Aktarım Modülü**	**Sözleşme Tarafları**	**İlave Önlem**
Eski Standart Sözleşme Maddeleri	• Veri sorumlusundan veri işleyene • Veri sorumlusundan veri sorumlusuna	• Sadece AB içerisinde yerleşik veri aktaran sözleşmeye taraf olabilir	Gerektirmez.
Yeni Standart Sözleşme Maddeleri	• Veri sorumlusundan veri işleyene • Veri sorumlusundan veri sorumlusunda • Veri işleyenden veri sorumlusuna • Veri işleyenden veri işleyene	• AB dışında yerleşik veri aktaran da sözleşmeye taraf olabilir. • Veri aktarılan, AB denetim makamlarına tabidir.	Teknik, organizasyonel ve sözleşmeye dayalı önlemler gerektirir.

Yeni standart sözleşme maddelerinde, şirket grupları veya ortak işbirliği içinde yer alan birden fazla veri aktaran tarafın sözleşme yapması ve "yerleştirme maddesi"ne (*docking clause*) istinaden zaman içinde sözleşmeye yeni tarafların eklenmesi

imkânı bulunmaktadır[250]. İsteğe bağlı olan bu madde, veri aktaran üçüncü tarafların ayrı bir sözleşme yapmadan mevcut sözleşmeye katılmasına izin verir. Üçüncü taraflar, aktarımın ayrıntılarının, uygulanan teknik ve organizasyonel tedbirlerin ve alt işleyenlerin listesinin olduğu ilgili ekleri de imzalayarak sözleşmeye dâhil olabilirler. Bu yeni sistemin, mevcut veri işleme uygulamaları için özellikle satın almalar, alt işleyenler ve ilave kurumsal varlıklar bağlamında daha çok esneklik ve kolaylık sağlayacağı düşünülmektedir[251].

ABAD'ın Schrems II kararının doğurduğu ihtiyaç neticesinde yeni standart sözleşme maddelerinde, kararda yer alan endişeleri karşılayan iki hüküm bulunmaktadır. Bunlardan ilki, veri aktarılan, yerel kanunların standart sözleşme maddelerinin sağladığı koruma düzeyini zayıflatmadığını garanti etmeli ve bu garantiyi desteklemek için yerel kanun değerlendirmesini belgelemelidir. Ayrıca veri aktarılan taraf, talep üzerine bu belgeleri ilgili AB veri koruma makamlarına iletmeli ve ilave önlemler aldıklarını belirtmelidir. İkinci hüküm ise, standart sözleşme maddelerinin veri aktarılanın söz konusu kişisel verilere ilişkin hükümetin erişim taleplerini dava etmesini aramasıdır. Ayrıca, veri aktarılan yasal olarak izin verildiği durumlarda, veri aktaranı ve mümkünse ilgili kişiyi söz konusu erişim talebine ilişkin bilgilendirmelidir.

Schrems II kararının bir diğer sonucu olarak yeni standart sözleşme maddeleri, şirketlerin veri aktarımı etki değerlendirmesini içeren "Veri Koruma Etki Değerlendirmesi" yapmasını ve bu değerlendirmeyi belgelendirerek talebe istinaden ulusal denetim makamına sunmasını gerektirir. Veri aktarımı etki değerlendirmesi, verilerin aktarıldığı üçüncü ülkenin yasalarının GDPR ve standart

[250] "Commission Implementing Decision (EU) 2021/914 of 4 June 2021", Annex, Section I, https://eur-lex.europa.eu/eli/dec_impl/2021/914/oj?uri=CELEX%3A32021D0914&locale=en, Erişim Tarihi: 30.11.2021.

[251] Martin Braun and others, "European Commission adopts and publishes new Standard Contractual Clauses for international transfers of personal data", 7 June 2021, https://www.wilmerhale.com/en/insights/blogs/wilmerhale-privacy-and-cybersecurity-law/20210607-european-commission-adopts-and-publishes-new-standard-contractual-clauses-for-international-transfers-of-personal-data Erişim Tarihi: 30.11.2021.

sözleşme maddeleri ile çelişip çelişmediğini ve veri koruması için ilave önlemin gerekli olup olmadığını içermelidir. Örnek verecek olursak, bu değerlendirme veri aktarılanın FISA 702'ye tabi olup olmadığını belirlemelidir[252]. Söz konusu değerlendirme devamlı olarak takip edilmeli ve üçüncü ülke yasalarında değişiklik olduğu takdirde bu değişikliğe istinaden revize edilmelidir[253].

Yeni standart sözleşme maddelerinin ekleri de mevcut olanların eklerinden daha fazla detay içermektedir. Kişisel verileri saklama süreleri, özel nitelikli kişisel veriler için ilave korumaların tanımlanması, veri aktarılan tarafından alınan teknik ve idarî önlemlerin ayrıntılı olarak açıklanması bu detaylara örnek olarak verilebilir. Bu detayların fazla olması nedeniyle, standart sözleşme maddeleri eklerinin hazırlanması için daha uzun bir zamana ihtiyaç duyulacağı açıktır.

Yeni standart sözleşme maddeleri birtakım güvenlik önlemleri içerir. Yeni standart sözleşme maddeleri EK II'de, verilerin güvenliğini sağlamaya ilişkin tedbirlerde dâhil olmak üzere, uygun bir koruma seviyesi için gerekli teknik ve organizasyonel önlemlerin neler olabileceği ayrıntılı olarak yer almaktadır. Ek II'ye göre bu önlemler genel değil özel ifadelerle tanımlanmalıdır. Bu önlemler, işlemenin kapsamı, doğası, bağlamı ve amacı ile gerçek kişilerin hak ve özgürlüklerine yönelik riskler göz önünde bulundurularak uygun bir güvenlik seviyesi sağlamaya yöneliktir. En dikkat çeken ve önemli önlemler, takma ad kullanma ve şifreleme önlemleridir[254].

Yeni standart sözleşme maddeleri, veri aktarılanın bu maddeler kapsamındaki yükümlülüklerine uygunluğunu gösterebileceğini açıkça belirtmekte ayrıca veri aktarılana ulusal denetim makamının talebi üzerine söz konusu uygunluk belgelerini sağlama zorunluluğu getirmektedir. Mevcut standart sözleşme

[252] Compagnucci, Aboy ve Minssen, "Cross-Border Transfers", s. 9.
[253] Compagnucci, Aboy ve Minssen, "Cross-Border Transfers", s. 9.
[254] "Commission Implementing Decision (EU) 2021/914 of 4 June 2021", Annex, Section II, https://eur-lex.europa.eu/eli/dec_impl/2021/914/oj?uri=CELEX%3A32021D0914&locale=en, Erişim Tarihi: 30.11.2021, s.31.

maddelerinin aksine yeni standart sözleşme maddelerine göre veri aktarılanlar, AB denetim makamlarına tabidir ve ilgili kişiler veri aktarılan hakkında AB denetim makamları ve mahkemelerine şikâyette bulunabilecektir. Ayrıca veri aktarılanların, veri ihlallerini doğrudan AB denetim makamlarına bildirmeleri gerekmektedir.

Yeni standart sözleşme maddeleri veri aktaranlar ve özellikle veri sorumlusu konumunda olan veri aktarılanlar için, GDPR'ın gereklilikleri ile uyumlu olan daha fazla yükümlülük ve gereksinim bulundurmaktadır. Bu yükümlülükler arasında, ilgili kişilerin GDPR haklarını kullanma taleplerini karşılamak, aktarılma amaçları kapsamında ihtiyacı sona eren kişisel verileri silmek, üçüncü ülke makamlarının kişisel verilere erişim talebine ilişkin dava açmak, ilgili kişilere bildirimde bulunma ile veri ihlallerini AB makamlarına bildirme yükümlülüğü ve aktarılan veriler için teknik ve idarî ek önlemler alınması yer almaktadır. Muhtemelen veri aktarılanların bu yükümlülükleri gerçekleştirmek için kişisel veri koruma politikalarında değişiklik yapmaları gerekecektir[255].

Yeni standart sözleşme maddelerinin kullanımı ve yorumlanmasına ilişkin EDPB henüz bir rehber yayınlamamıştır. EDPB'nin yayınlayacağı rehberi ile yeni standart maddelerinin kullanımı ve uygun güvenceler için daha fazla pratik sağlanması mümkün olacaktır.

2.2.3.3 Schrems II Kararı Sonrası EDPB'nin Tavsiyeleri

ABAD'ın Schrems II kararının ardından EDPB, taslak hali 10 Kasım 2020 tarihinde[256] ve nihai hali 18 Haziran 2021 tarihinde[257] olmak üzere Schrems II kararındaki gereklilikler kapsamında, aktarılan kişisel verilerin AB düzeyinde

[255] Bkz. Gordon, Argento ve Appenteng, "The European Union's New Standardized Data Transfer".
[256] Bkz. https://edpb.europa.eu/our-work-tools/documents/public-consultations/2020/recommendations-012020-measures-supplement_en,
Erişim Tarihi: 21.11.2021.
[257] Bkz. https://edpb.europa.eu/our-work-tools/our-documents/recommendations/recommendations-012020-measures-supplement-transfer_en,
Erişim Tarihi: 21.11.2021.

korunmasını sağlamak için aktarım mekanizmalarını tamamlayan ilave önlemlere ilişkin tavsiyeler yayınlamıştır[258]. EDPB tavsiyelerine göre, tercih edilen aktarım mekanizması GDPR ve Şart kapsamında bireylerin temel hak ve özgürlüklerine eşdeğer düzeyde koruma sağlamak için bazı ilave önlemler içermelidir. Tavsiyeler ayrıca üçüncü ülkelerde kamu yetkililerinin kişisel verilere erişimine karşı önlem almak için dikkate değer bir rehberlik sunmaktadır.

EDPB'nin tavsiyelerinde, veri aktarımında AB yasalarının belirlediği koruma seviyesini temin etmenin veri aktaran ile birlikte veri aktarılanların da yükümlülüğü olduğu belirtilmektedir. Veri aktaranlar olarak veri sorumluları veya veri işleyenler, veri aktarılanlar ile verilerin korunmasını sağlamak için işbirliği içinde olmalı ve bu amaç doğrultusunda alınan önlemlerin etkisini takip etmelidir. EDPB söz konusu tavsiyelerde, kişisel verilerin yeterlilik kararı olmayan üçüncü ülkelere aktarılması kapsamında veri aktaran ve veri aktarılanın aktarımları değerlendirmeleri için altı adımlı sistemi takip etmelerini önermektedir. EDPB'nin nihai tavsiyeleri, belirli bir veri aktarımı için ilave önlemlerin gerekli olup olmadığını belirlemiştir. Veri aktaran tarafından izlenecek olan altı adımlı yol haritası aşağıda özetlenecektir;

Adım 1 – "Veri aktarımlarınızı bilin": Veri aktaranlar, ileriye yönelik aktarımlar da dâhil olmak üzere üçüncü ülkelere kişisel veri aktarımlarından haberdar olmalıdır. Bu kapsamda, hesap verebilirlik ilkesinin bir gereği olarak tüm işleme faaliyetleri verileri aktaranlar tarafından kaydedilmeli, veriler haritalanmalı, ilgili kişiler bilgilendirilmeli ve veri minimizasyonu ilkesine uyulmalıdır[259]. Nitekim veri aktarımlarını kaydetmek ve haritalamak zor olsa da verilerin işlendiği her yerde esasen eşdeğer bir koruma seviyesi sağlamak için bu kayıt işlemi bir gerekliliktir[260].

[258] Nihai tavsiyeler ile kamuoyu ile istişare için yayınlanan taslak tavsiyeler arasında en önemli fark, nihai tavsiyelerde veri aktaranların sadece üçüncü ülke yasalarını değil aynı zamanda üçüncü ülke kamu yetkililerinin gözetim uygulamalarının da gözden geçirmesi gerektiğini belirtmesidir.
[259] EDPB, "Recommendations 01/2020", s.8-9.
[260] Compagnucci, Aboy ve Minssen, "Cross-Border Transfers", s. 6.

Adım 2 – "Güvendiğiniz aktarım mekanizmasını belirleyin": Bu adımda, aktarım için GDPR 5. Bölümde yer alan uygun aktarım mekanizmasının belirlenmesi gerekmektedir. Üçüncü bir ülkeye yönelik yeterlilik kararı mevcutsa sonraki adımların uygulanmasına gerek yoktur. Ancak bir yeterlilik kararının mevcut olması ilgili kişinin şikâyet hakkını, denetim makamlarının mahkeme önünde dava açmasını ve ABAD'a başvurmasını engellemez[261]. Ayrıca, kişisel verilerin aktarımına GDPR m.49'da yer alan istisnalar yoluyla hükümde yer alan koşullar dikkate alınarak devam edilebilir. Yapılacak aktarım bir yeterlilik kararı veya istisnalar kapsamına girmiyorsa, GDPR m.46'da yer alan uygun güvenceler kapsamında aktarım için 3. adımdan devam edilmelidir[262].

Adım 3 – "Güvenmekte olduğunuz GDPR m.46 kapsamındaki uygun güvencenin aktarımın tüm koşulları ışığında etkili olup olmadığını değerlendirin": Veri aktaranların, ileriye dönük aktarımlarda dâhil olmak üzere, üçüncü ülkenin kamuya açık yasa, mevzuat ve/veya uygulamalarının m.46'da yer alan uygun güvencelerin etkinliğini etkileyip etkilemediğini değerlendirmek için veri aktarılan ile birlikte bir veri aktarım etki değerlendirmesi yapması gerekmektedir. Söz konusu değerlendirme, aktarılan verilerin korunmasına ilişkin üçüncü ülkede bulunan mevzuat ve uygulamaları, üçüncü ülke kamu makamlarının kişisel verilere erişip erişemeyeceği ve gözetim yasaları uygulamaları, GDPR m.45(2)'de yer alan yeterliliği değerlendirmede kullanılan kriterler ve üçüncü ülke hukuk sisteminin farklı yönleri (hukukun üstünlüğü, yasa dışı kişisel verilere erişime karşı bireylerin adli tazminat hakkı vb.) dikkate alınarak yapılmalıdır[263]. Ayrıca değerlendirmede kullanılacak kaynak ve bilgilerin tarafsız, güvenilir, doğrulanabilir ve kamuya açık olması ve talep edildiğinde denetim makamı veya adli makamlara sunmak üzere belgelenmesi gerekmektedir[264]. Değerlendirme sonucuna göre aktarım mekanizmasının etkili olduğunun belirlenmesi koruma seviyesinin AB'de

[261] EDPB, "Recommendations 01/2020", s.12.
[262] EDPB, "Recommendations 01/2020", s.13.
[263] Case C-311/18, Schrems II, para. 104; EDPB, "Recommendations 01/2020", s.15.
[264] EDPB, "Recommendations 01/2020", s.18-19.

sağlanana eşdeğer bir koruma seviyesi olduğunun göstergesidir[265].

Adım 4 – "İlave önlemlerin benimsenmesi": Veri aktarımı etki değerlendirmesine göre, GDPR m.46 aktarım mekanizmasının etkili olmadığı tespit edilirse, veri aktaranın veri aktarılan ile işbirliği içinde ilave önlemlere ihtiyaç olup olmadığını değerlendirmesi gerekir[266]. İlave önlemler, aktarım mekanizmasının sağladığı mevcut güvencelerin tamamlayıcısı anlamındadır[267]. İlave önlemler sözleşmeye dayalı, teknik veya organizasyonel nitelikte olabilir[268]. Bu önlemler, m.46'da yer alan güvencelere ilave edilirse, aktarılan veriler için üçüncü ülkede AB standardına esasen eşdeğer bir düzeyde koruma sağlanabilir. Hangi ilave önlemlerin etkili olabileceği ilk üç adımda yer alan değerlendirme dikkate alınarak duruma göre belirlenmelidir[269]. Ayrıca EDPB, veri aktaranın veri aktarılan ile işbirliği içinde, üçüncü ülkenin sorunlu mevzuatına istinaden kamu makamlarının erişim talep ettiği aktarılan verilerin korunmasında hangi ilave önlemleri alacağını belirlemesini etkileyecek kapsamlı olmayan bir liste belirlemiştir[270].

Adım 5 – "Resmi prosedür adımları": Alınacak ilave önlemler belirlendiğinde resmi prosedürlerin yerine getirilmesi gerekir. Standart sözleşme maddeleri için ilave önlemler alınacaksa, söz konusu ilave önlemler standart sözleşme maddeleri ile çelişmediği ve GDPR'ın garanti ettiği koruma düzeyinin zayıflatılmamasını sağlamak için yeterli olduğu takdirde ulusal denetim makamından onay alınmasına gerek yoktur[271].

6. Adım – "Uygun aralıklarla tekrar değerlendirme": Veri aktaranın veri aktarılan ile işbirliği içinde verilerin aktarıldığı üçüncü ülkede, üçüncü ülkenin koruma

[265] Case C-311/18, Schrems II, para. 105; EDPB, "Recommendations 01/2020", s.20.
[266] EDPB, "Recommendations 01/2020", s.21.
[267] GDPR Gerekçe 109; EDPB, "Recommendations 01/2020", s.21;Case C-311/18, Schrems II, para. 133.
[268] EDPB, "Recommendations 01/2020", s.28.
[269] EDPB, "Recommendations 01/2020", s.21.
[270] EDPB, "Recommendations 01/2020", s.22.
[271] EDPB, "Recommendations 01/2020", s.23-24.

düzeyine ilişkin ilk değerlendirme ile veri aktarım etki değerlendirmesinin ve özel aktarıma dayalı olarak alınan ilave önlemleri etkileyebilecek yeni gelişmeler olup olmadığının sürekli olarak takip edilmesi ve gözden geçirilmesi gerekir[272]. Bu durum ayrıca, GDPR m.5(2)'de yer alan hesap verebilirlik ilkesine uyumu göstermektedir. Alınan ilave önlemlerin üçüncü ülkede artık etkili olmaması, kuralların ihlal edilmesi veya artık yerine getirilmesi mümkün olmadığında, veri aktaranlar standart sözleşme maddelerine istinaden yapılan bir aktarımın askıya alınabilmesi veya yasaklanabilmesi için yeterli sistemler oluşturmalıdırlar[273].

Öte yandan EDPB'nin tavsiyelerinde dikkat çeken bazı önemli noktalar bulunmaktadır. Tavsiyelerde özellikle gözetim uygulamaları amacıyla üçüncü ülkelerdeki kamu makamlarının kişisel verilere erişiminin sadece uygun şekilde uygulanan teknik önlemler vasıtasıyla engellenebileceği veya etkisiz hale getirilebileceği ifade edilerek, tek başına yeterli olmayan sözleşmeye dayalı ve organizasyonel önlemlerin tamamlayıcısı olarak teknik önlemlerin kişisel verilere erişimi engelleyerek verilerin koruma seviyesini artıracağı belirtilmiştir[274]. Ayrıca bu önlemlerin tek başına değil birlikte uygulandığında etkili olacağı ifade edilmiştir[275].

Üçüncü ülkenin yasa ve uygulamaları sorunlu bir mevzuata sahipse, veri aktaran aktarımı askıya alabilir, ilave önlemler alabilir veya ilave önlemler almadan aktarıma devam edebilir. Ancak ilave önlemler almadan veri aktarımına devam etmek için, sorunlu mevzuatın, uygulama da ilgili veri aktarımına veya veri aktarılana uygulanmıyor olması şartı bulunmaktadır. Bu durumda sorunlu mevzuatın veri aktarımına veya veri aktarılana uygulanmayacağı ve veri aktarılanın m.46 kapsamındaki yükümlülüklerini yerine getirmesini engellemeyeceği, veri aktaran ve veri aktarılan işbirliği ile ayrıntılı bir rapor hazırlanarak

[272] EDPB, "Recommendations 01/2020", s.25.
[273] EDPB, "Recommendations 01/2020", s.25.
[274] EDPB, "Recommendations 01/2020", s.22.
[275] EDPB, "Recommendations 01/2020", s.22.

belgelendirilmesi gerekmektedir[276]. Bu belgelendirme hesap verebilirlik ilkesinin bir gereğidir.

Söz konusu tavsiyeler EDPB'nin vermiş olduğu bir görüş veya karar olmadığı gibi yasal olarak da bağlayıcı değildir. EDPB tavsiyeleri aktarımlar için dikkate alınacak önemli bir rehber niteliğindedir. EDPB'nin tavsiyelerine ilave olarak ulusal denetim makamlarının da yayınladığı rehberler olabilir. Nitekim Fransa ulusal denetim makamı (CNIL) tarafından AB dışına veri aktarımına ilişkin yayınlanan bir rehber bulunmaktadır[277].

2.2.4 Onaylı Davranış Kuralları ve Buna Bağlı İzleme Prosedürü

"Davranış Kuralları" *(Code of Conduct)*, 95/46 sayılı Direktifte sadece verilerin işlenmesi için yasal dayanak olarak düzenlenmiş olup uluslararası veri aktarımları için yasal dayanak olarak kullanılmamaktaydı. Ancak GDPR m.46(2)(e)'de, GDPR m.40 uyarınca onaylı davranış kuralları ile birlikte üçüncü ülkede bulunan veri sorumlusu veya veri işleyenin, ilgili kişilerin hakları da dâhil olmak üzere uygun güvenceler sağlamaya yönelik bağlayıcı ve uygulanabilir taahhütlerinin, kişisel verilerin üçüncü ülkelere veya uluslararası kuruluşlara aktarımı için yasal dayanak olarak kullanılabileceği düzenlenmiştir. GDPR'da davranış kuralları için bir tanım yapılmamıştır, fakat m.40'da davranış kurallarına ilişkin hükümler yer almaktadır. EDPB ise davranış kuralları ve izleme organları hakkında kılavuz ilkeler rehberi[278] ve davranış kuralları aktarım mekanizması kapsamında üçüncü ülkelere kişisel veri aktarımlarıyla ilgili GDPR m.40(3)'ün uygulanmasına yönelik rehber[279] yayınlamıştır.

---

[276] EDPB, "Recommendations 01/2020", s.17-18.
[277] Bkz. https://www.cnil.fr/fr/responsables-de-traitement-comment-identifier-et-traiter-des-transferts-de-donnees-hors-ue, Erişim Tarihi: 21.11.2021.
[278] Bkz. https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-12019-codes-conduct-and-monitoring-bodies-0_en, Erişim Tarihi: 21.11.2021.
[279] Bkz. EDPB, "Guidelines 04/2021 on codes of conduct as tools for transfers", 7 July 2021, https://edpb.europa.eu/system/files/2021-07/edpb_guidelinescodesconducttransfers_publicconsultation_en.pdf, Erişim Tarihi: 21.11.2021.

GDPR m.40(1)'de, GDPR'ın doğru olarak uygulanmasına katkı sağlaması amacı taşıyan davranış kurallarının hazırlanmasının üye devletler, denetim makamları, EDPB ve Komisyon tarafından teşvik edileceği açıkça belirtilmiştir. Bu ifadeden, davranış kurallarının GDPR açısından, veri koruma ilkelerinin uygulanmasında önemli bir yere sahip olduğu anlaşılmaktadır. Bu anlamda davranış kurallarının sadece veri aktarımları için oluşturulmadığı, GDPR'ın düzenli ve etkili bir şekilde uygulanabilmesi için en uygun uygulama yöntemlerini de içerdiği görülmektedir[280].

GDPR m.40(2)(j)'de kişisel verilerin üçüncü ülkelere veya uluslararası kuruluşlara aktarılmasına ilişkin davranış kurallarının, veri sorumluları veya veri işleyenleri temsil eden "birlikler" *(associations)* ve "diğer organlar" (*other bodies*) tarafından hazırlanabileceği, değiştirebileceği ya da kapsamının genişletebileceği yer almaktadır. Bu anlamda, davranış kuralları şirketleri temsil eden birlik ve diğer kuruluşlar tarafından oluşturulan ortak bir metindir.

GDPR m.40(3)'de, GDPR'a tabi olmayan veri sorumluları ve veri işleyenler tarafından da m.40(5) uyarınca onaylanan davranış kurallarına ve bu davranış kurallarının m.40(9) kapsamında genel geçerliliğe sahip olunması hususuna, m.46(2)(e)'de yer alan koşullar altında üçüncü ülkelere veya uluslararası kuruluşlara kişisel veri aktarımları için uygun güvenceler sağlanması amacıyla uyulabileceği yer almaktadır. Bu durumda, GDPR'a tabi olmayan veri sorumlusu veya işleyenlerin, söz konusu uygun güvenceleri uygulamak için sözleşme veya diğer bağlayıcı belgeler aracılığıyla ilgili kişilerin haklarını da içeren bağlayıcı ve uygulanabilir taahhütlerde bulunmaları gerekmektedir. Bu hüküm, üyeleri GDPR'a tabi olmayan fakat AB'de bulunan iş ortaklarının kendilerine veri aktarımlarını kolaylaştırmak isteyen üçüncü ülkedeki ticari birliklerin kullanımını kapsayabilir[281]. Veri sorumlusu ve veri işleyenler böyle bir davranış kuralını kabul ettiği takdirde, davranış kurallarının onaylanması için kabul etmek zorunda

[280] Baran Kızılırmak, "Cross-Border Transfer of Personal Data Under GDPR Regime and Turkish Legal Framework", Master Thesis, University Of Hamburg, Septermber 2020, s.35; Bulck,s.245.
[281] Kuner, Bygrave ve Docksey, *GDPR: A Commentary*, s.807.

oldukları GDPR kapsamındaki bağlayıcı ve uygulanabilir taahhütlere uymak durumunda olacaklardır[282].

İlgili birlikler veya diğer organlar, bir davranış kuralı hazırlamak, mevcut olanı güncellemek veya ekleme yapmak isterse GDPR m.55 uyarınca taslak davranış kuralını GDPR'da yer alan ilgili şartlara uygun olabilmesi için ulusal denetim makamının onaya sunar. Taslak davranış kurallarının tek bir AB ülkesinde veri işlemeyi kapsaması halinde ilgili denetim makamı söz konusu davranış kurallarının yeterli düzeyde uygun önlemleri içerip içermediğini ve GDPR'da bulunan şartlara uyup uymadığını değerlendirdikten sonra taslak davranış kurallarını onaylar, tescil eder ve yayımlar[283]. Denetim makamları, onayladığı davranış kurallarının yanında vermiş olduğu onay için dikkate aldığı kriterleri de yayınlar[284].

İlgili davranış kuralları birden çok AB üye ülkesinde kişisel veri işlemeyi kapsıyorsa, GDPR m.63'de yer alan prosedüre uygun olarak denetim makamı ilgili davranış kurallarını EDPB'ye sunar[285]. EDPB taslak davranış kurallarını kendi görüşüyle birlikte Komisyon'a sunar[286]. Komisyon, GDPR uygulama tasarrufları aracılığıyla, onaylı davranış kurallarının, değişikliklerinin veya kapsam genişletmelerinin, alacağı bir Komisyon Kararı ile Birlik içinde genel geçerliliğe sahip olduğuna karar verebilir ve uygun şekilde ilan edilmesini sağlar[287]. Komisyon onaylı davranış kurallarının AB içerisinde genel geçerliliğinin bulunduğuna dair uygulama tasarrufları ilan edebilir[288]. Fakat burada bahsedilen genel geçerliliğin yasal olarak ne ifade ettiği GDPR tarafından açıklanmamıştır[289]. EDPB, değişiklikler ve kapsam genişletmelerde dâhil onaylanmış tüm davranış kurallarını bir kayıtta toplar ve yayınlar[290].

---

[282] GDPR m.40(3).
[283] GDPR m.40(5)-40(6).
[284] Giakoumopoulos, Buttarelli ve O'Flaherty, *Handbook on European Data Protection Law*, s.182.
[285] GDPR m.40(7).
[286] GDPR m.40(8).
[287] GDPR m.40(9)-(10).
[288] GDPR m.40(9).
[289] Kuner, Bygrave ve Docksey, *GDPR: A Commentary*, s.807.
[290] GDPR m.40(11).

Onaylı davranış kuralları, GDPR m.41'de yer alan izleme prosedürüne tabidir. GDPR m.41(1)'e göre, davranış kuralları için taahhütte bulunan ve bu kurallara bağlı kalan veri sorumlusu ve veri işleyenlerin, bu bağlılıklarına ve taahhütlerine uyup uymadığını kontrol etmek, izlemek ve uyumu sağlamak için ilgili denetim makamının akredite ettiği özel bir organ atanabilir. Söz konusu organın bahsedilen görevlerini etkin olarak gerçekleştirebilmesi için, davranış kurallarına ilişkin konularda ispatlanmış uzmanlığa sahip olmak, bağımsız olmak, yerine getirdiği görevlerin çıkar çatışmasına sebep olmaması, kural ihlallerine ilişkin şikayetleri değerlendirecek şeffaf prosedür ve yapıya sahip olmak gibi kriterleri taşıması gerekmektedir[291]. GDPR m.41(3)'e göre ulusal denetim makamı, söz konusu organın akredite edilebilmesi için belirlediği taslak kriterleri görüş bildirmesi için EDPB'ye iletir.

Veri sorumluları ve veri işleyenlerin davranış kurallarına bağlı olması AB kanunlarına uygun hareket ettiğinin ispatı ve veri korumasına öncelik vermelerinin göstergesi olarak avantaj sağlar ve belirli sektörlerin hukuki gerekliliklere uyması ve veri işlemenin şeffaf şekilde yapılması için yol gösterici bir rehber olur[292].

2.2.5 Onaylı Sertifikasyon Mekanizmaları

GDPR m.46(2)(f)'de, GDPR m.42 uyarınca onaylı bir sertifikasyon mekanizması ile birlikte üçüncü ülkedeki veri sorumlusu veya veri işleyenin, ilgili kişinin hakları dâhil olmak üzere uygun güvenceler sağlamaya yönelik bağlayıcı ve uygulanabilir taahhütlerinin, kişisel verilerin üçüncü ülkelere veya uluslararası kuruluşlara aktarılmasına yasal dayanak olacağı düzenlenmiştir.

Yeni bir aktarım mekanizması olan sertifikaların GDPR'da tanımı bulunmamakla beraber GDPR m.42(1)'de veri koruma mühürleri ve işaretleri ile birlikte sertifika mekanizmalarından bahsedilmektedir. AB dışında bulunan bir şirket, kişisel

[291] GDPR m.41(2).
[292] Giakoumopoulos, Buttarelli ve O'Flaherty, *Handbook on European Data Protection Law*, s.182.

verilere uygun koruma sağlandığını gösteren sertifika almak için sertifika başvurusunda bulunabilir. Sertifikaya ilave olarak AB dışında bulunan şirket tarafından sertifikada yer alan standartlara uymak için yasal olarak bağlayıcı bir taahhütte bulunulması durumunda, GDPR m.46(2)(f)'e göre AB'den alınan veriler için uygun güvence sağlandığı kabul edilir. Bu yöntem ile sertifikalandırılan bir kuruluş, GPDR m.25 kapsamında GDPR ile uyumlu olduğunu gösterir ve m.32 kapsamında bir güvenlik seviyesi sağlamak için uygun teknik ve organizasyonel tedbirleri doğrulayarak veri aktarımları için koruma sağlamış olur[293].

GDPR m.42(5)'e göre sertifikalar şirketlere sadece ulusal denetim makamları veya ulusal denetim makamları tarafından belirlenen standartları karşılayarak akredite edilen belgelendirme kuruluşları tarafından verilebilir. Ancak söz konusu kuruluş birden fazla AB ülkesinden kişisel verilerin aktarılmasına ilişkin sertifika verecekse, akreditasyon için gerekli standartları ilgili AB ülkelerinin ulusal denetim makamları belirler ve EDPB'nin onayına sunar. EDPB veya ulusal denetim makamı, bir kuruluşun belgelendirme kuruluşu olarak akredite edilmesi için standartları belirledikten sonra, ulusal denetim makamı tarafından söz konusu standartları karşılayan kuruluşun belgelendirme kuruluşu olduğuna dair akreditasyon işlemi gerçekleştirilir.

Hâlihazırda akredite edilmiş sertifika sağlayıcıları bulunmamakla birlikte henüz söz konusu akreditasyon standartları da belirlenmemiştir. Ancak, EDPB tarafından 2018 yılında yayınlanan sertifikasyon sistemine ilişkin kılavuz[294], ulusal denetim makamları ve ulusal akreditasyon kuruluşlarının sertifikasyonla ilgili hükümleri yorumlaması ve uygulaması hususunda bir rehberlik sağlamaktadır.

GDPR m.42(2)'ye göre sertifikasyon mekanizmaları GDPR'a tabi olmayan veri sorumluları veya veri işleyenler tarafından da kullanılabilir. Bu durum, üyeleri

[293] ICO,"International Transfer".
[294] Bkz. https://edpb.europa.eu/our-work-tools/documents/public-consultations/2018/guidelines-12018-certification-and-identifying_en, Erişim Tarihi: 21.11.2021.

GDPR'a tabi olmayan fakat AB'deki iş ortaklarının AB'de yer alan kişisel verileri kendilerine aktarmasını kolaylaştırmak isteyen üçüncü bir ülkedeki ticaret birliğini *(trade association)* kapsayabilir[295]. Bu tür sertifikasyon mekanizmaları, m.46(2)(f)'de atıfta bulunulan şartlar gereğince üçüncü ülkelere veya uluslararası kuruluşlara kişisel veri aktarımları kapsamında üçüncü ülkede bulunan veri sorumlusu veya veri işleyenin sağladığı uygun korumaların varlığını göstermek için oluşturulabilir. GDPR m.42(2) üçüncü ülkelerde yer alan veri sorumluları veya veri işleyenleri için düzenlenmiş olsa da, ilgili kuruluşlar söz konusu sertifikasyon mekanizmalarını kullanmak istediklerinde bağlayıcı ve uygulanabilir taahhütlerde bulunmak durumundadırlar.

GDPR m.42(3)'e göre sertifikasyon mekanizması gönüllülük esasına dayanır ve sürecin şeffaf olması gerekir. Sertifikanın alınabilmesi için kriterler, sertifikasyon kuruluşunun bağlı olduğu ulusal denetim makamı tarafından belirlenebilir, fakat sertifika birden fazla AB ülkesinden kişisel verilerin aktarılmasına ilişkin olacaksa ulusal denetim makamları sertifika kriterlerinin belirlenmesi hususunu son karar için EDPB'ye iletebilir. Belirlenen kriterler ulusal denetim makamları ve akredite sertifika kuruluşları tarafından, yaptıkları başvuruya istinaden şirketlere sertifika verilmesinde kullanılır. GDPR m.42(5)'e göre, kriterlerin EDPB tarafından onaylanması durumunda AB genelinde geçerli ortak bir sertifika olan Avrupa Veri Koruma Mührü verilebilir, fakat bu mührün uluslararası veri aktarımları kapsamında yasal bir etkiye sahip olup olmadığı net değildir[296].

GDPR m.42(6)'ya göre, sertifika başvurusunda bulunan bir şirket, başvuruda bulunduğu ulusal denetim makamları veya akredite sertifika kuruluşlarının yapacağı değerlendirme için, talep ettiği sertifika prosedürüne ilişkin gerekli olan tüm bilgileri ve işleme faaliyetlerine erişimi ulusal denetim makamları veya akredite sertifika kuruluşlarına sağlamalıdır. GDPR m.42(7)'ye göre ise verilen sertifikalar en fazla üç yıl geçerli olmakta ve üç yıl içinde şirketin vermiş olduğu

[295] Kuner, Bygrave ve Docksey, *GDPR: A Commentary*, s.808.
[296] Kuner, Bygrave ve Docksey, *GDPR: A Commentary*, s.808.

taahhüde uygun davranıp davranmadığına ilişkin takip ilgili sertifikasyon kuruluşları tarafından yapılmaktadır. Sertifikalar veri koruma görevlisi gibi kişilere değil veri sorumlusu ve veri işleyenlere verilir.

Sertifikasyon mekanizmaları, davranış kurallarının yanında veri sorumlusu ve veri işleyenlerin GDPR ile uyumlu olduğunu gösteren bir başka yöntemdir[297]. Sertifikasyon mekanizmaları ilgili kişilerin, kuruluşların veri işleme kapsamında sağladıkları koruma düzeyini hızlı bir şekilde değerlendirmesine olanak tanımasının yanında sertifikasyon mekanizmasına uymayı tercih eden veri sorumluları ve veri işleyenler için daha fazla şeffaflık ve güvenilirlik sağlar[298].

Davranış kuralları gibi sertifikasyon mekanizması da, GDPR kapsamında mevcut uygun güvenceler arasında yeni ve henüz kullanılmamış bir yöntemdir. Nitekim Schrems II kararı ile Gizlilik Kalkanının geçersiz kılınması ve standart sözleşme maddeleri için yüksek standardın getirilmesi, özellikle küçük ve orta büyüklükteki işletmelerin AB'den ABD'ye veri aktarımlarında davranış kuralları ve sertifikasyon mekanizması yöntemlerini kullanmasının önünü açabilir.

2.2.6 Özel Sözleşme Maddeleri

AB dışına uygun güvenceler mekanizması ile kişisel veri aktarımı yapılabilmesi için GDPR'da yer alan alternatif yollardan birisi de GDPR m.46(3)(a)'da düzenlenen özel (*ad hoc*) sözleşme maddeleridir. İlgili madde de yer alan hükme göre, AB'de bulunan veri sorumlusu veya veri işleyen ile üçüncü ülkede veya uluslararası kuruluşta bulunan veri sorumlusu, veri işleyen veya veri alıcısı arasında özel sözleşme maddeleri ile kişisel veri aktarımı yapılabilmektedir.

Komisyonun onayladığı standart sözleşme maddelerinin aksine standart olmayan özel sözleşme maddeleri spesifik bir kişisel veri aktarımına mahsus olarak

[297] Giakoumopoulos, Buttarelli ve O'Flaherty, *Handbook on European Data Protection Law*, s.183.
[298] Giakoumopoulos, Buttarelli ve O'Flaherty, *Handbook on European Data Protection Law*, s.183.

düzenlenmektedir. Bu nedenle, özel sözleşme maddelerinin her aktarımda ulusal denetim makamı tarafından onaylanması gerekmektedir[299]. Ayrıca standart sözleşme maddelerinin mevcut olması, GDPR m.46(3)'de yer alan özel sözleşme maddelerinin kullanılmasına engel teşkil etmemektedir[300].

GDPR m.46(3)(a)'da yer alan özel sözleşme maddelerinin onaylanması için EDPB'nin görüşü gereklidir[301]. GDPR m.46(4)'e göre, aktarım için özel sözleşme maddelerine başvurulduğu durumlarda, GDPR m.63'de yer alan tutarlılık mekanizması uygulanır. EDPB'nin özel sözleşme maddeleriyle ilgili yayınladığı bir rehberi ve AB üye ülkelerinin denetim makamları tarafından onaylanan özel sözleşme maddesi bulunmamaktadır.

2.2.7 İdari Düzenlemelere Eklenen Hükümler

GDPR m.46(3)(b)'de, kamu kuruluşları veya organları arasındaki idarî düzenlemelere, etkili ve uygulanabilir ilgili kişi haklarını içeren hükümler eklenmesi yoluyla uygun güvence sağlanabileceği yer almaktadır. GDPR m.46(3)(b) ve Gerekçe 108, AB'de yer alan kamu kuruluşları ve organlarından, üçüncü ülkelerdeki kamu makamları, kuruluşları veya ilgili görev veya işlevlere sahip uluslararası kuruluşlara kişisel veri aktarımlarının, ilgili kişilerin uygulanabilir ve etkili haklarının mutabakat zaptı (*memorandum of understanding*) gibi bir idarî düzenlemeye eklenerek gerçekleştirilebileceğini düzenlemektedir. Bu hükme göre AB dışına kişisel veri aktarımı, iki kamu makamı arasında yapılacak mutabakat zaptı gibi bir anlaşma ile yapılmaktadır[302]. Bu yöntemle veri aktarımı için taraflardan en az birisinin yasal olarak bağlayıcı anlaşma düzenleme yetkisinin bulunmaması gerekmektedir. Taraflarının ikisinin de yasal olarak bağlayıcı anlaşma düzenleme yetkisi varsa GDPR m.46(2)(a)'da yer alan "Kamu Kurumları

[299] Bilgi IT Law Institute, "Kişisel Verilerin Korunmasına İlişkin Düzenlemeler", s.27.
[300] Kızılırmak, "Cross-Border Transfer", s.34.
[301] GDPR m.64(1)(d).
[302] GDPR Gerekçe 108; GDPR Gerekçe 114.

veya Organları Arasında Yasal Olarak Bağlayıcı ve Uygulanabilir Belgeler" kullanılır.

İdari düzenlemelerin, aktarımın yapılacağı ilgili AB ülkesinin ulusal denetim makamı tarafından m.63 uyarınca tutarlılık mekanizması kapsamında onaylanması gerekmektedir[303]. Birden çok AB ülkesinden aktarım yapılacaksa denetim makamının onayı ile birlikte EDPB'nin olumlu görüşü alınmalıdır[304]. İkiden fazla kamu makamı arasında ve birden fazla ülkeye kişisel veri aktarım durumu mevcutsa da EDPB'nin görüşü ve onayı gerekmektedir[305].

Kamu makamları arasındaki aktarımlar için düzenlenen m.46(2)(a) gibi m.46(3)(b)'de sınırlı durumlar için kullanılabilmektedir[306]. Ayrıca, bu düzenlemeler kamu ve özel kuruluşlar arasında kullanım için uygun değildir[307]. EDPB tarafından 15 Aralık 2020 tarihinde, m.46(2)(a) ve m.46(3)(b) uyarınca AB'de yer alan kamu kuruluşları ve organlarından üçüncü ülkelerdeki kamu kuruluşlarına veya uluslararası kuruluşlara kişisel verilerin aktarılmasına ilişkin rehber yayınlanmıştır[308].

2.3 Belirli Durumlar İçin İstisnalar

GDPR m.49 "Spesifik Durumlara Yönelik İstisnalar" *(Derogations for specific situations)* başlığı ile düzenlenmiş olup m.49(1)'de bir yeterlilik kararının mevcut olmadığı ve uygun güvencelerin kullanılamadığı durumlarda kişisel verilerin AB haricindeki üçüncü bir ülkeye veya uluslararası bir kuruluşa aktarılabilmesi için gereken istisnai durumlar belirtilmiştir. Üçüncü ülkelere veri aktarımı için

[303] GDPR m.46(4).
[304] Tess Blair et al, "Appropriate Safeguards in the GDPR", Morgan Lewis, 14.02.2019, https://www.morganlewis.com/pubs/2019/02/appropriate-safeguards-in-the-gdpr, Erişim Tarihi: 11.10.2021.
[305] Bilgi IT Law Institute,"Kişisel Verilerin Korunmasına İlişkin Düzenlemeler", s.28.
[306] Tess Blair et al, "Appropriate Safeguards".
[307] ICO, "International transfer".
[308] Bkz. https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-22020-articles-46-2-and-46-3-b-regulation_en, Erişim Tarihi: 11.10.2021.

istisnaların kullanılması, yeterli düzeyde bir korumanın mevcut olmadığı anlamına gelir. Ancak, ABAD'ın Schrems II kararında istisnaların sadece yeterli koruma sağlandığı takdirde kullanılabileceğini ima eden[309], "*kişisel verilerin üçüncü bir ülkeye aktarımının gerçekleştirilmesine dayanan GDPR 5. Bölümün hükmüne bakılmaksızın bu koruma seviyesi garanti edilmelidir*[310]*"* şeklindeki tespiti, m.49'un gerekçesiyle ters düşmemelidir. Nitekim istisnaların mantığı, ilk olarak m.45 ve m.46'da yer alan aktarım yöntemlerinin kullanılması, bu yöntemler mevcut değilse yani yeterli koruma olmadığında aktarım için hukuki dayanak oluşturması açısından istisnalara başvurulması gerektiğidir.

ABAD Schrems II kararında, Gizlilik Kalkanı Anlaşmasının geçersiz kılınması durumunda yasal boşluğun doldurulması amacıyla kişisel verilerin GDPR m.49'da yer alan istisnalara dayanarak aktarılabileceğini dolayısıyla aktarımlar için yasal bir boşluk oluşmadığını tespit etmiştir[311]. Bu durum m.49'da yer alan istisnalar için gizli bir atıftır ve istisnaların Gizlilik Kalkanı'nın geçersiz kılınmasının yerini doldurabilmesi için yardımcı olabileceği anlamına gelmektedir[312]. ABAD'ın Schrems II kararında istisnalar ile ilgili vardığı bu sonuç, Mahkemenin GDPR'ın 5. Bölümünde yer alan veri aktarımına ilişkin hiyerarşik yapıyı görmezden geldiği şeklinde yorumlanmaktadır[313]. Ancak hem EDPB'nin hem de m.49'un ifadesine göre istisnaların katı olarak yorumlanması gerekmektedir. ABAD'ın kendi ifadesinden de anlaşıldığı üzere[314] istisnaların kullanımının yalnızca gerekli olanla sınırlı olması gerekirken, Gizlilik Kalkanı Anlaşması gibi bir anlaşma kapsamında alınan bir yeterlilik kararı, kapsamına giren tüm kişisel verilerin aktarılmasına imkân sağlar. Bu sebeple istisnalar geçersiz kılınan yeterlilik kararlarının yerini dolduramaz[315].

[309] Kuner, Bygrave ve Docksey, GDPR: *Update of Selected Articles*, s.162.
[310] Case C-311/18, *Schrems II*, para. 92.
[311] Case C-311/18, *Schrems II*, para. 202.
[312] Kuner, Bygrave ve Docksey, *GDPR: Update of Selected Articles*, s.162.
[313] Kuner, Bygrave ve Docksey, *GDPR: Update of Selected Articles*, s.162.
[314] Case C-311/18, *Schrems II*, para. 176.
[315] Kuner, Bygrave ve Docksey, *GDPR: Update of Selected Articles*, s.162.

İstisnalara dayanarak veri aktarımı yapabilmek için, söz konusu aktarımın tekrar eden şekilde ve geniş kapsamlı olmaması gerekmekte[316] ve aktarıma ilişkin yeterlilik kararı ve uygun güvenceler gibi başka bir yasal dayanağın olmaması şartı bulunmaktadır. Üçüncü ülkelere veya uluslararası kuruluşlara yasal olarak veri aktarılması için istisnaların son çare olması istisnanın doğası ile uyumlu olup[317] istisnalar doğası gereği veri aktarımları için ilave koruma sağlamazlar. GDPR m.49'da yer alan istisnaların dar kapsamlı yorumlanarak aktarım için kural haline gelmemesi gerekmektedir[318]. GDPR m.49'un uygulanması sırasında, m.44'e göre, üçüncü ülkelere veya uluslararası kuruluşlara kişisel verileri aktaran veri sorumlusu veya veri işleyen GDPR'da bulunan diğer hükümlere ilişkin yükümlülükleri yerine getirmelidir. Ayrıca, m.44'de yer aldığı üzere GDPR 5. Bölümdeki hükümlerin uygulanmasının gerçek kişilerin temel hak ve özgürlüklerini engellemeyecek şekilde gerçekleştirilmesi durumu m.49'da yer alan istisnaların uygulanması için de geçerlidir. Bu sebeple, m.49(1)'de yer alan istisnalar veri aktarımının genel ilkelerinin muafiyet durumu olup madde başlığından da anlaşılacağı üzere belirli durumlar için kullanılmalı ve dar bir şekilde yorumlanarak kural haline gelmemelidir[319]. Ayrıca, GDPR m.49(2)-(4)'de açıkça belirtilen ve bazı istisnalar için düzenlenen sınırlamalar, istisnaların dar kapsamda yorumlanması ve tedbirli kullanılması açısından önemlidir[320].

İstisnalar, yeterli koruma veya uygun güvence sağlamadığından ve m.49'a göre yapılan aktarımlar için ilgili makamlardan izin alınması gerekmediğinden bu aktarım yönteminde ilgili kişilerin temel hak ve özgürlüklerine ilişkin daha fazla risk bulunmakta ve bu nedenle ilgili aktarımlarda veri sorumluları, ilgili kişilerin aktarımdan sonra verilerinin işlenmesine yönelik sahip oldukları temel hak ve

[316] European Data Protection Board (EDPB), "Guidelines 2/2018 on derogations of Article 49 under Regulation 2016/679", 25.05.2018, s.4, https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_2_2018_derogations_en.pdf, Erişim Tarihi: 16.11.2021.
[317] Giakoumopoulos, Buttarelli ve O'Flaherty, *Handbook on European Data Protection Law*, s.264.
[318] Theodorakis,s.42.
[319] EDPB, "Guidelines 2/2018", s.4; EDPB, "Recommendations 01/2020", s.13.
[320] Kuner, Bygrave ve Docksey, *GDPR: A Commentary,* s.846.

güvencelerin süreceğine ilişkin garanti veren çözümleri sunmalıdır[321]. Bununla beraber GDPR'da yer alan yasal veri işleme için belirlenen şartlara uyulabilmesi durumuna istinaden, kişisel verilerin temin edildiği kaynağa (ilgili kişiler veya başka kaynaklar) bakılmaksızın aktarım için kullanılan istisnaya ilişkin ilgili kişilerin bilgilendirilmesi gerekir[322]. Ayrıca, AB veya AB üye ülkelerinin iç hukuklarında yer alan kamu yararı nedeniyle veri aktarımlarını sınırlandırılabileceği de unutulmamalıdır[323].

GDPR m.49(1)'in 2. Paragrafı uyarınca "veri sorumlusunun zorlayıcı meşru menfaatleri" istisnasının kullanılabilmesi için yapılan aktarımların "tekrar etmeyen" şekilde olması gerekmekte ve bu ifade sadece bu hükümde açıkça yer almaktadır. EDPB, tekrarlanmayan aktarımları, "*bir defadan fazla olabilen fakat düzenli olmayan ve sıra dışı rastgele olan eylemler, bilinmeyen şartlar altında ve keyfi zaman aralıklarında gerçekleşen aktarımlar*"[324] olarak tanımlamıştır. Tanıma göre, tekrar eden aktarımlar için yasal dayanak olarak bir istisna kullanılıyorsa bu kullanım istisna değildir. Ayrıca, GDPR Gerekçe 111'de yer almakta olan "ara sıra" terimi, GDPR m.49(1)(b), m.49(1)(c) ve m.49(1)(e)'de yer alan sözleşme ve yasal iddialar istisnaları için geçerli olmakta ve bu istisnaların kullanımını sınırlandırmaktadır.

Bununla birlikte, ara sıra aktarım sınırlamasına açık rıza, kamu yararı, hayati menfaat ve kamu sicili istisnaları tabi değildir. Ayrıca WP29'a göre, belirli durumlar için istisnalar münferit aktarımlarla ilgili kullanılmalı ve tekrar eden aktarımlar için kullanılamamalıdır[325]. Örneğin, milyonlarca kişinin verisini

[321] EDPB, "Guidelines 2/2018", s.4.
[322] Bkz. EDPB, "Guidelines 03/2020 on the processing of data concerning health for the purpose of scientific research in the context of the COVID-19 outbreak", 21 April 2020, s.12, https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_202003_healthdatascientificresearchcovid19_en.pdf, Erişim Tarihi: 15.11.2021.
[323] EDPB, "Guidelines 2/2018", s.4.
[324] EDPB, "Guidelines 2/2018", s.4.
[325] Article 29 Working Party , "Working document on a common interpretation of Article 26 (1) of Directive 95/46 of 24.10.1995" ("WP 114"), Brussels, 25 November 2005, s.2, https://www.pdpjournals.com/docs/88080.pdf , Erişim Tarihi: 11.10.2021.

işleyerek tüm dünyadaki otel, havayolu vb. şirketlere online rezervasyon sistemi sağlayan bir dağıtım şirketi AB'deki verileri istisnalardan biri olan sözleşme yapma zorunluluğuna istinaden ABD'de yer alan sunuculara aktarıyorsa, toplu bir aktarım yapıldığından söz konusu aktarım GDPR hükümlerine uygun değildir, çünkü toplu aktarımlar için hukuki dayanak olarak istisnalar kullanılamamaktadır[326].

İstisnaların kullanılabilmesi için veri aktarımı belirli bir amaç için "gerekli" olmalıdır. Bu kapsamda bazı istisnalar için "gereklilik testi[327]" *(necessity test)* yapılarak aktarımın gerekli olup olmadığı belirlenmelidir. Gereklilik testi, veri aktaranın kişisel verilerin aktarımının, istisnanın özel amacı için gerekli olup olmadığı hususunda bir değerlendirme yapmasını gerektirir[328]. GDPR m.49(1)(b) ve m.49(1)(c) de yer alan sözleşme, m.49(1)(d) de yer alan kamu yararı, m.49(1)(e) de yer alan yasal iddialar ve m.49(1)(f) de yer alan ilgili kişilerin veya diğer kişilerin hayati menfaatlerinin korunması istisnaların kullanılabilmesi için veri aktarımının belirli bir amaç için gerekli olması koşuluna istinaden gereklilik testi yapılmalıdır[329]. Gereklilik testi m.49(1)(a) da yer alan ilgili kişiden açık rıza alınması, m.49(1)(g) da yer alan Birlik kamu sicilinden yapılan aktarımlar ve m.49(1)'in 2. paragrafta da yer alan veri sorumlusunun zorlayıcı meşru menfaatleri istisnalarında kullanılmaz.

EDPB, açık rıza ve kamu yararı istisnalarının COVID 19 salgını ile mücadelede sadece küresel olarak tıbbi durumun aciliyeti sebebiyle geçici bir tedbir olarak kullanılması gerektiğini ifade etmiştir[330]. COVID 19 salgınının özelliği söz konusu istisnaların araştırma amacıyla yapılan ilk aktarımlarda kullanılmasını yasal kılsa da aynı konuda uzun süreli ve tekrar eden aktarımlar olacaksa, yeterlilik kararı veya uygun güvencelerin kullanılması gerekecektir[331].

[326] Giakoumopoulos, Buttarelli ve O'Flaherty, *Handbook on European Data Protection Law*, s.265.
[327] EDPB, "Guidelines 2/2018", s.5.
[328] EDPB, "Guidelines 2/2018", s.5.
[329] EDPB, "Guidelines 2/2018", s.5.
[330] EDPB, "Guidelines 03/2020", s.13.
[331] EDPB, "Guidelines 03/2020", s.13.

GDPR m.49(1)(b), m.49(1)(c) ve m.49(1)'in 2. Paragrafı ve m.49(4)'ün ifadelerinde veri sorumlularına atıfta bulunulurken, m.49(6) ve atıfta bulunduğu m.49(1)'in 2. Paragrafı veri işleyenlerden de bahseder. Bu kapsamda, söz konusu istisnanın veri sorumlusu veya veri işleyenin gerçekleştirdiği aktarımlardan hangisi için geçerli olduğu, ilgili istisnanın ifadesi ve amacına göre belirlenmelidir[332].

Kişisel verilerin aktarılması için 95/46 Sayılı Direktif m.26(1)'de düzenlenen istisnalar, GDPR m.49'da yer alan istisnaların temelini oluşturmaktadır[333]. GDPR'da, Direktifte yer alan istisnalarla beraber ilave istisnalar düzenlenmiş ve istisnaların belirsiz olan bazı sınırlamaları ve kullanımları GDPR'da açıkça belirtmiştir. GDPR m.49'da düzenlenen istisnalar aşağıda detaylı olarak incelenecektir.

2.3.1 Açık Rıza

Veri koruma hukukunun temel ilkelerinden birisi olan ilgili kişinin katılımı, ilgili kişinin rızasını da kapsamaktadır[334]. Veri aktarımı için ilgili kişiden rıza alınması 95/46 sayılı Direktifte klasik hukuki dayanaklardan birisiydi ve GDPR'da da bu hukuki dayanak devam etmektedir. GDPR m.49'da yer alan ilk istisna da ilgili kişiden açık rıza alınmasıdır. Bir yeterlilik kararı ve uygun güvencelerin mevcut olmaması durumunda, ilgili kişiye aktarımın riskleri hakkında bilgi verilmesinin ardından, ilgili kişinin söz konusu aktarıma açıkça rıza göstermesi halinde verilerin AB dışında yer alan üçüncü bir ülkeye veya uluslararası bir kuruluşa aktarılabileceği GDPR m.49(1)(a)'da düzenlenmiştir. GDPR m.49(3)'e göre bu istisna kamu yetkilerinin kullanımı kapsamında kamu kuruluşlarının gerçekleştirdiği faaliyetlerde kullanılmamaktadır.

[332] Kuner, Bygrave ve Docksey, *GDPR: A Commentary*, s.846.
[333] Kuner, Bygrave ve Docksey, *GDPR: A Commentary*, s.844.
[334] Kızılırmak, "Cross-Border Transfer", s.41.

Rızanın geçerli olabilmesi için taşıma gereken genel şartlar GDPR m.4(11)'de ve m.7'de yer almaktadır. GDPR m.49(1)(a)'da yer alan "rıza" için de geçerli olan[335] ve rızada yer alması gereken şartları içeren bir rehber de WP29 tarafından yayımlanmıştır[336]. Ayrıca, üçüncü ülkelere ve uluslararası kuruluşlara veri aktarılmasına hukuki dayanak oluşturması için m.49(1)(a)'da yer aldığı üzere rızanın taşıması gereken ilave koşullar bulunmaktadır. GDPR, veri korumaya ilişkin risklerin olması durumunda açık rızayı gerekli kılar. GDPR m.49(1)(a)'da yer alan açık rızanın, uluslararası aktarımların daha yüksek risk taşımasından dolayı GDPR m.9(2)(a)'da yer alan hassas veriler için gerekli olan rıza ile aynı seviyede ve m.4(11)'de tanımlanan rızadan daha katı olması gerekmektedir[337]. Bu yüksek seviye, kişisel verilerin aktarılmasına izin vermenin dolaylı olarak ifade edilmemesini ve bir web sitesinde boş kutucuğu işaretlemek, tıbbi tedavi için bir rıza formuna elektronik imza ile onay vermek gibi bazı eylemlerle ispat edilmesini gerektirir[338].

İlgili kişinin rızası, GDPR m.4(11)'de ilgili kişinin beyan ederek veya açık bir onaylama hareketi göstererek kendisiyle ilgili kişisel verilerin işlenmesini kabul ettiğini gösteren özgür olarak verilmiş özel, bilgilendirilmeye dayalı ve açık bir gösterge olarak tanımlanmıştır. GDPR m.7'de ise rızanın genel şartları tanımlanmış ve hükme göre, rızanın yazılı bir beyan olarak verilmesi halinde rıza talep formunda yer alan söz konusu rıza diğer hususlardan açık olarak ayırt edilecek halde, anlaşılır ve kolay olarak erişilebilir olmalıdır. Ayrıca rıza açık ve sade bir dil ile yazılarak sunulmalı ve istenildiği zaman ilgili kişinin vermiş olduğu rızayı geri çekme hakkı mevcut olmalıdır.

Rızanın geçerli olması koşullarından birisi olan rızanın spesifik yani sadece bir amaç için olması gerekliliğine istinaden GDPR m.49(1)(a) kapsamında veri

[335] EDPB, "Guidelines 2/2018", s.6.
[336] Article 29 Working Party (WP29), "Guidelines on Consent under Regulation 2016/679", ("WP 259" Rev.01), 7 Haziran 2018, https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=623051, Erişim Tarihi: 30.11.2021.
[337] Kuner, Bygrave ve Docksey, *GDPR: A Commentary*, s.847.
[338] WP29, "Guidelines on Consent", s.18-19.

aktarımının yasal olması için açık rızanın, belirli bir veri aktarımı için özel olarak verilmesi gerekmektedir[339]. Bu durum, gelecekte meydana gelebilecek belirsiz bir veri aktarımı ve aktarıma ilişkin özel şartların bilinmediği durumlar için "battaniye rıza" diye tabir edilen rızanın alınmasını engellemiş olmaktadır[340]. Açık rızanın spesifik özellikte olması gerekliliği, aktarımın içeriğine yönelik şeffaflığı ve ilgili kişinin bir noktaya kadar aktarımı kontrol edebilmesini sağlamakta, ayrıca verilen açık rızanın gelecekteki aktarımlar için geçerli olmaması sonucunu doğurmaktadır[341]. Bu nedenle, veri sorumlusu yapılacak aktarıma özel bir rıza alınıp alınmadığını kontrol etmelidir[342].

GDPR m.4(11)'de düzenlenen ilgili kişinin aktarıma ilişkin "bilgilendirilmesi" koşuluna istinaden ilgili kişinin bilgilendirilmesi gereken konular; kişisel veri aktarılanlar ve kategorileri, verilerin aktarılacağı ülke veya ülkeler, aktarımın yapılmasını gerektiren nedenler, aktarılacak veri türleri, istendiği zaman açık rızanın geri çekilme hakkının var olduğu ve aktarıma ilişkin olası riskler şeklindedir[343]. Ayrıca, rıza için ilgili kişinin bilgilendirilmesi gerekliliğine ilave olarak GDPR m.49(1)(a)'da yer alan hükme göre, ilgili kişinin bir yeterlilik kararı ve uygun güvencelerin olmamasından dolayı aktarıma ilişkin oluşabilecek riskler hakkında da bilgilendirilmesi gerekmektedir. GDPR m.49(1)(a)'da yer alan ilgili kişinin aktarımın olası riskleri hakkında bilgilendirilmesi koşulu GDPR m.4(11)'de yer alan bilgilendirilmiş rızayı daha da güçlü hale getirmektedir[344]. Bu şekilde yapılan bilgilendirme ile ilgili kişiler, aktarımın sadece kendi rızalarına istinaden gerçekleşeceğini ve başka bir AB veri koruma kuralının mevcut olmayacağının farkında olacaklardır[345]. Bu bilgilendirmeler aktarım gerçekleşmeden önce

[339] EDPB, "Guidelines 2/2018", s. 7.
[340] Kuner, Bygrave ve Docksey, *GDPR: A Commentary*, s.847.
[341] Bilgi IT Law Institute, "Kişisel Verilerin Korunmasına İlişkin Düzenlemeler", s.85.
[342] EDPB, "Guidelines 2/2018", s.7.
[343] ICO, "International Transfers".
[344] EDPB, "Guidelines 2/2018", s.7.
[345] Kızılırmak, "Cross-Border Transfer", s.42.

yapılmalıdır. İlgili maddelerde belirtilen şartlarda bilgilendirme yapılmadığı takdirde açık rıza istisnası kullanılamamaktadır[346].

GDPR'a göre ilgili kişilerin verdikleri rızayı istedikleri zaman geri alma hakları bulunmaktadır. GDPR, rızanın verilmesinin kolay olduğu kadar geri alınmasının da veri sorumluları tarafından kolay hale getirilmesini ve ilgili kişilerin verdikleri rızayı geri çekme hakları olduğuna dair bilgilendirilmesini gerektirir [347].

GDPR'da yer alan açık rıza şartları son derece yüksek standartlara sahiptir ve ilgili kişinin istediği zaman açık rızayı geri çekme hakkının bulunması da bu standartların uygulanmasını zorlaştırmaktadır[348]. Bu şartlar ışığında, yurtdışına veri aktarımı için hukuki dayanak olarak kullanılan rızanın riskli bir tercih olduğu değerlendirilmektedir[349]. GDPR kapsamında rıza için gerekli olan tüm şartları sağlayarak ilgili kişilerden tek bir eylem ile rıza vermelerini içeren olumlu bir onay almak kolay bir yöntem değildir[350]. Önceden işaretlenmiş kutucuklar, doldurulmuş formlar veya sessizlik ve hareketsiz kalma rızanın şartlarına uygun değildir[351]. Gerek açık rızanın alınması ve yürütülmesi konusundaki zorluklar gerekse geri çekme hakkından dolayı veri sorumluları aktarımlar için daha çok diğer hukuki dayanakları tercih etme eğilimindedirler[352].

COVID 19 salgını kapsamında yapılan aktarımlar için açık rıza istisnasının, COVID 19 salgını ile mücadele etmek için veri aktarımının gerektiği durumlarda yasal bir dayanak oluşturabileceği EDPB tarafından belirtilmiştir[353]. Ancak, açık rıza istisnasının aktarımlara ilişkin genel kuralın muafiyeti olduğu ve kısıtlayıcı

[346] EDPB, "Guidelines 2/2018 ", s.8.
[347] GDPR m.7(3).
[348] Bilgi IT Law Institute, "Kişisel Verilerin Korunmasına İlişkin Düzenlemeler", s.86.
[349] Theodorakis,s.45.
[350] Kızılırmak, "Cross-Border Transfer",s.42.
[351] GDPR Gerekçe 32.
[352] ICO, "International Transfers".
[353] EDPB, "Guidelines 03/2020", s.12-13.

olarak ve durum bazında değerlendirilmesi gerektiği de EDPB tarafından vurgulanmıştır[354].

Ayrıca, GDPR Gerekçe 171'de, GDPR'dan önce alınan rızanın GDPR'ın hükümlerine uygun olması durumunda tekrar rıza alınmasına gerek olmadığı belirtilmiştir. Bu hüküm, GDPR kapsamındaki rızanın Direktif kapsamındaki rızadan daha katı gerekliliklere sahip olduğunu açıkça göstermektedir.

2.3.2 Sözleşmenin İfası

GDPR m.49(1)(b)'de veri sorumlusu ile ilgili kişi arasında bulunan bir sözleşmenin yürütülmesi veya ilgili kişinin talebine istinaden sözleşme öncesinde yer alan önlemlerin uygulanması açısından gerekli olması durumunda kişisel verilerin üçüncü ülkelere veya uluslararası kuruluşlara aktarılabileceği hükmü yer almaktadır. İstisnada bahsedilen güvencelere ilişkin talep ilgili kişi tarafından yapılmalı ve hüküm gereği sözleşmenin yürütülmesinden önceki bir süreyle ilgili olmalıdır. GDPR'da yer alan bu istisnanın Direktif'te yer alan aynı istisnadan farkı, "ilgili kişinin talebine yanıt olarak" yerine "ilgili kişinin talebine istinaden" ifadesinin yer almasıdır. Böylece sözleşme öncesi tedbirlerin uygulanması durumunun ilgili kişinin talebine istinaden başlatılması gerektiği daha net ifade edilmiştir.[355] Ayrıca, bu durumda sözleşmenin kurulması ve ifa edilmesi için aktarım zorunlu olmalıdır[356]. GDPR m.49(3)'e göre bu istisna kamu görevlilerinin kullanımı kapsamında kamu kuruluşlarının gerçekleştirdiği faaliyetlerde kullanılmamaktadır.

GDPR Gerekçe 111 kapsamında, bu istisnaya dayanarak yapılan veri aktarımları, aktarımın ara sıra yapıldığı ve bir sözleşmeye istinaden gerekli olduğu durumlarda yapılabilir. Bir sözleşmenin yürütülmesine ilişkin istisnalar epeyce fazla olsa da

[354] EDPB, "Guidelines 03/2020", s.12.
[355] Kuner, Bygrave ve Docksey, *GDPR: A Commentary*, s.848.
[356] Bilgi IT Law Institute, "Kişisel Verilerin Korunmasına İlişkin Düzenlemeler", s.29.

Gerekçe 111'de yer alan "gereklilik" ve "ara sıra yapılan aktarımlar" koşulları ile bu istisna sınırlandırılmıştır[357]. Ayrıca, GDPR m.49(1)(b)'de veri aktarımının ne zaman gerekli olduğuna ilişkin, istisnanın kullanımını sınırlandırıcı tanım yer almaktadır. Veri aktarımının gerekliliği için yapılacak "gereklilik testi" de, bu istisnaya dayanarak yapılacak aktarımların sayısını sınırlamaktadır. Bu istisnanın kullanılabilmesi için yapılan gereklilik testine göre veri aktarımı ile sözleşmenin amaçları arasında yakın ve doğrudan bir bağlantı olması gerekir[358]. Bu anlamda, gereklilik testi kapsamında veri sorumlusu her zaman, sözleşmenin yürütülmesi için aktarımın gerekli olup olmadığını değerlendirmelidir[359].

GDPR Gerekçe 111'e göre kişisel verilerin üçüncü ülkelere bu istisna kapsamında aktarılabilmesi için aktarımın ara sıra yapılıyor olması gerekmektedir. Bu çerçevede EDPB, bu istisnanın düzenli bir ilişki içinde sistemli olarak gerçekleşen veri aktarımlarını içermediği ve bir iş ilişkisi içinde gerçekleşen birçok aktarım için kullanılamayacağını ifade etmiştir[360]. Aktarımın "ara sıra" veya "ara sıra olmayan" şeklinde yapılıp yapılmadığının belirlenmesi, duruma göre tayin edilmelidir[361]. Aktarımın ara sıra olduğuna dair örnek durum, bir şirket çalışanının iş sözleşmesi gereği yurtdışında yaptığı müşteri ziyaretleri kapsamında toplantı düzenlenmesi için kişisel verilerinin şirket tarafından müşterilere gönderilmesi olabilir[362]. Örneğin, çok uluslu bir şirketin eğitim düzenlediği üçüncü bir ülkede bulunan eğitim merkezine eğitime katılan çalışanların kişisel verileri sistemli olarak aktardığında yapılan aktarımlar "ara sıra" olarak kabul edilmez, yani sürekli devam eden bir ilişkide düzenli olarak yapılan veri aktarımları sistemli ve tekrar eden olarak görülür ve "ara sıra" anlamında değerlendirilmez[363].

[357] EDPB, "Guidelines 2/2018", s.8.
[358] EDPB, "Guidelines 2/2018", s.8.
[359] Kızılırmak, "Cross-Border Transfer", s.45.
[360] EDPB, "Guidelines 2/2018", s.9.
[361] EDPB, "Guidelines 2/2018", s.9.
[362] EDPB, "Guidelines 2/2018", s.9.
[363] EDPB, "Guidelines 2/2018", s.9.

Bir turizm firmasının rezervasyon yapmak amacıyla AB vatandaşı müşterisinin kişisel verilerini üçüncü bir ülkede bulunan bir otele aktarması bu istisnaya dayanarak yapılan aktarıma tipik bir örnek olarak verilebilir[364]. Burada önemli olan otel ile turizm firmasının düzenli bir iş ilişkisi olmaması gerektiğidir[365]. Ayrıca, sözleşmenin taşıdığı müşterilerin seyahat organizasyonu amacı ile veri aktarımı arasında yeterli derecede bağlantı bulunmaktadır[366]. Bu istisnaya dayanılarak, ilgili kişinin talebine istinaden sözleşme öncesi alınan önlemlerin uygulanması amacıyla da aktarım yapılabilmektedir. Hükümde bahsedilen sözleşme öncesi önlemler, ilgili kişinin bir sözleşme imzalamadan önce başlattığı önlemleri kapsayacak şekilde geniş yorumlanmaktadır[367]. Bu duruma, AirBnB'nin AB vatandaşı müşterisinin verilerini, üçüncü bir ülkedeki ev sahibine, bir daireye ilişkin bilgi talebinin bir parçası olarak rezervasyondan önce aktarması örnek olarak verilebilir[368]. Örneğin, bir seyahat acentesinin bir müşterinin seyahati için yaptığı ön rezervasyon sözleşme öncesi önlem kapsamında düşünülebilir.

2.3.3 İlgili Kişi Yararına Sözleşmenin İmzalanması ve Yürütülmesi İçin Gereklilik

Kişisel verilerin üçüncü ülkelere veya bir uluslararası kuruluşa aktarılmasına ilişkin istisnalardan üçüncüsü GDPR m.49(1)(c)'de düzenlenmiş olup hükme göre; ilgili kişi yararına veri sorumlusu ile başka bir gerçek veya tüzel kişi arasında yapılan bir sözleşmenin imzalanması veya yürütülmesi için aktarımın gerekli olması gerekmektedir. 95/46 sayılı Direktif m.26(1)(c)'de yer alan "veri sorumlusu ve üçüncü şahıslar arasında" ifadesi, GDPR m.49(1)(c)'de "veri sorumlusu ile bir gerçek veya tüzel kişi arasında" şeklinde değiştirilmiştir. GDPR m.49(3)'e göre bu istisnada kamu yetkilerinin kullanımı kapsamında kamu kuruluşlarının gerçekleştirdiği faaliyetler kapsamında kullanılamamaktadır[369].

[364] Bilgi IT Law Institute,"Kişisel Verilerin Korunmasına İlişkin Düzenlemeler", s.87.
[365] Bilgi IT Law Institute,"Kişisel Verilerin Korunmasına İlişkin Düzenlemeler", s.87.
[366] EDPB, "Guidelines 2/2018", s.9.
[367] Kuner, Bygrave ve Docksey, *GDPR: A Commentary,* s.848.
[368] Theodorakis, s.45.
[369] GDPR m.49(3).

GDPR Gerekçe 111 veri aktarımlarının sadece aktarımın ara sıra ve bir sözleşmeyle ilgili olarak gerekli olduğu durumlarda gerçekleşebileceğini açıklamaktadır. Bu durum sözleşmeye dayalı bir aktarım için kullanılabilen m.49(1)(c) istisnası için de geçerlidir. Bu nedenle kişisel veriler bu istisnaya dayanarak gereklilik testi ile birlikte ancak aktarımın ara sıra olması koşuluyla aktarılabilir.

Bu istisnanın GDPR m.49(1)(b)'den farkı, sözleşmenin ilgili kişinin yararına düzenlenmiş olması fakat ilgili kişinin sözleşmeye taraf olmamasıdır. Bu istisnayı m.49(1)(b)'de yer alan istisnadan ayıran en önemli fark ise ilgili kişi dışında üçüncü kişilerin verilerinin de bu sözleşmeye göre aktarılmasıdır[370]. Bu istisnanın kullanılmasına, bir seyahat şirketinin rezervasyon yapmak amacıyla üçüncü ülkede yer alan bir otele AB vatandaşı olan müşterisinin ailesine ait kişisel verileri aktarması örnek olarak verilebilir[371].

2.3.4 Kamu Yararı

GDPR m.49(1)(d)'de yer alan istisna uyarınca kişisel verilerin üçüncü ülkelere veya uluslararası bir kuruluşa aktarılabilmesi için yapılacak aktarım, kamu yararına ilişkin önemli sebeplerden dolayı gerekli olmalıdır. GDPR m.49(4)'de ise bu istisnada atıfta bulunulan kamu yararının, AB Hukukunda veya veri sorumlusunun tabi olduğu üye ülke hukukunda tanınan bir kamu yararı olduğu belirtilmektedir. Bu nedenle sadece üçüncü ülkenin hukukunda yer alan ve AB veya üye ülke hukukunda dayanağı olmayan bir kamu menfaati, önemli kamu menfaati koşuluna dayalı veri aktarımı için yasal bir dayanak sağlamaz[372]. Ayrıca üye ülkenin tabi olduğu uluslararası taahhütlerde bu kapsama girmektedir[373]. Örneğin, bu istisna belli amaçları olan ve uluslararası iş birliği sağlayan AB'nin veya üye devletlerin karşılıklılık ilkesine istinaden imzalamış olduğu bir anlaşma kapsamında

[370] Bilgi IT Law Institute,"Kişisel Verilerin Korunmasına İlişkin Düzenlemeler", s.87.
[371] ICO,"International Transfers".
[372] Kuner, Bygrave ve Docksey, *GDPR: A Commentary,* s.850.
[373] Kuner, Bygrave ve Docksey, *GDPR: A Commentary,* s.849.

kullanılabilir[374]. AB ile üçüncü ülke arasında bulunan Karşılıklı Adli Yardım Anlaşması'na (A Mutual Legal Assistance Treaty – "MLAT") dayalı aktarımlar bu istisna kapsamında karşılıklılık ilkesine göre değerlendirilir ve MLAT'nin varlığının kamu yararı şartını sağladığı kabul edilir[375].

Kamu yararı istisnasının COVID 19 salgınına ilişkin aktarımlar için de yasal bir dayanak oluşturabileceği EDPB tarafından belirtilmiştir[376]. COVID 19 salgını kapsamında, sadece kamu makamları değil, aynı zamanda özel kuruluşlarda (uluslararası bir ortaklık bağlamında bir aşının geliştirilmesi konusunda işbirliği yapan bir üniversitenin araştırma enstitüsü gibi) önemli kamu yararı istisnasına dayanabilecektir[377]. Ancak, kamu yararı istisnası genel kuralın istisnası olduğundan kısıtlayıcı yorumlanmalı ve mutlaka vaka bazında değerlendirilmelidir[378].

EDPB, COVID 19 salgınının, benzeri görülmemiş bir ölçek ve nitelikte olağanüstü bir sağlık krizi olduğunu[379] ve bu sebeple uluslararası veri aktarımlarına gerekçe olabilecek, tedavi belirlemek veya aşı geliştirmek gibi önemli bir kamu yararı gerekçesi oluşturduğunu belirtmiştir[380].

GDPR m.49(5)'e göre, bir yeterlilik kararının bulunmadığı durumlarda, önemli kamu yararı sebepleriyle özel nitelikli kişisel verilerin üçüncü bir ülkeye veya uluslararası bir kuruluşa aktarılmasına, AB veya üye ülke hukukunda açık bir şekilde sınırlama getirilebilir. Üye ülkeler sınırlamalara ilişkin hükümleri Komisyona bildirmelidir.

Bu istisnada dikkat edilmesi gereken husus, hükümde yer alan kamu yararı ifadesinin önemli kamu yararları olarak sınırlandırılmış olmasıdır. Bu çerçevede,

[374] Bilgi IT Law Institute,"Kişisel Verilerin Korunmasına İlişkin Düzenlemeler", s.88.
[375] Bilgi IT Law Institute,"Kişisel Verilerin Korunmasına İlişkin Düzenlemeler", s.30-31.
[376] EDPB, "Guidelines 03/2020", s.12-13.
[377] EDPB, "Guidelines 03/2020", s.13.
[378] Bkz. EDPB, "Guidelines 03/2020", s.12-13.
[379] EDPB, "Guidelines 03/2020", s.12.
[380] EDPB, "Guidelines 03/2020", s.12-13.

kamu yararı kavramının net olmaması ve önemli olması durumu hükmün dar ve dikkatli olarak yorumlanmasını gerektirir. Ayrıca bu istisnadan temelde kamu makamları yaralanabilmekteyse de özel kuruluşlarda kamu yararına ilişkin veri aktarımlarında bu istisnayı kullanabilir[381]. Bu durum GDPR Gerekçe 112'de yer alan ve hem kamu makamları hem de özel kuruluşlar tarafından yapılan aktarımlar için verilen örneklerden anlaşılmaktadır[382]. GDPR Gerekçe 112'de, salgınların takip edilmesi, afet gibi durumlara yönelik insani yardım hususu da önemli bir kamu yararı olarak yer almaktadır. Aynı Gerekçede yer alan bir diğer hükme göre, rıza vermesi fiziksel veya yasal olarak mümkün olmayan bir kişinin kişisel verilerinin, Cenevre Sözleşmesi dâhilindeki bir görevi gerçekleştirmek veya silahlı çatışmalarda Uluslararası İnsancıl Hukuka *(International Humanitarian Law)* uymak için, önemli bir kamu yararı veya ilgili kişinin hayati menfaatlerinden dolayı uluslararası insani yardım kuruluşlarına aktarılması gerekli görülmektedir. Buradan anlaşılacağı üzere bu istisnanın uygulanabilmesi için gerekli olan veri sorumlusu ve/veya veri alıcısının nitelik olarak kamu, özel veya uluslararası kuruluş olup olmadığı değil, ortada önemli bir kamu yararının olması gerektiğidir[383]. Ayrıca GDPR m.9(2)(g)'de yer alan özel kategorilerdeki kişisel verilerin işlenmesi için kamu yararının "kayda değer" olması gerekliliğine istinaden bu istisna her kamu yararı söz konusu olduğunda kullanılamayacaktır.

GDPR Gerekçe 111 ve 112'de yer alan açıklamalara göre bu istisnanın kullanımı "ara sıra" olarak sınırlandırılmamış olmasına rağmen bu durum m.49'da yer alan istisnalara dayanılarak yapılan aktarımların kural haline gelemeyeceği genel şartına aykırı olacaktır. Bu nedenle kamu yararı istisnasına dayanılarak yapılan aktarımların büyük ölçekli ve sistematik şekilde yapılmaması[384] ve aktarım süreklilik taşıyorsa bu istisnaya dayanılarak değil uygun güvencelere dayanılarak yapılması gerekmektedir.

[381] EDPB, "Guidelines 2/2018", s.11.
[382] EDPB, "Guidelines 2/2018", s.11.
[383] EDPB, "Guidelines 2/2018", s.11.
[384] EDPB, "Guidelines 2/2018", s.11.

2.3.5 Yasal İddialarda Bulunulması, Bu İddiaların Uygulanması veya Savunulması

GDPR m.49(1)(e)'ye göre, yasal iddialarda bulunulması, bu iddiaların uygulanması veya savunulması bakımından aktarımın gerekli olması durumunda kişisel veriler üçüncü ülkelere veya uluslararası bir kuruluşa aktarılabilecektir. GDPR Gerekçe 111'e göre, ilgili kişinin açık rızasını verdiği bir aktarımın bir sözleşme veya yasal iddia ile ilgili olarak "ara sıra" ve "gerekli" olduğu hallerde aktarımın adli prosedür veya düzenleyici kurumlar önündeki prosedürler dahil olmak üzere idarî veya herhangi bir mahkeme dışı prosedür içinde olup olmadığına bakılmaksızın belirli durumlarda aktarım olasılığına ilişkin hükümler eklenmelidir. Bu istisnanın kullanımında yapılacak gereklilik testi, ilgili veriler ile hukuki durumun belirli olarak kurulması, kullanılması veya savunulması arasında yakından ve önemli bir ilişkininin varlığını ortaya koymalıdır[385].

İstisnada bahsedilen yasal iddiaların hukuki olarak bir dayanağa sahip olması ve yasalar tarafından düzenlenmiş resmi süreçlerle ilgili olması gerekmektedir[386]. Bu süreçlerin sadece adli veya idarî yargı süreçleri ile ilgili olmasına gerek yoktur. Örneğin, yargılama süreci başlamamış olanlar da dâhil olmak üzere özel hukuk ve ceza hukuku kapsamında adli yargıda bulunan tüm yasal işlemler bu istisna kapsamına girmektedir[387]. Veri sorumlusunun üçüncü bir ülkedeki dava açma veya bir birleşme için onay isteme gibi prosedürleri gerçekleştirmek için eylemleri de bu istisna kapsamına girer[388]. Ayrıca, yasal veya resmi işlemlerin başlatılabileceği ihtimaline karşı bu istisna kullanılamamaktadır[389].

AB üyesi ülkelerin ulusal kanunlarında kişisel verilerin üçüncü bir ülkenin mahkemelerine veya diğer kurumlarına aktarılmasını yasaklayan veya sınırlandıran

[385] EDPB, "Guidelines 2/2018", s.12.
[386] Bilgi IT Law Institute,"Kişisel Verilerin Korunmasına İlişkin Düzenlemeler", s.88.
[387] ICO, "International Transfers".
[388] EDPB, "Guidelines 2/2018", s.11.
[389] EDPB, "Guidelines 2/2018", s.11.

hükümlerin yer alabileceği hususu veri sorumluları tarafından göz önünde bulundurulmalıdır[390]. Son olarak, bu istisna kamusal yetkilerin kullanılmasında kamu görevlileri tarafından görev tanımları kapsamında sürdürülen faaliyetler için kullanılabilir[391].

2.3.6 İlgili Kişi veya Başkalarının Hayati Çıkarlarının Korunması

GDPR m.49(1)(f) ve Gerekçe 112 uyarınca kişisel verilerin üçüncü ülkelere veya uluslararası kuruluşlara aktarılabileceği diğer bir istisna hükmü ise, ilgili kişinin fiziksel veya hukuki engeller sebebiyle rıza vermesinin mümkün olmadığı ve aktarımın ilgili kişinin veya diğer kişilerin hayatî menfaatinin korunması açısından gerekli olduğu durumdur. Hükme göre, yapılacak aktarım ile hayatî menfaati korunacak olan kişi, ilgili kişi veya başka bir kişi olabilir. Veri aktarımının bir kişinin sağlığını, fiziksel bütünlüğünü veya yaşamını daim kılmak için gerekmesi bu istisna kapsamında düşünülmelidir[392]. Üçüncü bir ülkede acil bir tıbbî müdahale gerektirecek durumda olan ve bilinci yerinde olmayan bir AB vatandaşının kişisel verilerinin söz konusu üçüncü ülkeye aktarılması ve deprem, sel, fırtına gibi doğal afet durumlarında mağdurların yeri ve durumunun tespit edilmesi için belirli kişisel verilerin acil olarak aktarılması ilgili kişinin veri aktarımı için onay veremeyeceği durumlara örnek olarak verilebilir[393]. Böyle bir durumda, yasa tarafından ilgili kişinin içinde bulunduğu ciddi zarar riskinin söz konusu ilgili kişinin kişisel verilerinin korunmasından daha önemli olduğu varsayılmıştır[394]. Bu durumda göz önünde bulundurulması gereken konu ise ilgili kişinin bilincinin açık ve geçerli bir karar verebilecek durumda olduğu ve onayının alınmasının mümkün olduğu durumlarda bu istisnanın kullanılamayacağıdır. Örneğin sağlıkla ilgili genel bir muayene durumunda bu istisnaya dayanılarak veri aktarımı yapılamayacaktır[395].

---

[390] EDPB, "Guidelines 2/2018", s.12.
[391] GDPR m.49(3).
[392] Kuner, Bygrave ve Docksey, *GDPR: A Commentary,* s.852.
[393] EDPB, "Guidelines 2/2018", s.13.
[394] EDPB, "Guidelines 2/2018", s.12.
[395] ICO, "International Transfers".

Bu istisnanın kullanılması için, söz konusu aktarım ilgili kişinin veya başka kişilerin şahsi menfaatlerini ilgilendirmeli ve önemli bir tıbbi teşhis durumu için gerekli olmalıdır. Örneğin, ilgili kişinin veya başka kişilerin verilerinin aktarılmasının, tıbbî bir tedavi için değil de tıbbî bir araştırma için gerekli olması durumunda, kişinin sağlığı veya hayatının tehlikede olmaması sebebiyle kişisel sağlık verilerinin aktarılması bu istisnaya dayanılarak yapılamaz[396]. Bu istisnanın kullanılabilmesi için önemli olan kriter ilgili kişinin verilerin aktarılması için fiziksel, zihinsel veya yasal olarak rıza verememesidir[397]. Bu çerçevede ilgili kişinin tam ehliyetli olduğu durumlarda ve rızasının istenebildiği her durumda bu istisna uygulama alanı bulmayacaktır.

2.3.7 Birlik Kamu Sicilinden Yapılan Aktarımlar

GDPR m.49(1)(g)'ye göre üçüncü ülkelere veya uluslararası bir kuruluşa yapılan aktarımın, AB ve AB üyesi ülkenin hukukuna göre kamuoyuna bilgi sağlanmasının amaçlandığı ve genel olarak kamuoyu veya meşru bir menfaati ispat edebilen herhangi bir kişi tarafından istişareye açık olan bir sicilden yapılması durumunda bu istisna kullanılabilecektir. Hükümde ayrıca, kişisel verilerin söz konusu istişareye açık sicilden AB veya AB üyesi ülkelerin yasaları tarafından belirlenen istişareye yönelik ortaya konan koşullar yerine getirildiği ölçüde aktarılabileceği yer almaktadır. Bahse konu siciller kamuoyunu bilgilendirme amacı taşıdığından, özel kuruluşların sicilleri bu istisna kapsamında değildir[398]. Bu istisna, AB ve AB üye devletlerinde bulunan kamu kayıtlarından veri aktarımını kapsamaktadır. Adli sicil ve tapu sicil kayıtları, dernek ve şirket sicilleri bu sicillere örnektir.

GDPR m.49(2), bu istisna kapsamında yapılacak aktarımları sicilde yer alan tüm kişisel verilere veya veri kategorilerine yer verilmeyecek şekilde sınırlandırmıştır. Kanunla oluşturulmuş bir sicilden aktarım yapılması ve meşru menfaati olan

[396] Kuner, Bygrave ve Docksey, *GDPR: A Commentary*, s.852.
[397] EDPB, "Guidelines 2/2018", s.13.
[398] EDPB, "Guidelines 2/2018", s.13.

kişilerin bu sicile başvurması durumunda, aktarım bu kişilerin talebine istinaden veya bu kişiler alıcı ise yapılabilir[399]. Bu hüküm ile ilgili kişilerin temel haklarının korunması amaçlanmakla beraber veri aktaranların her daim ilgili kişilerin menfaatlerini dikkate almasını gerektirmektedir[400]. Ayrıca, bu istisna, kamu makamlarının kamu yetkilerinin kullanılmasında gerçekleştirdiği faaliyetler için de uygulama alanı bulacaktır[401].

2.3.8 Veri Sorumlusunun Zorlayıcı Meşru Menfaatleri

GDPR m.49(1)'in 2. paragrafında, 95/46 sayılı Direktifte bulunmayan bir istisnaya yer verilmiştir. Bu istisnaya göre, hükümde açıkça belirtilen bazı koşullar mevcut olduğu takdirde ve veri sorumlusunun zorlayıcı meşru menfaatlerinin de gerektirmesi durumunda kişisel veriler üçüncü bir ülkeye veya uluslararası bir kuruluşa aktarılabilir. Hükümde, bu istisnanın GDPR m.45 ve m.46'da yer alan aktarım mekanizmalarından herhangi birinin kapsamına girmeyen ve m.49(1)'de sayılı diğer istisnaların uygulanmadığı durumlarda kullanılabileceği yer almaktadır. Ayrıca GDPR Gerekçe 113'den bu istisnanın bilimsel, akademik veya tarihsel bir araştırma için verilerin aktarılması durumunda da kullanılmak amacıyla düzenlendiği anlaşılmaktadır[402]. GDPR m.49(3)'e göre bu istisna kamu yetkilerinin kullanılması hususunda kamu makamları tarafından gerçekleştirilen faaliyetlerde kullanılamamaktadır.

Bu istisnanın kullanılabilmesi için hükümde yer alan ilk koşul aktarımın sürekli olmaması ve tekrar etmemesi gerektiğidir. Bu durum aktarımın birden çok olabileceği fakat devam eden ve düzenli bir aktarım olmaması gerektiği şeklinde yorumlanmalıdır. Aktarım, yalnızca sınırlı sayıda ilgili kişiyi ilgilendirmelidir. Sınırlı sayı ifadesi için bir değer belirlenmemiş olup aktarım sayısının ilgili aktarım türüne uygun olacak şekilde az olabileceği ve bu sayının mevcut duruma

[399] GDPR Gerekçe 111.
[400] GDPR Gerekçe 111.
[401] GDPR m.49(3).
[402] Kuner, Bygrave ve Docksey, *GDPR: A Commentary*, s.854.

göre değişebileceği ifade edilmiştir[403].

Hükümde yer aldığı üzere aktarım veri sorumlusunun zorlayıcı meşru menfaatleri için gerekli olmalıdır. Ayrıca, veri sorumlusunun bu zorlayıcı meşru menfaatleri ilgili kişinin menfaatleri, hakları ve özgürlüklerine göre daha baskın olmalıdır. Bu bağlamda meşru menfaat ifadesi yorumlanırken kişisel verilerin korunması hakkının özüne zarar verilmemelidir[404]. Burada geçen "zorlayıcı" olarak kabul edilecek "meşru menfaatler" GDPR m.6(1)(f)'de yer alan meşru menfaatlerin hepsi için geçerli olamayacağından istisnanın kapsamı sınırlanmaktadır[405]. Örneğin, bir veri sorumlusunun kendini veya işini ciddi bir zarardan veya cezadan korumak için kişisel verileri aktarmak zorunda kalması zorunlu meşru menfaate örnek olarak verilebilir[406].

EDPB'nin son çare (*a last resort*) olarak ifade ettiği bu istisnayı kullanmadan önce GDPR'da bulunan hesap verebilirlik ilkesi[407] kapsamında hem GDPR m.45 ve 46'da yer alan aktarım araçlarının hem de m.49(1)'de yer alan istisnaları kullanmanın mümkün olmadığı veri sorumlusu tarafından gösterilebilmelidir[408]. Veri sorumlusunun zorlayıcı meşru menfaatlerinin ilgili kişinin menfaatleri veya hak ve özgürlüklerinden baskın olup olmadığını tespit etmek amacıyla denge testi yapılması gerekmektedir[409]. Bu kapsamda veri sorumlusunun veri aktarımına ilişkin tüm koşulları değerlendirmesi ve bu değerlendirmeye göre aktarımı yapılacak verilerin korunması amacıyla "uygun güvenceler" sağlaması gerekmektedir. Yapılan değerlendirmede aktarımın, ilgili kişinin meşru menfaatleri ve temel hak ve özgürlükleri üzerindeki olası riskleri değerlendirilmelidir. Bu riskler ve ilgili kişinin hak ve özgürlükleri için uygun güvencelerin neler olduğu değerlendirilirken, veri sorumlusu tarafından verilerin niteliği, veri işlemenin amacı

[403] EDPB, "Guidelines 2/2018", s.15.
[404] Küzeci, s.347.
[405] EDPB, "Guidelines 2/2018", s.15.
[406] EDPB, "Guidelines 2/2018", s.15.
[407] GDPR m.5(2) ve m.24(1).
[408] EDPB, "Guidelines 2/2018", s.14.
[409] EDPB, "Guidelines 2/2018", s.15.

ve süresi, menşe ülkedeki, üçüncü ülkedeki ve varsa verilerin aktarıldığı son ülkedeki durum dikkate alınmalıdır[410].

Ayrıca, veri sorumlusunun söz konusu riskleri en aza indirgemek için alması gereken ve zorunlu olan ek önlemler olmadığı takdirde ilgili kişinin menfaatleri veya hak ve özgürlükleri veri sorumlusunun menfaatlerinden her zaman baskın olacaktır[411]. Bu önlemler, aktarımdan sonra en kısa sürede ilgili verilerin silinmesine veya verilerin işleme amaçlarını sınırlandırmaya yönelik önlemler, verilerin şifrelenerek aktarılması, veri işleme amaçları haricinde verilerin kullanılmasına yönelik teknik ve operasyonel önlemler olabilir[412]. Veri sorumlusunun veri aktarımına ilişkin ilgili ulusal denetim makamını bilgilendirmesi gerekir. Ayrıca veri sorumlusu, ilgili kişiye GDPR m.13 ve m.14'de yer alan ilgili bilgilerin sağlanmasına ilaveten aktarım ve gözetilen zorlayıcı meşru menfaatler hakkında da ilgili kişiyi bilgilendirmelidir. GDPR m.49(6)'ya göre veri sorumlusu veya veri işleyen, söz konusu değerlendirmeyi ve uygun güvenceleri m.30'da atıf yapılan kayıtlarla belgelemelidir.

İstisnalar arasında yer alan açık rıza alınması şartlarının zorlayıcı olması ve diğer istisnaların kapsamının sınırlı olması veri sorumluları için bu istisnanın kullanımını daha uygun kılmaktadır[413]. Ancak kişisel verilerin aktarılmasında kolaylık sağlanması amacıyla düzenlenen bu istisnanın kullanımının hükümde yer alan koşullar sebebiyle oldukça kısıtlanmış olduğu görülmektedir[414].

[410] GDPR Gerekçe 113.
[411] EDPB, "Guidelines 2/2018", s.16.
[412] EDPB, "Guidelines 2/2018", s.16.
[413] Theodorakis, s.47.
[414] Kuner, Bygrave ve Docksey, *GDPR: A Commentary*, s.853.

3 KİŞİSEL VERİ AKTARIMINA İLİŞKİN DİĞER ÖNEMLİ HUSUSLAR

3.1 Birlik Yasası Kapsamında Yetkilendirilmemiş Aktarım veya Bilgilendirmeler

Kişisel verilerin aktarılmasında dikkate alınması gereken ve yeni bir hüküm olan GDPR m.48 ve Gerekçe 115, üçüncü ülke mahkemelerinin ya da idarî makamlarının kararları ile veri sorumlusu veya veri işleyenden kişisel verilerin aktarılmasının veya ifşa edilmesinin talep edildiği durumlarda, GDPR 5. Bölümde yer alan aktarımlara ilişkin diğer gerekçelere halel gelmeksizin, söz konusu taleplerin yalnızca talepte bulunan üçüncü ülke ile AB veya AB üye ülkeleri arasında yürürlükte olan MLAT gibi uluslararası bir anlaşmanın mevcut olduğu durumlarda tanınabileceği veya uygulanabileceği belirtilmiştir. Hükümde bahsedilen MLAT'lerin yanı sıra ticari veya hukuki davalarda yurtdışında kanıt elde etmeye ilişkin düzenlenmiş Lahey Delil Sözleşmesi[415] (*Hague Evidence Convention*), Avrupa Konseyi Siber Suç Sözleşmesi[416] ve AB-ABD Şemsiye Anlaşması[417] (*EU-US Umbrella Agreement*) söz konusu uluslararası anlaşmalara örnek verilebilir. GDPR Gerekçe 115'de uluslararası anlaşmaların olmadığı durumlarda, söz konusu taleplerin üçüncü ülke hukukunun ülke dışında uygulanması durumuna yol açacağı, bununda GDPR'ın amaçladığı gerçek kişilerin korunmasına engel olabileceği belirtilmiştir.

[415] Bkz. Hague Evidence Convention, Convention of 18 March 1970 on the Taking of Evidence Abroad in Civil or Commercial Matters, https://www.hcch.net/en/instruments/conventions/full-text/?cid=82, Erişim Tarihi: 9.10.2021.

[416] Bkz. Council of Europe, "Convention on Cybercrime", ETS No. 185, https://www.coe.int/en/web/conventions/full-list?module=treaty-detail&treatynum=185, Erişim Tarihi: 9.10.2021.

[417] European Union, "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", [2016] OJ L336/3, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:22016A1210(01)&rid=3, Erişim Tarihi: 9.10.2021.

GDPR m.48'in, üçüncü ülke mahkemelerinin ve idarî makamlarının yargı yetkilerini sınırları dışında kullanması iddialarını kısıtlamak ve üçüncü ülkelerin herhangi bir yasal dayanak olmaksızın kişisel verilerin AB'den aktarılmasını veya bunlara erişimini zorunlu kılan yasal gereklilikleri yoluyla AB Veri Koruma Hukukunun atlatılmasını önlemek amacıyla düzenlendiği görülmektedir[418]. GDPR m.48 ancak bir uluslararası anlaşma mevcut ise üçüncü ülke mahkemelerinin veya idarî makamlarının kararları çerçevesinde aktarımların hukuka uygun olacağını belirtmiş ve böyle bir anlaşmanın mevcut olmaması durumunda 5. Bölümde yer alan diğer yasal gerekçelere dayanarak verilerin aktarılmasına izin vermiştir. Bu anlamda 48. madde, veri koruma koşullarına uyarlanmış ve mutlak olmayan bir "yasak hükmü" *(blocking statute)* olarak yorumlanmaktadır[419]. GDPR m.48'de yer alan "bu bölüm uyarınca diğer transfer gerekçelerine halel getirmeksizin" ifadesi ile bu madde kapsamında kişisel verilerin aktarılmasına izin verilmediği durumlarda aktarım için 5. Bölümde yer alan diğer hükümlerin yasal bir dayanak olabileceği belirtilmiştir. Uygulamada ise 48. maddede yer alan bu ifade bağlamında aktarıma yasal dayanak olarak yalnızca m. 49'da yer alan istisnaların kullanabileceği görülmektedir[420].

GDPR m.48'in ifadesinden üçüncü bir ülkenin idarî makam ve mahkeme kararlarının AB'den üçüncü ülkelere kişisel veri aktarımı için tek başına yasal dayanak olamayacağı anlaşılmaktadır[421]. GDPR Gerekçe 115'e göre, söz konusu kararlara ilişkin aktarımlar sadece GDPR 5. Bölümde belirtilen şartlara uygun olduğu takdirde veya açıklamanın veri sorumlusunun tabi olduğu AB Hukuku ya da üye devlet hukukunda tanınan önemli bir kamu yararının gerektirmesi durumunda yasal olacaktır.

48. maddenin uygulanabilmesi için kişisel verilerin aktarılmasını gerektiren üçüncü ülke mahkeme veya idarî makamları tarafından alınmış bir kararın veri sorumlusu

[418] Kuner, Bygrave ve Docksey, *GDPR: A Commentary*, s.830.
[419] Kuner, Bygrave ve Docksey, *GDPR: A Commentary*, s.830.
[420] Kuner, Bygrave ve Docksey, *GDPR: A Commentary*, s.835.
[421] Theodorakis, s.43.

veya veri işleyene yönlendirilmesi gerekmektedir[422]. Bununla ilgili olarak EDPB'nin görüşünde m.48'in veri sorumlusu ve veri işleyenlere üçüncü ülkelerin mahkeme veya idarî makamlarının kararlarına ilişkin taleplerini yasal bir dayanak mevcut olmadığı takdirde reddetme yükümlülüğü getirdiği ve MLAT gibi uluslararası bir anlaşma varsa, reddedilen talebe ilişkin aktarımlar için üçüncü ülke yetkilisinin söz konusu anlaşmalara yönlendirilmesi gerektiği yer almaktadır[423]. Ancak m.48'de veri sorumlusu ve veri işleyenin bu yükümlülüklerinden bahsedilmemekte, sadece bu tür üçüncü ülke taleplerinin tanınabilir ve uygulanabilir olmadığı yer almaktadır. Bu noktada EDPB'nin yorumu m.48'in anlaşılması açısından önemlidir.

Öte yandan, üçüncü ülke ile Birlik arasında imzalanan bir uluslararası anlaşmanın GDPR m.48 kapsamında veri aktarımına yasal dayanak olabilmesi için bu anlaşmanın TFEU'nun V. Başlığı çerçevesinde yapılmış uluslararası bir anlaşma olması, AB Hukuku kapsamına girmesi ve bağlayıcı olması gerekmektedir[424]. Ayrıca, uluslararası anlaşmanın yargı kararlarının tanınması ve uygulanmasına uygun olarak düzenlenmiş olması gerekmektedir. 48. maddede bahsi geçen karşılıklı adli yardımlaşma anlaşmaları, GDPR kapsamı dışında kalan ve kolluk kuvvetleri arasındaki veri aktarımlarını kapsayan anlaşmalardır. Bu çerçevede, GDPR 5. Bölümde yer alan veri aktarımına ilişkin bir hükmün aktarım için yasal dayanak olarak GDPR kapsamına girmeyen bir anlaşmaya atıf yapması GDPR'ın çelişkisi olarak yorumlanmaktadır[425].

[422] Bu çerçevede Snowden ifşaatları ile gündeme gelen yaygın hükümet elektronik gözetimi 48. madde kapsamına girmeyecektir, çünkü söz konusu gözetim üçüncü ülke makamlarının veri sorumlusu veya işleyenlerden verileri aktarmasını ve bir emrin AB'de tanınmasını veya uygulanmasını istemeden verilere erişmeyi içerir. Bkz. Kuner, Bygrave ve Docksey, *GDPR: A Commentary*, s.834.
[423] EDPB, "Guidelines 2/2018", s.5.
[424] Kuner, Bygrave ve Docksey, *GDPR: A Commentary*, s.834.
[425] Kuner, Bygrave ve Docksey, *GDPR: A Commentary*, s.831.

3.2 Uluslararası Anlaşmalara Dayalı Aktarımlar

Kişisel verilerin belirli bir amaç için üçüncü ülkelere aktarılması kapsamında AB ile üçüncü ülkeler arasında uluslararası anlaşmalar yapılabilir. GDPR'da kişisel verilerin üçüncü ülkelere aktarılmasına ilişkin aktarım mekanizmaları 5. Bölümde düzenlenmiş, ancak uluslararası anlaşmalar bu mekanizmalara açık bir şekilde dâhil edilmemiştir[426]. GDPR Gerekçe 102'de, GDPR veya AB Hukukunun diğer hükümlerini etkilemediği ve bireylerin temel hak ve özgürlüklerinin korunmasını sağlamak için uygun güvenlik önlemlerini içerdiği takdirde, üye devletlerin kişisel verilerin üçüncü ülkelere veya uluslararası kuruluşlara aktarılmasını içeren uluslararası anlaşmalar akdedebileceği yer almaktadır. Söz konusu gerekçeye göre GDPR, kişisel verilerin aktarımına ilişkin Birlik ve üçüncü ülkeler arasında düzenlenen bu uluslararası anlaşmalara halel getirmez.

GDPR Gerekçe 102'de yer alan bu ifade çerçevesinde uluslararası veri aktarımı için AB Hukuku kapsamında AB ve üçüncü ülkeler arasında bazı anlaşmalar düzenlenmiştir. AB ve ABD kanun uygulayıcı makamları arasında alışverişi yapılan kişisel verilerin korunmasına ilişkin tedbirler sağlamaya yönelik[427] AB ve ABD tarafından imzalanan Şemsiye Anlaşması, aktarılan kişisel verilerin korunmasına yönelik Terör Finansmanı Takip Programı kapsamında ABD ile finansal mesajlaşma verilerinin aktarılmasına ilişkin yapılan anlaşma[428] bu uluslararası anlaşmalara örnek olarak verilebilir. Öte yandan, veri aktarımı için

[426] Siyuan Chen, "Cross-border Data Transfer After Schrems II: The Globalization of EU Standards of Data Protection Through Adequacy Decisions or Trade Agreements?", Master Thesis, Lund University, Spring 2021 s.39.
[427] European Commission, "Statement by Commissioner Věra Jourová on the European Parliament consent vote on the conclusion of the EU-U.S. data protection "Umbrella Agreement", 1 December 2016, https://ec.europa.eu/commission/presscorner/detail/en/STATEMENT_16_4182, Erişim Tarihi: 9.10.2021.
[428] Bkz. Council Decision 2010/412/ of 13 July 2010 on the conclusion of the 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 the purposes of the Terrorist Finance Tracking Program 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 the purposes of the Terrorist Finance Tracking Program. [2010] OJ L195/3, EUR-Lex - 32010D0412 - EN - EUR-Lex (europa.eu), Erişim Tarihi: 16.10.2021.

uluslararası anlaşmaların yanında OECD Gizlilik İlkeleri[429] ve APEC Sınır Ötesi Gizlilik Kuralları[430] gibi uluslararası veri aktarımını ilgilendiren ancak yasal olarak bağlayıcı olmayan başka önemli uluslararası belgeler de bulunmaktadır.

Uluslararası veri aktarımıyla ilgili çok taraflı en önemli anlaşma ise Avrupa Konseyinin 108 Sayılı Sözleşmesidir[431]. Bağlayıcılığı uluslararası anlamda kabul gören tek anlaşma olan 108 Sayılı Sözleşme, 1970'li yıllardan itibaren Avrupa Konseyinin yapmış olduğu çalışmalar neticesinde 1 Ekim 1985 tarihinde yürürlüğe girmiştir. Bugün 108 Sayılı Sözleşme 55 ülke tarafından imzalanmış ve onaylamış olmakla birlikte AB üye ülkelerinin tamamı 108 Sayılı Sözleşme'ye taraftır[432]. 108 Sayılı Sözleşme'nin kişisel verilerin aktarımına ilişkin 12. maddesinde, münhasıran, mahremiyetin korunması için sözleşmeye taraf bir ülkenin diğer bir taraf ülkeye kişisel verilerin aktarılmasını yasaklayamayacağı veya özel izne tabii tutamayacağı yer almaktadır. İlaveten, taraf olmayan bir ülkeye verilerin aktarılabilmesi için ilgili ülkenin yeterli koruma sağlaması gerektiği sözleşmede belirtilmiştir. 108 Sayılı Sözleşme ile GDPR arasındaki uluslararası kişisel veri aktarımına dair ilişki GDPR Gerekçe 105'de yer almaktadır. Söz konusu gerekçede, GDPR kapsamında üçüncü bir ülkeye yönelik yeterlilik kararı alınırken ilgili ülkelerin 108 Sayılı Sözleşme'ye katılımının özellikle dikkate alınacağı vurgulanmıştır.

Uluslararası veri aktarımına ilişkin ilave hükümler içeren 181 Sayılı Ek Protokol[433]

---

[429] Bkz. Organisation For Economic Co-Operation and Development (OECD), "The OECD Privacy Framework (2013)", https://www.oecd.org/sti/ieconomy/privacy-guidelines.htm, Erişim Tarihi: 9.10.2021.

[430] Bkz. Asia Pacific Economic Cooperation (APEC), "Privacy Framework" (2005), https://www.apec.org/publications/2005/12/apec-privacy-framework, Erişim Tarihi: 9.10.2021.

[431] Bkz. Council of Europe, "Convention for the protection of individuals with regard to automatic processing of personal data", ETS No.108, https://rm.coe.int/16808ade9d, Erişim Tarihi: 9.10.2021.

[432] Sözleşmeye taraf olan ülkelerin güncel listesi için bkz. https://www.coe.int/en/web/conventions/full-list?module=signatures-by-treaty&treatynum=108, Erişim Tarihi: 9.10.2021.

[433] Ek protokol için bkz. 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", ETS No.181, https://rm.coe.int/1680080626; Protokole taraf olan ülkelerin güncel listesi için bkz. https://www.coe.int/en/web/conventions/full-list?module=treaty-detail&treatynum=181, Erişim Tarihi: 9.10.2021.

ise 108 Sayılı Sözleşme'nin ayrılmaz bir parçasıdır. 108 Sayılı Sözleşme ve 181 Sayılı Ek Protokol'e göre, taraf ülkeler arasında aktarımın yapılacağı ülkede yeterli korumanın olup olmadığına bakılmadan veya özel bir izin gerekmeden veri aktarımı yapılabilecek olup, taraf olmayan ülkelere aktarımlar için ise izin gerekmektedir. Dolayısıyla taraf olmayan ülkeler veri koruma otoriteleri tarafından ilan edilen yeterli korumanın bulunduğu ülkeler listesine göre değerlendirilebilecektir.

2018 yılında modernize edilen 108 Sayılı Sözleşme[434] ("Sözleşme 108+") taraf devletler tarafından uluslararası düzeyde uygulanmak üzere ve kişisel verilerin korunmasına ilişkin kuralların güncellenerek daha yüksek bir koruma seviyesine sahip olunması amacıyla hazırlanmıştır. Sözleşme 108+ m.14(1)'de sadece kişisel verilerin korunması amacıyla taraf devletlerin aralarında yapacağı aktarımlarda kişisel verilerin aktarımının yasaklanamayacağı veya özel bir izne tabi tutulamayacağı yer almaktadır.

Kişisel veri aktarımını ele alan bir diğer uluslararası anlaşma örneği de PNR anlaşmalarıdır. PNR, yolcuların isimleri, seyahat süreleri, tarih ve planları ve ödeme yöntemleri gibi operasyonel işlemler için hava yolları tarafından yolculardan alınan bilgileri içermektedir. Dolayısıyla, PNR'ın kişisel verileri içermiş olması PNR anlaşmasının kişisel verilerin korunması ile ilgili olduğunu göstermektedir. Pek çok ülke, terörle mücadele ve güvenlik endişeleri sebebiyle PNR'ın paylaşımını kapsayan anlaşmalar imzalamaktadır. AB de terör suçlarını veya ciddi uluslararası suçları önlemek, tespit etmek, araştırmak ve kovuşturmak için PNR'ın diğer üçüncü ülkelerdeki yetkili makamlara aktarılmasına ilişkin Avustralya[435], Kanada[436] ve

[434] Council of Europe, "Modernised Convention for the Protection of Individuals with Regard to the Processing of Personal Data", https://rm.coe.int/convention-108-convention-for-the-protection-of-individuals-with-regar/16808b36f1, Erişim Tarihi: 9.10.2021.
[435] European Union, "Agreement between the European Union and Australia on the processing and transfer of Passenger Name Record (PNR) data by air carriers to the Australian Customs and Border Protection Service", OJ L 186, 14.7.2012, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A22012A0714%2801%29, Erişim Tarihi: 12.10.2021.
[436] European Union, "Agreement between the European Community and the Government of Canada on the processing of Advance Passenger Information and Passenger Name Record data",

ABD[437] ile anlaşmalar yapılmıştır. Buna ek olarak, 2016 yılında EU-PNR Direktifi[438] olarak bilinen 2016/861 sayılı Direktif yayınlamıştır. Söz konusu Direktif, AB üye ülkelerinin, terör suçlarını ve ciddi suçları önlemek, tespit etmek, soruşturmak veya kovuşturmak için PNR bilgilerini üçüncü ülkelerdeki yetkili makamlara aktarmalarına yasal bir dayanak oluşturmaktadır.

Öte yandan, 2019 yılında Alman Sivil Haklar Derneği (*German Society for Civil Rights* – "GFF"), EU-PNR Direktifinin kişisel verilerin korunması ve özel hayata saygı hakkını ihlal ettiği gerekçesiyle, Alman ve Avusturya mahkemeleri önünde direktife karşı yasal işlem başlatmıştır. Bunun neticesinde Ocak 2020'de Almanya Köln Bölge Mahkemesi, söz konusu direktif ve Alman uygulama yasasının özellikle Şart başta olmak üzere AB Hukuku ile uyumlu olup olmadığı sorusu ile davayı ön karar için ABAD'a havale etmiştir. Yaşanan bu gelişme, yolcu verilerinin toplu olarak işlenmesini sona erdirmeye yönelik önemli bir adım olarak değerlendirilmektedir[439]. Nitekim ABAD'ın daha önce almış olduğu kararlara bakıldığında, EU-PNR Direktifini geçersiz kılması muhtemeldir.

Avrupa Komisyonu, 6 Eylül 2005'de 95/46 sayılı Direktif m.25 uyarınca Kanada Gümrük Sınır Hizmetleri Ajansı'nın AB'den Kanada'ya yapılan uçuşlarda, PNR verilerinin aktarımı için yeterli düzeyde koruma sağladığını tespit eden bir yeterlilik kararını kabul etti. Ardından, 2006 yılında AB ve Kanada arasında, PNR verilerinin işlenmesine ilişkin bir anlaşma imzalandı. Söz konusu yeterlilik kararının ve AB-Kanada PNR anlaşmasının 2009'da geçerliliğinin sona ermesinin

---

OJ L 82, 21.3.2006, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A22006A0321%2801%29, Erişim Tarihi: 9.10.2021.

[437] European Union, "Agreement between the United States of America and the European Union on the use and transfer of passenger name records to the United States Department of Homeland Security", OJ L 215, 11.8.2012, https://eur-lex.europa.eu/legalcontent/EN/TXT/?uri=CELEX%3A22012A0811%2801%29&qid=1638794233250, Erişim Tarihi: 12.10.2021.

[438] Directive (EU) 2016/681 of the European Parliament and of the Council of 27 April 2016 on the use of passenger name record (PNR) data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime, OJ 2016 L 119/132. https://eur-lex.europa.eu/eli/dir/2016/681/oj, Erişim Tarihi: 12.10.2021.

[439] Bkz. https://www.liberties.eu/en/stories/european-court-of-justice-to-decide-on-pnr-directive/18148, Erişim Tarihi: 08.01.2022

ardından AB ve Kanada, PNR verilerinin işlenmesi ve AB'den Kanada'ya aktarılması için 25 Haziran 2014'te yeni bir taslak anlaşma üzerinde anlaştılar. Ardından Avrupa Konseyi taslak anlaşma için Avrupa Parlamentosu'ndan onay istedi. Avrupa Parlamentosu onay vermeden önce AB Hukuku ve Şart'ın 7, 8 ve 52(1) maddeleri kapsamında anlaşmanın uygunluğuna ilişkin ABAD'dan görüş talebinde bulundu. Nihai durumda ABAD, 26 Temmuz 2017'de yayınladığı AB-Kanada taslak PNR anlaşmasına ilişkin 1/15 sayılı görüşünde (Opinion 1/15)[440], AB ile Kanada arasında PNR verilerinin aktarımını içeren taslak anlaşmanın hükümlerinin birçoğunun Şart ile uyumsuz olduğunu ve mevcut haliyle sonuçlandırılamayacağını tespit ederek anlaşmanın güncellenmesi gerektiğini ifade etmiştir. ABAD'ın söz konusu görüşü, bir uluslararası anlaşmanın Şart ile uyumluluğuna ilişkin alınmış ilk karar olup AB Hukuku açısından önemli sonuçları bulunmaktadır.

ABAD, 1/15 sayılı görüşünde ilk olarak uluslararası bir anlaşmanın AB'nin anlaşmaları ve bunların dayandığı anayasal ilkelerle uyumlu olması gerektiğini ifade etmiş[441] ve söz konusu taslak PNR anlaşmasının AB Hukukunun temel gerekliliklerine uygun olmadığını belirtmiştir. Mahkeme, anlaşmada öngörülen hükümler ile PNR verilerinin AB'den Kanada'ya aktarılmasının, Şartın 7. maddesi uyarınca özel hayata saygı ve 8. maddesi uyarınca kişisel verilerin korunmasına ilişkin temel haklara müdahaleyi gerektireceğini tespit etmiştir[442]. ABAD, PNR verilerinin işlenmesinin hava taşıyıcıları tarafından toplandığından farklı bir amaç izlediğini ve bu sebeple PNR verilerinin işlenmesinin yolcuların ayrı onayını veya kanunla belirlenen diğer meşru dayanakları gerektirdiğini tespit etti[443]. Mahkeme, PNR verilerinin bir kişinin hassas içerikli (ırk, din, dil, sağlık, cinsel yaşam) bilgilerini de içerebilecek önemli bilgilere sahip olabileceğini ve bu çerçevede bu verilerin aktarımını engelleyecek hüküm içermediği için anlaşma metninin Şart'ın

[440] Court of Justice Of European Union (CJEU), *Opinion 1/15 of the Court of Justice (Grand Chamber)*, ECLI:EU: C:2017:592, 26 July 2017.
[441] CJEU, *Opinion 1/15*, para. 67.
[442] CJEU, *Opinion 1/15*, para. 125, 126.
[443] CJEU, *Opinion 1/15*, para. 143.

7, 8, 21[444] ve 52. maddelerine uygun olmadığını tespit etmiştir[445]. Hassas verilerin ayrımcılık yapmama ilkesi için bir risk oluşturduğunu ve bu nedenle söz konusu bilgilerin aktarılması ve işlenmesinin kamu güvenliği ve ciddi suçlarla mücadele dışında kesin ve sağlam bir gerekçelendirme gerektiğini belirtmiştir[446]. Bu anlamda ABAD, hangi kişisel veri kategorilerinin işlenebileceğinin anlaşmada kesin olarak belirtilmesinin ve hassas kişisel veri kategorileri için yeterli korumanın sağlanmasının önemli olduğunu vurgulamıştır[447].

ABAD görüşünde, anlaşmada yer alan birden fazla hükmün, Şart'ın 7 ve 8. maddeleri kapsamında orantılı olmadığı ve Şart'ın 52. maddesi gereğince kesinlikle gerekli olanla sınırlı olmadıkları için gizlilik ve veri koruma haklarına müdahale ettiğini ifade etmiştir[448]. Mahkemeye göre anlaşma, PNR bilgilerinin diğer yetkililere ifşa edilmesi ve amacı haricinde kullanılmasına ilişkin özel şartlar içermeli ve PNR bilgilerinin saklanması, terörizm ve uluslararası suçlar bakımından oluşacak risk için nesnel kanıtlar ile sınırlı olmalıdır[449].

ABAD, PNR bilgilerinin Kanada tarafından üçüncü ülke yetkililerine ifşa edilmesi kapsamında esasen eşdeğer koruma düzeyinin, ya AB ile üçüncü ülke arasında yapılan uluslararası anlaşma ya da Komisyon'un aldığı bir yeterlilik kararı ile sağlanabileceğini ifade etmiştir[450]. Böylece, Schrems I'de belirttiği üçüncü ülkelere veri aktarımlarında AB Hukukuna esasen eşdeğer bir koruma düzeyinin gerekli olduğunu tekrar etmiş ve bu gerekliliğin Kanada'ya PNR aktarımlarını da kapsadığına karar vermiştir[451]. Buna göre bu tür anlaşmalar Schrems I'de yer alan AB Hukuku ile eşdeğerlilik standardını ve özellikle AB birincil hukukunu

[444] Ayrımcılık yapmama ilkesini düzenleyen Şart'ın 21. maddesine göre " *Cinsiyet, ırk, renk, etnik veya sosyal köken, genetik özellikler, dil, din veya inanç, siyasi veya diğer her türlü düşünce, bir ulusal azınlığa mensubiyet, servet, doğum, sakatlık, yaş veya cinsel eğilime dayalı her türlü ayrımcılık yasaktır*".
[445] CJEU, *Opinion 1/15*, para. 165.
[446] CJEU, *Opinion 1/15*, para. 165.
[447] CJEU, *Opinion 1/15*, para. 141.
[448] CJEU, *Opinion 1/15*, para. 181, 206 ve 217.
[449] CJEU, *Opinion 1/15*, para.232(d).
[450] CJEU, *Opinion 1/15*, para. 214.
[451] CJEU, *Opinion 1/15*, para. 134, 214.

oluşturan Şart'ın gerekliliklerini karşılamalıdır[452]. Bu bağlamda ABAD'ın 1/15 sayılı görüşünde, ilk defa uluslararası anlaşmaların uluslararası veri aktarımlarına yasal bir dayanak olabileceğini tespit etmiş[453] ve bu dayanağın kullanılabilmesinin koşullarını ortaya koymuştur[454].

Diğer bir PNR anlaşması ise 2004 yılında AB ve ABD arasında imzalanan ve PNR verilerinin ABD Gümrük ve Sınır Koruma Bürosu'na (US Bureau of Customs and Border Protection –"CBP") aktarılabilmesine ilişkin düzenlenen PNR Anlaşmasıdır[455]. 11 Eylül 2001 terör saldırılarından sonra ABD, ABD'li yetkililerin, ABD topraklarına, ABD topraklarından veya bu topraklar üzerinden gerçekleşen uçuşlardaki yolcuların PNR verilerine erişebilmesini sağlayan bir yasa çıkardı. Komisyon, bu yasanın AB mevzuatıyla çelişmesi düşüncesine istinaden ABD makamları ile yaptığı müzakereler neticesinde AB'den ABD'ye aktarılan PNR verileri için yeterli düzeyde koruma sağladığına karar veren bir yeterlilik kararını kabul etti. Bu kararın ardından Avrupa Konseyi, AB ile ABD PNR anlaşmasının imzalanmasını onaylayan bir kararı kabul etti ve 28 Mayıs 2004 tarihinde anlaşma yürürlüğe girdi.

Avrupa Parlamentosu, söz konusu yeterlilik kararının kabulünün yasal olarak yetkisiz olduğu (ultra vires) ve bu kararın PNR anlaşmasının akdedilmesi için yasal dayanak teşkil etmediği düşüncesiyle ABAD'a dava açmıştır. ABAD, 30 Mayıs 2016 tarihinde verdiği karar ile yeterlilik kararının Direktif kapsamı dışında kalan kamu güvenliği ve kolluk faaliyetlerine dair kişisel verilerin işlenmesi ile ilgili olması sebebiyle kararın Direktif kapsamına girmediği ve kişisel verilerin

[452] Kuner, Bygrave ve Docksey, *GDPR: A Commentary*, s.777.
[453] CJEU, *Opinion 1/15*, para.214.
[454] Christopher Kuner, "Data Protection, Data Transfers, and International Agreements: the CJEU's Opinion 1/15", 26.07.2017, https://verfassungsblog.de/data-protection-data-transfers-and-international-agreements-the-cjeus-opinion-115/, Erişim Tarihi: 14.10.2021.
[455] Bkz. European Union, "Agreement between the European Community and the United States of America on the processing and transfer of PNR data by air carriers to the United States Department of Homeland Security, Bureau of Customs and Border Protection", OJ L 183, 20.5.2004, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A22004A0520%2801%29&qid=1639127925151, Erişim Tarihi: 12.10.2021.

aktarılması gerekliliğinin ABD iç hukukundan kaynaklanması sebepleriyle yeterlilik kararını iptal etmiştir. Ayrıca söz konusu PNR anlaşmasının akdedilmesini onaylayan Avrupa Konseyi kararını ise yeterlilik kararı ile aynı veri aktarımına yani Direktif kapsamı dışında kalan veri işlemlerine ilişkin olduğu gerekçesiyle iptal etmiştir[456].

Bazı durumlarda uluslararası anlaşmalara dayalı aktarımların yeterlilik kararı kapsamında yapılan aktarımlara göre daha uygulanabilir ve uygun çözüm olduğu görülmektedir. Öyle ki, ABAD'ın almış olduğu Schrems I ve II kararı, yeterlilik kararına istinaden yapılan aktarımlarda AB'nin üçüncü ülkelerin veri koruma standardı ile uygun bir ortak zeminde anlaşmak yerine, kendi veri koruma standardı konusundaki tek taraflı gerekliliklerinin, uluslararası veri aktarımı için sürdürülebilir ve küresel düzeyde uygulanabilir bir çözüm sağlama konusunda başarısız olduğunu göstermiştir[457]. Yeterlilik kararı, üçüncü ülkenin koruma düzeyine ilişkin tek taraflı bir tespit yaparken uluslararası anlaşmalar, anlaşmaya taraf olan tüm taraflara uluslararası yükümlülükler yükler. Yeterlilik kararları kapsamında yapılan aktarımlarda, meydana gelebilecek riskleri üstlenmek sadece AB'nin sorumluluğunda olsa da uluslararası anlaşmalar kapsamında üçüncü ülkeler de bu risklere ortak olmaktadır.

Öte yandan, bireylerin kişisel verilerinin korunmasını temel bir hak olarak gören AB ile verilerin korunması hakkına AB'den farklı bakış açısına sahip olan üçüncü ülkeler arasında verilerin aktarımı konusunda anlaşma yapılabilmesinin de kolay olmayacağı görülmektedir. Öyle ki AB'nin dış ilişkilerini ilgilendiren bir konu olan uluslararası anlaşmaların veri koruma kurallarının dâhil ederek müzakere edilmesi zor bir durumdur. Nitekim AB uluslararası anlaşmalarda, kişisel verilerin korunmasını sağlamak için kendi kurallarının benimsenmesini isteyerek her iki

[456] Bkz. European Union, "Agreement between the European Community and the United States of America on the processing and transfer of PNR data by air carriers to the United States Department of Homeland Security, Bureau of Customs and Border Protection", OJ L 183, 20.5.2004, https://curia.europa.eu/en/actu/communiques/cp06/aff/cp060046en.pdf, Erişim Tarihi: 10.10.2021.

[457] Chen, s.38.

tarafça benimsenen ortak bir güvence standardından kaçınmaktadır. Böyle bir durumun oluşmasının altında, muhtemelen üçüncü ülkelerin veri koruma sistemlerinde mahremiyet ve kişisel veri algısının AB'den farklı olması yatmaktadır. PNR anlaşmalarının iptal edilme gerekçeleri de bunlara bağlıdır.

Aslında, kişisel verilerin aktarılmasını içeren hem yeterlilik kararları hem de uluslararası anlaşmalar ABAD tarafından geçersiz kılınarak iptal edilebiliyor. Bunun altında ABAD'ın birçok görüş ve kararında belirttiği, AB'den üçüncü ülkelere veri aktarımında veri korumasının AB'nin birincil hukuku olan TFEU ve Şart ışığında okunması gerekliliği yatmaktadır. Nitekim bu gerekliliği taşıyamayan birçok uluslararası anlaşma ve yeterlilik kararı ABAD tarafından kabul görmemiş veya yürürlüğe girdikten kısa bir süre sonra iptal edilmiştir.

3.3 Üçüncü Ülkelere Veri Aktarımında Kural İhlalleri

Kişisel verilerin üçüncü ülkelere veya uluslararası kuruluşlara aktarılmasına ilişkin GDPR 5. Bölümde yer alan hükümler ihlal edildiğinde uygulanacak cezalar GDPR m.83(5)(c)'de düzenlenmiştir. Söz konusu düzenlemeye göre aktarımlara ilişkin kural ihlali olduğunda, m.83(2) uyarınca 20 milyon Euro'ya kadar veya bir teşebbüs olması durumunda, şirketin bir önceki mali yılında gerçekleşen dünya genelindeki yıllık cirosunun %4'üne kadar (hangisi daha yüksekse yüksek olan bedel kadar) idarî para cezası kesilir. Bu tutarlar GDPR'da yer alan en ağır para cezası düzeyindedir.

95/46 sayılı Direktif kapsamında, aktarımlara ilişkin kural ihlalleri sebebiyle verilecek para cezaları AB üye ülkelerin ulusal yasalarında belirlenen meblağlar kadardı[458]. Etkili bir ulusal yasası olan Almanya'da ihlaller için uygulanan ceza miktarı en fazla 300 Bin Euro'ydu ve bu tutar bile ABD standartlarına göre çok az kalmaktaydı[459]. Direktifin tersine GDPR'da uluslararası kişisel veri aktarımlarına

[458] 95/46 Sayılı Direktif m.24.
[459] Theodorakis, s.48.

ilişkin ihlaller için kesilecek ceza miktarları hükme bağlanmış ve büyük oranda artırılmıştır.

GDPR m.83(1)'e göre her denetim makamı, uluslararası aktarımlarında dâhil olduğu bu maddenin 4, 5 ve 6. fıkralarında yer alan ihlallere ilişkin, bu madde gereğince idarî para cezalarının kesilmesinin her münferit durum için ölçülü, etkili ve caydırıcı olmasını sağlamakla yükümlüdür. Ayrıca, her münferit durum için idarî para cezası kesilip kesilmeyeceği ve her dava için idarî para cezasının tutarı belirlenirken, m.83(2)'de belirtilen koşulların dikkate alınması gerekmektedir.

GDPR yürürlüğe girdiği tarihten itibaren üçüncü ülkelere veri aktarımı ihlallerine ilişkin kesilen bazı önemli cezalar bulunmaktadır[460]. Bu zamana kadar kişisel veri aktarımlarının ihlaline ilişkin verilen en yüksek ceza İspanya ulusal denetim makamı tarafından Vodafone İspanya firmasına verilen idarî para cezasıdır[461]. Söz konusu ceza GDPR m.83(5)(c) uyarınca ve 2.000.000 EUR'su GDPR m.44'ün ihlali sebebiyle verilen toplam 8.150.000 EUR tutarındaki cezadır. Bunun haricinde, Fransa ulusal denetim makamı tarafından Futura Internationale[462] firmasına verilen 500.000 EUR'luk idarî para cezası ve Norveç ulusal denetim makamının Ferde AS[463] firmasına verdiği 496.000 EUR tutarındaki idarî para cezası, GDPR m.44'ün ihlalini de içeren diğer önemli cezalardır.

[460] Bkz. https://www.enforcementtracker.com/, Erişim Tarihi: 12.10.2021.
[461] İspanya Veri Koruma Otoritesi, ilgili kişinin haklarının yeterince korunamaması sebebiyle Vodafone Spain firmasına toplam 8.150.000 EUR idarî para cezası vermiş bu miktarın 2.000.000 EUR'su GDPR m.44'ün ihlali için verilmiştir. Bkz. Agencia İspanola Proteccion Datos (AEPD), https://www.aepd.es/es/documento/ps-00059-2020.pdf, Erişim Tarihi: 23.10.2021.
[462] Fransa Veri Koruma Otoritesi, Fransız ısı yalıtım şirketi Futura Internationale'a aralarında GDPR m.44'ün de bulunduğu GDPR'ın birkaç maddesini ihlal ettiği gerekçesi ile toplam 500.000 EUR para cezası vermiştir. Bkz. https://www.legifrance.gouv.fr/cnil/id/CNILTEXT000039419459/, Erişim Tarihi: 23.10.2021.
[463] Norveç Veri Koruma Otoritesi, Norveçli otoyol ücreti şirketi Ferde AS'nin GDPR'ı ihlal ettiği için 5.000.000 Kron idarî para cezası vermiştir. Cezanın gerekçesi arasında, Çin'e yasa dışı veri aktarımı sebebiyle GDPR m.44'ün ihlal edilmesi de bulunuyordu.
Bkz. https://www.datatilsynet.no/contentassets/7121f4f2de614186bc535823c9da7102/20_01727-3vedtak-om-overtredelsesgebyr---ferde-as.pdf, Erişim Tarihi: 23.11.2021.

4 TÜRK HUKUKU KAPSAMINDA KİŞİSEL VERİLERİN YURTDIŞINA AKTARIMI

4.1 Kişisel Verileri Koruma Kanununda (KVKK) Yurtdışına Aktarımının Genel Çerçevesi

Türkiye için kişisel verilerin[464] korunmasının kanun düzeyinde düzenlenmesi gerekliliği ilk kez 08.03.2001 tarihli Türkiye'nin AB Katılım Ortaklığı Belgesinde yer almıştır[465]. AB Adli İşbirliği Teşkilatı (EUROJUST) ve AB Polis Teşkilatı (EUROPOL) kurumları ile yapılacak olan işbirliği sözleşmelerinde ve AB Vize Muafiyeti Yol Haritası çalışmalarında da Türkiye'nin kişisel verileri koruma düzenlemelerinin AB standartları ile uyumlu olmasının beklendiği ifade edilmiştir[466]. Kişisel verileri koruma konusu Türkiye'nin AB'ye Katılım Ulusal Programına dâhil edilmiş fakat o tarihten 2014 yılına gelinceye kadar Türkiye'de veri korumaya ilişkin herhangi bir düzenleme yapılmamıştır[467]. Öte yandan Türkiye, kişisel verilerin korunması hususunda uluslararası bağlayıcılığa sahip çok taraflı bir sözleşme olan ve 1981 yılında imzaladığı 108 Sayılı Sözleşmeye taraftır. Söz konusu sözleşme, imzalanmasından 35 yıl sonra 2016 yılında onaylanmış ve yürürlüğe girmiştir[468]. 7 Nisan 2016 tarihinde yürürlüğe giren 6698 Sayılı Kişisel Verilerin Korunması Kanunu[469] ("KVKK"), Türkiye'de veri korumasına ilişkin

---

[464] KVKK m.3(d)'ye göre Kişisel veri; "*kimliği belirli veya belirlenebilir gerçek kişiye ilişkin her türlü bilgi"* olarak tanımlanmıştır.

[465] Bkz. Accession Partnership Document for Turkey, "Council Decision of 8 March 2001 on the principles, priorities, intermediate objectives and conditions contained in the Accession Partnership with the Republic of Turkey", 2001/235/EC, https://www.ab.gov.tr/files/AB_Iliskileri/Tur_En_Realitons/Apd/Turkey_APD_2001.pdf, Erişim Tarihi: 9.10.2021; Kızılırmak, "Cross-Border Transfer", s.18.

[466] Berna Akçalı Gür, "Uluslararası Hukuk ve AB Hukuku Boyutuyla Kişisel Verilerin Yurt Dışına Aktarılması", *Marmara Üniversitesi Hukuk Fakültesi Hukuk Araştırmaları Dergisi,* 25/2 (Aralık 2019), s.869.

[467] Kızılırmak, "Cross-Border Transfer", s.18.

[468] Sözleşmeye taraf olan ülkelerin güncel listesi için bkz. https://www.coe.int/en/web/conventions/full-list?module=signatures-by-treaty&treatynum=108, Erişim Tarihi: 01.01.2022.

[469] Kişisel Verilerin Korunması Kanunu, Kanun Numarası: 6698, Kabul Tarihi: 24.03.2016, Resmi Gazete: 7.04.2016/ 29677

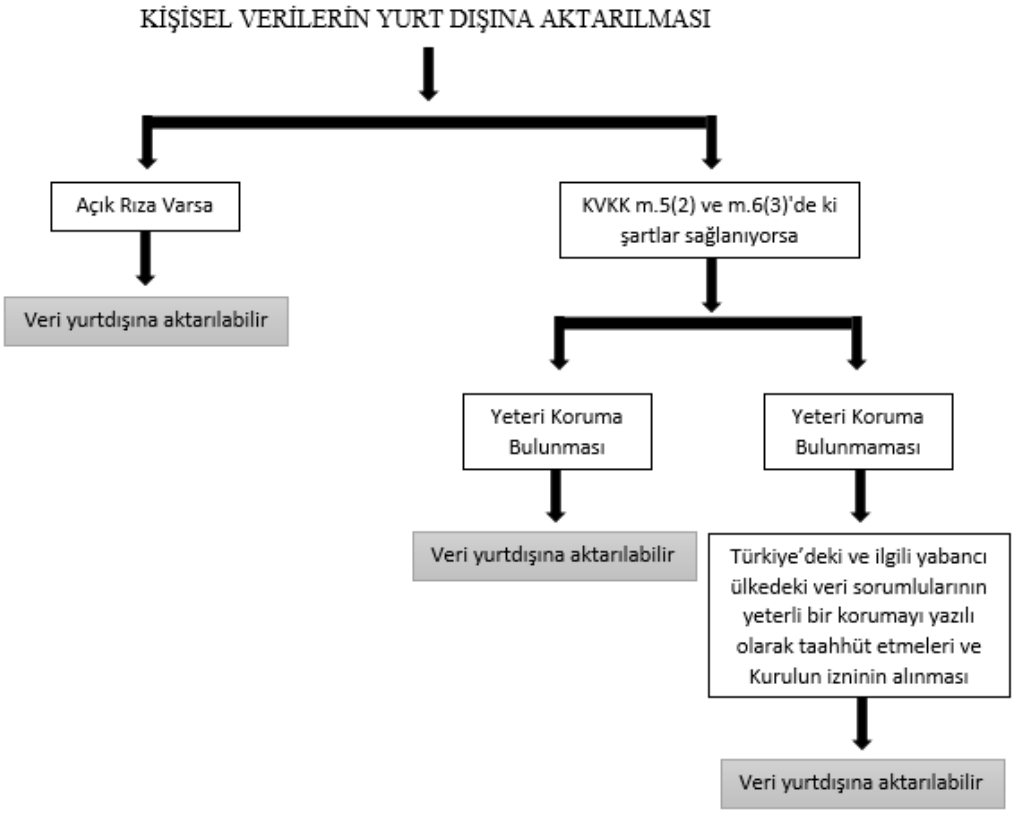
temel hukuki çerçeve olarak düzenlenmiştir[470]. KVKK, 2018 yılında GDPR'ın yürürlüğe girmesinden önce AB'de kişisel verilerin korunması konusunda yürürlükte olan 95/46 sayılı Direktif dikkate alınarak hazırlanmıştır. Ayrıca, KVKK'nın uygulanmasından sorumlu olması amacıyla da Kişisel Verileri Koruma Kurul'u (Kurul) oluşturulmuştur. KVKK, kişilerin özel hayatını, temel hak ve özgürlüklerini korumak amacıyla kişisel verileri işleyen veri sorumluları ve veri işleyenlerin uyması gereken kurallar ve yükümlülükleri düzenleyerek gerçek ve tüzel kişilere hukuki güvence sağlamaktadır[471].

KVKK'nın düzenlenme nedenlerinden birisi de yurtdışına kişisel veri aktarımı konusu olup bu husus KVKK'nın 9. maddesinde düzenlenmiştir. KVKK'da kişisel verilerin yurtdışına aktarılması tanımlanmamış olmakla birlikte Türkiye'den yabancı bir ülkeye kişisel verilerin aktarılması bir kişisel veri işleme faaliyeti olarak kabul edilmektedir[472].

KVKK m.9(1)'de yurtdışına kişisel veri aktarımı ilgili kişinin açık rızası alınmadan gerçekleştirilemeyecek bir işleme faaliyeti olarak belirlenmiştir. Bu hüküm ilgili kişiden açık rıza alınmasının, yurtdışına kişisel verilerin aktarılmasında ana ilke olduğunu göstermektedir. Söz konusu hükme göre ilgili kişinin açık rızası olduğu takdirde yurtdışına kişisel verilerin aktarılması için başka bir şart aranmamaktadır[473]. Ayrıca, KVKK'da yurtdışına aktarım için şart koşulan ilgili kişiden açık rıza alınması hükmü KVKK m.5 ya da m.6 uyarınca kişisel verilerin işlenmesi bakımından öne çıkan bir hukuka uygunluk nedenidir.

[470] Kızılırmak, "Cross-Border Transfer", s.19.
[471] Türkiye Bilişim Derneği, "1. Çalışma Grubu Raporu: Sınır Aşan Veri", *Kamu Bilgi İşlem Merkezleri Yöneticileri Birliği Kamu Bilişim Platformu XXII*, Aralık 2019, s.14.
[472] KVKK m.3(e).
[473] Bilgi IT Law Institute, "Kişisel Verilerin Korunmasına İlişkin Düzenlemeler", s.97.

Şekil 4.1 KVKK'da Kişisel Verilerin Yurtdışına Aktarımı Şeması



Açık rıza KVKK m.3(1)(a)'da "*belirli bir konuya ilişkin, bilgilendirilmeye dayanan ve özgür iradeyle açıklanan rıza*" olarak tanımlanmaktadır. Kişisel Verileri Koruma Kurumu'na ("Kurum") göre kişisel verilerin yurtdışına aktarılması kapsamında m.9'da ifade edilen açık rızanın, m.3(1)(a)'da tanımlanan açık rızada belirtilen özellikleri taşıması gerekmektedir[474].

Kurum tarafından yayımlanan "Açık Rıza Rehberine"[475] göre, veri sorumlusu veya veri işleyen tarafından belirli bir işleme veya aktarım faaliyeti ile sınırlandırılmayan açık rıza geçerli olmayacaktır. Bu nedenle açık rızanın hangi işleme faaliyeti veya

[474] 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*, İstanbul: Onki Levha Yayıncılık, 2020, s.926.
[475] Bkz. KVKK,"Açık Rıza Rehberi", https://kvkk.gov.tr/yayinlar/A%C3%87IK%20RIZA.pdf, Erişim Tarihi: 14.10.2021.

aktarımla ilgili alınacağının veri sorumlusu tarafından belirtilmesi gerekmektedir. Söz konusu rehberde, "kişisel verilerimin aktarılmasını kabul ediyorum" şeklinde verilen açık uçlu bir rızanın açık rıza olarak kabul görmeyeceği belirtilmiştir. Bu kapsamda veri işlenmesinde veya aktarılmasında birden fazla kategori varsa açık rızanın hangi verilerin ne amaçla işleneceği gibi işlemeye ilişkin tüm hususlar açısından verilmesi gerektiği belirtilmiştir. Bunun yanında, veri işleme veya aktarım amaçları değişecekse değişen amaçlar için ve ikincil bir işleme veya aktarım yapılacaksa ikincil işlemler için de ayrıca açık rıza alınması gerekmektedir. Ayrıca, ilgili kişinin[476] özgür bir şekilde açık rıza vermesinin göstergesi olarak, veri sorumlusu tarafından ilgili kişinin hangi konuya rıza verdiği, verilerin hangi amaçla kullanılacağı, verdiği rızanın sonuçlarının ne olacağı ve veri işleme veya aktarımına ait tüm konular hakkında açık ve net bir şekilde bilgilendirilmesi gerekmektedir.

Söz konusu rehbere göre, verilen rızanın geçerli olması için bir diğer koşulun da rıza beyanın özgür iradeyle verilmiş olmasıdır. Bu koşula göre rıza beyanının kişinin kendi verdiği karar ile ve içinde bulunduğu davranışın farkında olarak verilmesi gerekmektedir. Kişinin iradesini engelleyen tehdit, hile ve zorlama gibi hallerde özgür iradeyle karar vererek rıza göstermek mümkün olmamaktadır. İlgili kişi ve veri sorumlusu arasındaki ilişkinin işçi işveren arasındaki ilişki gibi tarafların aynı konumda olmadığı veya birbirinin üzerinde etkiye sahip olduğu durumlarda verilen rızanın özgür iradeyle verilip verilmediğinin dikkatlice incelenmesi gerektiği de rehberde belirtilmiştir. Ayrıca, açık rıza alınması, ilgili kişiye ürün veya hizmet sunulması ya da ilgili kişinin ürün veya hizmetten yararlandırılması için ön şart olarak sunulmamalıdır. İlaveten, ilgili kişinin istediği zaman vermiş olduğu rızayı geri çekme hakkı vardır. İlgili kişi rızayı geri çektiğini veri sorumlusuna bildirdiği andan itibaren geri çekme işlemi geçerli sayılır, yani bu andan itibaren veri işleme veya veri aktarım işlemine son verilmelidir[477].

[476] KVKK m.3 (1)(ç)'de ilgili kişi, kişisel verisi işlenen gerçek kişi olarak tanımlanmıştır.
[477] KVKK, "Açık Rıza Alırken Dikkat Edilecek Hususlar", https://www.kvkk.gov.tr/Icerik/2037/Acik-Riza-Alirken-Dikkat-Edilecek-Hususlar, Erişim Tarihi: 01.01.2022.

Açık rızanın kişisel verilerin işlenmesi veya aktarımından önce alınması gerektiği Kurul tarafından ifade edilmiştir[478]. Açık rızanın alınmasında, gerek KVKK'da gerekse Kurul tarafından herhangi bir şekil şartı belirtilmemiş, açık rızanın yazılı olmasına gerek olmadığı ve elektronik ortamda veya çağrı merkezi vb. yollarla da alınabileceği bildirilmiştir[479]. Açık rızanın alındığına dair ispatlama sorumluluğu veri sorumlusunda olup açık rıza beyanlarının ne kadar süre saklanacağı da makul bir süre olması şartıyla veri sorumluları tarafından belirlenmelidir[480]. Kurum tarafından açık rızanın bir irade beyanı olduğu[481] ve aktif bir hareket ile ifade edilmesi gerektiği[482] belirtilmektedir. Örneğin, internette boş bir kutucuğun işaretlenmesi aktif harekete örnek gösterilebilir, fakat önceden işaretlenmiş kutucuğun kişiye sunulması aktif bir hareket değildir[483].

KVKK'da veri sorumlularına getirilen yükümlülükler arasında, m.10(1)(c)'de veri sorumlusu veya yetkilendirdiği kişinin ilgili kişiyi, işlenen kişisel verilerin kimlere ve hangi amaçla aktarılabileceği konusunda bilgilendirme yükümlülüğü bulunmaktadır. Ayrıca m.11(ç)'de herkesin veri sorumlusuna başvurarak kendisiyle ilgili yurt içinde veya yurt dışında kişisel verilerin aktarıldığı üçüncü kişileri bilme hakkına sahip olduğu düzenlenerek ilgili kişinin bilgilendirilme hakkı belirtilmiştir.

Kişisel verilerin işlenmesi ve yurtdışına aktarılması hususunda ilgili kişinin izninin alınmasının KVKK'da önemli şekilde vurgulandığı görülmektedir. Ayrıca T.C. Anayasası m.20'de de kişisel verilerin işlenmesinin açık rızaya göre

---

[478] Aşıkoğlu ve Uzun, "Kişisel Verilerin Yurtdışına", s.954; Kurul, "Amazon Turkey Perakende Hizmetleri Limited Şirketi hakkındaki başvuru ile ilgili 27.02.2020 Tarihli ve 2020/173 Sayılı Karar Özeti", https://www.kvkk.gov.tr/Icerik/6739/2020-173, Erişim Tarihi: 15.11.2021.
[479] Bkz. KVKK, "Doğru Bilinen Yanlışlar Dokümanı", s.27, https://kvkk.gov.tr/SharedFolderServer/CMSFiles/ca752cda-c3df-4645-8d5e-e2a507e63200.pdf, Erişim Tarihi: 8.10.2021.
[480] KVKK,"Doğru Bilinen Yanlışlar Dokümanı", s.27.
[481] KVKK, "Açık Rıza Rehberi", s.5.
[482] KVKK, "Kişisel Verilerin Korunması Kanunu Hakkında Sıkça Sorulan Sorular", s.23-25, https://www.kvkk.gov.tr/Icerik/4196/Kisisel-Verilerin-Korunmasi-Kanunu-Hakkinda-Sikca-Sorulan-Sorular , Erişim Tarihi: 8.10.2021.
[483] Aşıkoğlu ve Uzun, "Kişisel Verilerin Yurtdışına", s.955.

gerçekleşebileceği belirtilmiştir[484]. Öte yandan, KVKK m.5(1) ve 6(2)'de de açık rıza her zaman diğer kişisel veri işleme şartlarından önce yer almıştır[485].

Yurtdışına veri aktarımını daha az sayıda yapan veya küçük ölçekli şirketlerde açık rıza alınarak yurtdışına veri aktarımı daha kolay gerçekleştirilebilse de büyük ölçekli, sürekli veri aktaran ve yurtdışı ile ilişiği olan şirketlerde, özellikle verilen hizmetlerin yurtdışında bulunan sunucular aracılığıyla yapılması durumunda, açık rıza yönteminin uygulanması pek mümkün olmayabilir[486].

KVKK m.9(2)'de ilgili kişinin açık rızası aranmaksızın yurtdışına aktarılabilmesi için iki seçenek söz konusudur. Bu iki seçeneğin kullanılabilmesi için, özel nitelikli olmayan kişisel verilerin işlenmesi veya aktarılmasına ilişkin KVKK m.5(2)'de[487] yer alan şartlardan ya da özel nitelikli kişisel verilerin işlenmesi veya aktarılmasına ilişkin m.6(3)'te[488] yer alan şartlardan en az birinin mevcut olması gerekmektedir. Söz konusu şartlar, açık rıza aranmaksızın kişisel verilerin işlenmesini öngören

---

[484] Türkiye Cumhuriyeti Anayasası, Kanun Numarası: 2709, Kabul Tarihi: 18.10.1982, Resmi Gazete: 9.11.1982/ 17863.

[485] Aşıkoğlu ve Uzun, "Kişisel Verilerin Yurtdışına", s.934.

[486] Murat Volkan Dülger, "Yurtdışına Veri Aktarımında Milyonluk Ceza: Kişisel Verileri Koruma Kurulunun Amazon Kararı", 24 Şubat 2021, s.2, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3792388, Erişim Tarihi: 13.11.2021.

[487] KVKK m.5(2): "*Aşağıdaki şartlardan birinin varlığı hâlinde, ilgili kişinin açık rızası aranmaksızın kişisel verilerinin işlenmesi mümkündür:*

a) Kanunlarda açıkça öngörülmesi.

b) Fiili 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.

c) Bir sözleşmenin kurulması veya ifasıyla doğrudan doğruya ilgili olması kaydıyla, sözleşmenin taraflarına ait kişisel verilerin işlenmesinin gerekli olması.

ç) Veri sorumlusunun hukuki yükümlülüğünü yerine getirebilmesi için zorunlu olması.

d) İlgili kişinin kendisi tarafından alenileştirilmiş olması.

e) Bir hakkın tesisi, kullanılması veya korunması için veri işlemenin zorunlu olması.

f) İlgili kişinin temel hak ve özgürlüklerine zarar vermemek kaydıyla, veri sorumlusunun meşru menfaatleri için veri işlenmesinin zorunlu olması"

[488] KVKK m.6(3): "*Birinci fıkrada sayılan sağlık ve cinsel hayat dışındaki kişisel veriler (Kişilerin ırkı, etnik kökeni, siyasi düşüncesi, felsefi inancı, dini, mezhebi veya diğer inançları, kılık ve kıyafeti, dernek, vakıf ya da sendika üyeliği, ceza mahkûmiyeti ve güvenlik tedbirleriyle ilgili verileri ile biyometrik ve genetik veriler), kanunlarda öngörülen hâllerde ilgili kişinin açık rızası aranmaksızın işlenebilir. Sağlık ve cinsel hayata ilişkin kişisel veriler ise ancak kamu sağlığının korunması, koruyucu hekimlik, tıbbî teşhis, tedavi ve bakım hizmetlerinin yürütülmesi, sağlık hizmetleri ile finansmanının planlanması ve yönetimi amacıyla, sır saklama yükümlülüğü altında bulunan kişiler veya yetkili kurum ve kuruluşlar tarafından ilgilinin açık rızası aranmaksızın işlenebilir".*

istisnalardır. Maddenin devamında, açık rıza olmadığında sunulan seçenekler ile yurtdışına veri aktarımının hukuka uygun olması için aktarımın gerçekleşmesi mümkün kılınmıştır.

Söz konusu seçeneklerden birincisi m.9(2)(a)'da belirtildiği üzere kişisel verilerin aktarılacağı yabancı ülkede yeterli korumanın bulunmasıdır. Yeterli korumanın bulunduğu ülkeye kişisel veriler aktarılmak istendiğinde ve KVKK m. 5(2)'de veya m.6(3)'te yer alan şartlardan en az birisinin mevcut olması durumda ilgili kişinin açık rızası aranmaksızın kişisel veriler yurtdışına aktarılabilir. Bu yöntem, gerek hakkın korunması gerekse uygulamanın yürütülebilmesi bakımından kişisel verilerin yurtdışına hukuka uygun bir şekilde aktarılabilmesi için, hem aktarım işleminin hukuki bir dayanağının olması hem de aktarımın gerçekleşeceği ülkede kişisel verilerin yeterli bir şekilde korunacağının belirlenmesi açısından en uygun yoldur[489]. KVKK m.9(3)'de ise Kurul tarafından yeterli korumanın olduğu ülkelerin belirlenerek ilan edileceği ifade edilmektedir. Kurul tarafından yeterli koruma sağlandığı ilan edilmeyen tüm ülkelerin yeterli koruma sağlamadığı kabul edilmektedir[490].

Kurul'un 02.05.2019 tarih ve 2019/125 sayılı kararında[491] KVKK m.9(3) ve m.9(4) hükümlerine istinaden yeterli korumanın bulunduğu ülkelerin belirlenmesinde kullanılacak form ve esas alınacak kıstaslar açıklanmış olmasına rağmen, Kurul tarafından KVKK'nın yürürlüğe girmesinden bu zamana kadar geçen sürede yeterli korumanın bulunduğu ülkeler ilan edilmediğinden yurtdışına veri aktarımlarında bu seçenek henüz kullanılamamıştır. Yeterli korumanın bulunduğu ülkelerin henüz

[489] Murat Volkan Dülger, "Kişisel Verileri Koruma Kurulu'nun 108 Sayılı Sözleşme Hakkındaki Kararı ve Yurt Dışına Veri Aktarımı Sorunu", 24 Şubat 2021, s.3, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3792396, Erişim Tarihi: 20.11.2021.
[490] Aşıkoğlu ve Uzun, "Kişisel Verilerin Yurtdışına", s.927.
[491] Kurul'un "Yeterli korumanın bulunduğu ülkelerin tayininde kullanılmak üzere oluşturulan form" hakkında 02.05.2019 tarihli ve 2019/125 sayılı Kararı için bkz. https://www.kvkk.gov.tr/Icerik/5469/-Yeterli-korumanin-bulundugu-ulkelerin-tayininde-kullanilmak-uzere-olusturulan-form-hakkindaki-02-05-2019-tarihli-ve-2019-125-sayili-Kurul-Karari, Erişim Tarihi: 13.10.2021.

açıklanmamış olması, ticari olarak olası yatırımcılar açısından ülkede yatırım yapılması yönünde olumsuz bir etken olmaktadır[492].

Kişisel verilerin yurtdışına aktarılmasında bir diğer seçenek ise m.9(2)(b)'de belirtilmiş olup hükme göre verilerin aktarılacağı ülkede yeterli korumanın bulunmaması durumunda, KVKK m.5(2) ve m.6(3)'de yer alan şartlardan en az birinin var olması, Türkiye'deki ve ilgili yabancı ülkedeki veri sorumlularının yeterli bir korumayı yazılı olarak taahhüt etmeleri ve Kurul'un izninin bulunması şartlarının hepsi var olduğu takdirde ilgili kişinin açık rızası aranmaksızın kişisel veriler yurt dışına aktarılabilmektedir. Ayrıca, söz konusu taahhüdün sadece Türkiye ve yurtdışında yerleşik veri sorumluları tarafından verilmesi gerektiği belirtilse de, Kurul daha sonra bu taahhüdü veri sorumlusundan veri işleyene kişisel veri aktarımlarında da geçerli olmak üzere genişletmiştir[493].

Taahhütnamenin ve taahhütname ekinde yer alması gereken bilgi ve belgelerin aktarımın yapılacağı veri sorumlusu veya veri işleyenden eksiksiz olarak temin edilmesi gerekmektedir. Yurtdışına kişisel veri aktarım süreçleri farklı olan veri sorumluları tarafından taahhütname ve ekinin kısa bir sürede hazırlanamayacağı düşünülmektedir [494]. Ayrıca taahhütname onay ve izin süreçlerinin uzun sürmesi ayrı bir zorluk olarak görülmektedir.

Kurum, ilk yöntem olan taahhütnameler için veri sorumlusundan veri sorumlusuna ve veri sorumlusundan veri işleyene aktarım olmak üzere iki taahhütname yayımlamıştır[495]. Bu belgelerde, hem verileri aktaran hem de verileri alan

---

[492] Türkiye Bilişim Derneği, "Sınır Aşan Veri", s.17.

[493] Kurul'un "Yurt Dışına Kişisel Veri Aktarımında Hazırlanacak Taahhütnamelerde Dikkat Edilmesi Gereken Hususlara İlişkin Duyurusu" için bkz. https://www.kvkk.gov.tr/Icerik/6741/YURT-DISINA-KISISEL-VERI-AKTARIMINDA-HAZIRLANACAK-TAAHHUTNAMELERDE-DIKKAT-EDILMESI-GEREKEN-HUSUSLARA-ILISKIN-DUYURU, Erişim Tarihi: 13.10.2021.

[494] Nilgün Serdar Şimşek, İpek Okucu Taftalı ve Mert Taşkın, "Kişisel Verilerin Korunması Kanunu Kapsamında Yurt Dışına Veri Aktarımlarında Çözümler", https://www.gsghukuk.com/tr/bultenler-yayinlar/makale-yazilar/kisisel-verilerin-korunmasi-kanunu-kapsaminda-yurt-disina-veri-aktarimlarinda-cozumler.html, Erişim Tarihi: 13.10.2021.

[495] Bkz. https://www.kvkk.gov.tr/Icerik/2053/Yurtdisina-Aktarim, Erişim Tarihi: 17.12.2021.

tarafından uyulması gereken veri korunmasına yönelik belirli yükümlülükler bulunmaktadır. Kurul tarafından 16.05.2018 tarihinde, söz konusu taahhütnamelerde bulunması gereken minimum şartlar açıklanmış ve veri sorumlularının yurtdışına veri aktarımını gerçekleştirebilmek için Kurul'dan izin alınmasını şart koşmuştur. Ayrıca, Kurul 07.05.2020 tarihinde yayınladığı "Yurt Dışına Kişisel Veri Aktarımında Hazırlanacak Taahhütnamelerde Dikkat Edilmesi Gereken Hususlara İlişkin Duyuru" ile taahhütname hazırlanırken dikkat edilmesi gereken usul ve esasa ilişkin hususları belirtmiştir. Hâlihazırda Kurul tarafından izin verilen taahhütname sayısı üç olmakla birlikte ilk taahhütname izni KVKK'nın yürürlüğe girmesinden yaklaşık beş yıl sonra 9 Şubat 2021 tarihinde TEB Arval Araç Filo Kiralama A.Ş.'ye verilmiştir. Daha sonra 4 Mart 2021 tarihinde Amazon Turkey ve 22 Haziran 2021 tarihinde Decathlon Türkiye firmalarına da taahhütname izni verilmiştir[496].

Kurul ayrıca, m.9(2)(b)'de bahsedilen Türkiye'de veya ilgili ülkedeki veri sorumlularının yeterli bir korumayı sağladıklarına ilişkin yazılı taahhütlerini, "Taahhütname" veya "Bağlayıcı Şirket Kuralları" aracılığıyla yapılabileceğini bildirmiştir[497]. Kurul 10.04.2020 tarihinde yayınladığı duyuruda, kişisel verilerin yurtdışına aktarılmasına ilişkin veri sorumlusundan veri sorumlusuna veya veri sorumlusundan veri işleyene yönelik taahhütnamelerin, şirketler arasındaki iki taraflı veri aktarılmasını kolaylaştırdığını, fakat bu uygulamanın çok uluslu şirketlerde uygulamada yeterince pratik olmadığını ve yetersiz kaldığını belirtmiştir[498]. Buna istinaden çok uluslu şirketler arasında veri aktarımında kullanılmak üzere başka bir yöntem olan Bağlayıcı Şirket Kurallarının belirlendiğini belirtmiş ve Bağlayıcı Şirket Kurallarını "*yeterli korumanın*

[496] Kurul tarafından izin verilen taahhütnameler için bkz. https://www.kvkk.gov.tr/Search?keyword=taahh%C3%BCtname&langText=tr, Erişim Tarihi: 16.11.2021.
[497] Bkz. KVKK, "Yurtdışına Aktarım", https://www.kvkk.gov.tr/Icerik/2053/Yurtdisina-Aktarim, Erişim Tarihi: 16.11.2021.
[498] Bkz. KVKK, "Bağlayıcı Şirket Kuralları Hakkında Duyuru", https://www.kvkk.gov.tr/Icerik/6728/YURT-DISINA-KISISEL-VERI-AKTARIMINDA-BAGLAYICI-SIRKET-KURALLARI-HAKKINDA-DUYURU, Erişim Tarihi: 16.11.2021.

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 tanımlamıştır[499]. Kurul, "Veri Sorumluları İçin Bağlayıcı Şirket Kuralları Başvuru Formu" ve "Veri Sorumluları İçin Bağlayıcı Şirket Kurallarında Bulunması Gereken Temel Hususlara İlişkin Yardımcı Doküman" yayınlamıştır.

Taahhütnamelerde olduğu gibi Bağlayıcı Şirket Kuralları için de Kurul'a başvuru yapılması ve KVKK m.9(2)(b)'ye göre Kurul'dan izin alınması gerekmektedir. Bağlayıcı Şirket Kuralları, özellikle çok uluslu şirketlerin açık rıza almadan kendi aralarında kişisel verileri aktarabilmelerini sağlamakta ve bu sebeple bu şirketlere kişisel veri aktarımlarında kolaylıklar sunmaktadır. Uygulamada ise, Bağlayıcı Şirket Kurallarını uygulayabilecek kritere haiz çok az sayıda firma olması ve veri sorumlularının büyük çoğunluğunun veri aktarımında bu kuralları kullanamayacak olması sebebiyle, Bağlayıcı Şirket Kurallarının tek başına yeterli düzeyde alternatif bir kişisel veri aktarımı yöntemi sunmadığı söylenebilir[500].

Bağlayıcı Şirket Kuralları kapsamında kişisel veriler grup üyesi şirketlerin haricinde yer alan kişilere aktarılamamaktadır. Grup üyesi şirketlerin dışında yer alan kişilere veri aktarımı yapılacaksa Bağlayıcı Şirket Kuralları yerine taahhütname seçeneğinin kullanılması gerekmektedir[501].

KVKK m.9(4)'de, Kurul'un yabancı ülkede yeterli koruma bulunup bulunmadığına ve m.9(2)(b) uyarınca taahhütnamelere izin verilip verilmeyeceğine ilişkin alacağı kararlarda dikkate alınacak kıstaslar[502] belirtilmiştir. Bu çalışmanın yapıldığı

[499] KVKK, "Bağlayıcı Şirket Kuralları Hakkında Duyuru".
[500] Dülger, "Kişisel Verileri Koruma", s.5-6.
[501] Dülger ve Kahraman, "KVKK'dan Kişisel Verilerin Yurt Dışına", s.5.
[502] KVKK m.9(4) uyarınca, *"Kurul yabancı ülkede yeterli koruma bulunup bulunmadığına ve ikinci fıkranın (b) bendi uyarınca izin verilip verilmeyeceğine;*
a) Türkiye'nin taraf olduğu uluslararası sözleşmeler,
b) Kişisel veri talep eden ülke ile Türkiye arasında veri aktarımına ilişkin karşılıklılık durumu,
c) Her somut kişisel veri aktarımına ilişkin olarak, kişisel verinin niteliği ile işlenme amaç ve süresi,

tarihte, yukarıda da belirtildiği üzere, Kurul tarafından henüz yeterli korumanın sağlandığı ülkeler belirlenmediğinden tüm ülkeler yeterli korumayı sağlamayan ülkeler olarak görülmektedir[503]. Bu durumda, açık rıza alınmadan tüm ülkelere yapılacak kişisel verilerin aktarılmasında m.9(2)(b) hükmüne göre hareket edilmesi gerekecektir.

KVKK m.9(5)'de, uluslararası sözleşme hükümleri saklı kalmak üzere, Türkiye'nin veya ilgili kişinin menfaatinin ciddi bir şekilde zarar göreceği durumlarda, söz konusu kişisel verilerin ancak ilgili kamu kurum veya kuruluşunun görüşü alınarak Kurul izniyle yurt dışına aktarılabileceği düzenlenmiştir[504]. Söz konusu hüküm ile hem ilgili kişinin ve Türkiye'nin menfaatinin zarar görmesini engellemek amacıyla Kurul'un izninin alınması şartı getirilmiş hem de uluslararası sözleşmelerde yer alan hükümlere göre hareket edilebileceği belirtmiştir[505]. Yani, uluslararası bir sözleşme mevcut olduğunda yurtdışına kişisel veri aktarımı söz konusu sözleşmenin hükümlerine istinaden yapılabilmektedir. Öte yandan, uluslararası sözleşme hükümlerinin saklı tutulması ifadesiyle, Türkiye'nin taraf olduğu ve T.C. Anayasası m.90'a[506] göre kanun hükmünde olan, temel hak ve özgürlüklerin korunmasına yönelik düzenlenmiş 108 Sayılı Sözleşme gibi uluslararası sözleşmelerde yer alan hükümlerin kişisel verilerin yurtdışına aktarılmasında hukuki dayanak olduğu ifade edilmektedir. Ancak Kurul, KVKK'nın 22.07.2020 tarih ve 2020/559 sayılı kararında, 108 Sayılı Sözleşmeye taraf olunmasının o ülkenin güvenli ülke olarak belirlenmesi açısından tek başına yeterli olmadığını ve söz konusu sözleşmeye taraf olmanın yalnızca yeterlilik kararı değerlendirmesinde

---

ç) Kişisel verinin aktarılacağı ülkenin konuyla ilgili mevzuatı ve uygulaması,
d) Kişisel verinin aktarılacağı ülkede bulunan veri sorumlusu tarafından taahhüt edilen önlemleri,
değerlendirmek ve ihtiyaç duyması hâlinde, ilgili kurum ve kuruluşların görüşünü de almak suretiyle karar verir".

[503] KVKK, "Madde Ve Gerekçesi İle Kişisel Verilerin Korunması Kanunu (Bilgi Notu) Ve Kişisel Verilerin Korunmasına İlişkin Terimler Sözlüğü", s.26, https://www.kvkk.gov.tr/Icerik/5388/Madde-ve-Gerekcesi-ile-Kisisel-Verilerin-Korunmasi-Kanunu-Bilgi-Notu-ve-Kisisel-Verilerin-Korunmasina-Iliskin-Terimler-Sozlugu, Erişim Tarihi: 13.11.2021.

[504] KVKK m.9(5).

[505] Bilgi IT Law Institute, "Kişisel Verilerin Korunmasına İlişkin Düzenlemeler", s.99.

[506] T.C. Anayasası, m.90.

dikkate alınacak olumlu bir unsur olduğunu belirtmiştir[507]. Bu duruma istinaden Kurul, açık rıza olmadan yurtdışına veri aktarımının, KVKK ile düzenlenen şartlar mevcut olduğunda ve veri sorumluları tarafından yeterli korumanın yazılı olarak taahhüt edilmesi ve Kurul'dan izin alınması durumunda mümkün olabileceğini belirtmektedir[508].

KVKK m.9(6)'da yer alan *"kişisel verilerin yurt dışına aktarılmasına ilişkin diğer kanunlarda yer alan hükümler saklıdır"* ifadesi ile söz konusu hükümlerde yurtdışına veri aktarılması gereken durumlar olduğunda ilgili kişinin açık rızası olmadan veya Kurul'dan izin alınmadan kişisel verilerin yurtdışına aktarılabileceği; bu durumda, söz konusu kanunun dayanak sağladığı aktarımların KVKK'da yer alan durumlardan bağımsız olacağı ve veri aktarımı için yetki verilen kurum ve kuruluşların haricinde Kurul'dan izin alınmasına gerek olmayacağı ileri sürülmektedir[509].

Kişisel verilerin yurtdışına aktarılmasına yönelik birçok uluslararası sözleşme veya belge olsa da 108 Sayılı Sözleşme veri aktarımına ilişkin temel sayılacak bir anlaşmadır. Türkiye, temel hak ve özgürlüklerle ilişkili olan 108 Sayılı Sözleşme ve Sözleşmeye ilişkin Ek Protokol'ü imzalayıp ulusal mevzuatına uyguladığından yurtdışına veri aktarımına ilişkin söz konusu sözleşmede yer alan hükümlerin uygulanması önceliklidir[510]. Ancak yukarda da belirtildiği üzere Kurul bu yorumu benimsememiştir.

KVKK m.15(7)'de, telafi edilmesi zor veya imkânsız zararların oluşması ve hukuka aykırılığın açıkça bulunması durumunda, kişisel verilerin işlenmesinin veya yurtdışına aktarımının durdurulabilmesi Kurul'un yetkisine verilmiştir. KVKK m.12'ye göre veri sorumlusu, kişisel verilerin hukuka aykırı işlenmesini ve verilere

[507] Kurul, "Kişisel verilerin 108 Sayılı Sözleşme dayanak gösterilerek yurt dışına aktarılması hakkında 22.07.2020 tarih ve 2020/559 sayılı Karar Özeti". https://kvkk.gov.tr/Icerik/6790/2020-559. Erişim Tarihi: 15.11.2021.
[508] Dülger, "Kişisel Verileri Koruma", s.12.
[509] Bilgi IT Law Institute, "Kişisel Verilerin Korunmasına İlişkin Düzenlemeler", s.100.
[510] Bilgi IT Law Institute, "Kişisel Verilerin Korunmasına İlişkin Düzenlemeler", s.103.

hukuka aykırı şekilde erişilmesini önlemek ile kişisel verilerin muhafaza edilmesi amacıyla uygun güvenliği sağlamak için her türlü idarî ve teknik önlemi almalıdır. Ayrıca, veri sorumlusu KVKK'nın uygulanması için kendi kurum veya kuruluşunda gerekli denetimleri sağlamak zorundadır. KVKK m.18'e göre m.12'de yer alan bu yükümlülükleri sağlamayanlar hakkında 15.000 Türk lirasından 1.000.000 Türk lirasına kadar idarî para cezası verilir.

Önemli bir ayrıntı olarak, Türkiye'de yerleşik veri sorumlusunun yurtdışına kişisel veri aktarımı için KVKK m.9'da yer alan yükümlülükleri yerine getirmesi gerekirken, yurtdışında yerleşik bir veri sorumlusu Türkiye'de bulunan ilgili kişilerin kişisel verilerini işleme faaliyeti için toplarsa yurtdışına veri aktarılmamış olacağından KVKK m.9'da yer alan yükümlülüklere tabi olmayacaktır[511]. Ancak, yurtdışındaki veri sorumlusunun KVKK kapsamında yer alan ilgili yükümlülüklere uyması ve Veri Sorumluları Siciline (VERBİS) kayıt olması gerekmektedir.

Yurtdışına aktarım konusunda Kurul'un önemli görevleri, KVKK'da m.9(3)'de yer alan yeterli korumanın sağlandığı ülkelere karar vermek ve bu karar için m.9(4)'de yer alan şartların mevcut olup olmadığın kontrol edilmesi, açık rızanın bulunmadığı hallerde m.5(2) ve m.6(3)'de yer alan durumlardan en az birinin mevcut olduğunun tespiti ve m.9(2)(b)'de yer alan taahhüde izin verilmesi ve kişisel verilerin işlenmesini veya yurtdışına aktarımını durdurma yetkisi olarak sayılabilir.

[511] Şimşek, Taftalı ve Taşkın," Kişisel Verilerin Korunması".

4.2 Kişisel Verileri Koruma Kurulunun Güncel Kararları Işığında Sınır Ötesi Aktarım Konusunun Değerlendirilmesi

4.2.1 Amazon Turkey Perakende Hizmetleri Ltd. Şti. Kararı

Kurul, kişisel verilerin yurtdışına aktarılması hususunda KVKK m.9'da yer alan yükümlülükleri sağlamadığı gerekçesiyle 27.02.2020 tarih ve 2020/173 sayılı kararla Amazon Türkiye'ye cezai yaptırımda bulunmuştur.

2016 yılında yürürlüğe girdiğinden itibaren Kurul tarafından yapılan açıklamalar, yayınlanan dokümanlar ve yapılan yasal düzenlemeler ile kişisel verilerin korunması hususunda hemen hemen tüm konulara açıklık getirilmiş fakat yurtdışına veri aktarımı konusunda bazı konular netlik kazanmamıştır[512]. Söz konusu belirsizlikler nedeniyle yurtdışına veri aktarımının hukuka uygun olarak yapılmasının uygulamada pek mümkün olmadığı ve yurtdışına veri aktarımı yapan veri sorumlusuna kurul tarafından cezai yaptırım uygulanmayacağı görüşleri mevcuttu[513]. Ancak Kurul tarafından verilen 27.02.2020 tarih ve 2020/173 sayılı kararla Amazon Turkey Perakende Hizmetleri Limited Şirketine ("Amazon Türkiye") idarî para cezası verilmesi bu belirsizliği netleştirmiştir.

Kurul, söz konusu kararında, başta yurtdışındaki iştiraklerine kişisel veri aktarımı olmak üzere kişisel verilerin korunması, e-ticaret mevzuatı ihlalleri, aydınlatma yükümlülüğünün yerine getirilmemesi ve yurtdışına hukuka aykırı kişisel veri aktarımı nedeniyle Amazon'a toplamda 1.200.000 TL'lik idarî para cezası kesmiştir. Kesilen cezanın daha çok Amazon'un yurtdışına kişisel verilerin aktarılması hususunda KVKK m.9'u ihlal ettiği gerekçesi ile verildiği düşünülmektedir[514]. İdari para cezasının yanında, tespit edilen ihlallere ilişkin bildirim metinlerinin güncellenmesi, söz konusu web sitesi ve ilişkili

[512] Dülger,"Yurtdışına Veri Aktarımında Milyonluk Ceza", s.1.
[513] Dülger,"Yurtdışına Veri Aktarımında Milyonluk Ceza", s.2.
[514] Dülger,"Yurtdışına Veri Aktarımında Milyonluk Ceza", s.8.

uygulamalarında Kanun'a uygun olarak düzenlenmesi ve Kurul'a bu konuda bilgi verilmesine karar verilmiştir[515].

Amazon kararı ile hem KVKK'ya uygun olmayan yurtdışına veri aktarımları için ceza verilmediği anlayışı sona erdirilmiş hem de m.9(2)'de yer alan taahhütnamelerin uygulamaya yönelik belirsizlikleri giderilmiştir[516]. Kurul'a sunulmuş ve onay beklenen taahhütnamelere dayanarak verilerin yurtdışına aktarılamayacağı ve taahhütnamelerin onaya sunulmuş olmasının idarî cezayı hafifletici bir neden olamayacağı konusu taahhütname uygulamasının giderilen belirsizliğidir[517].

Karara konu olan ihbar dilekçesinde, Amazon kullanıcısı tarafından Amazon'un hukuka aykırı veri işleme ve veri aktarımı yaptığına dair şikâyette bulunulmuştur[518]. Bu çalışmada incelenmekte olan kişisel verilerin yurtdışına aktarılması ile ilgili olarak ihbar dilekçesinde yer alan iddiaya göre, Amazon Türkiye'nin amazon.com.tr web sitesinde kişisel verilerin Amazon tarafından yurtdışına aktarılabileceğinin belirtildiği fakat web sitesinde ve bağlantılı olan mobil uygulamalarında, ne üyelik hesabı işlemlerinde ne de ürün veya hizmet satın alınırken kişisel verilerin yurtdışına aktarılmasına yönelik açık rızanın talep edilmediği belirtilmektedir. Bu bağlamda, Amazon yurtdışına aktarım için Kurul'dan taahhütname onayı almamışsa ve ilgili kişiden aktarım için açık rıza da alınmadığından dolayı KVKK m.9'u ihlal etmiş olabileceğine istinaden konunun Kurum tarafından incelenmesi talep edilmiştir. Kısaca, ihbar eden kişinin Amazon'un kişisel verileri yurtdışına aktarabileceğini belirttiğini, fakat açık rıza talep etmediğini ifade ettiği söylenebilir.

---

[515] Kurul,"Amazon Turkey Karar Özeti".
[516] Damla Yılmaz, "Kişisel Verileri Hukuka Uygun Şekilde Yurt Dışına Aktarabilmek Ne Kadar Mümkündür?", 2020 ,https://www.sistemglobal.com.tr/makaleler/kvkk-makaleler/kisisel-verileri-hukuka-uygun-sekilde-yurt-disina-aktarabilmek-ne-kadar-mumkundur/, Erişim Tarihi: 15.11.2021.
[517] Bkz. https://www.sistemglobal.com.tr/makaleler/kvkk-makaleler/kisisel-verileri-hukuka-uygun-sekilde-yurt-disina-aktarabilmek-ne-kadar-mumkundur/, Erişim Tarihi: 15.11.2021.
[518] Bkz. Asylegal, "Uluslararası Veri Aktarımı & KVKK Amazon Türkiye Kararı", https://www.asylegal.com/tr/uluslararasi-veri-aktarimi-kvkk-amazon-turkiye-karari/, Erişim Tarihi: 15.11.2021.

Amazon Türkiye, bu iddiaya karşılık yaptığı savunmada, müşterilerin hesap oluştururken Gizlilik Bildirimine onay vererek söz konusu bildirimde yer alan yurtdışına verilerin aktarılması hususunu kabul ettiğini ve ürün siparişi sırasında Gizlilik Bildiriminin kabul edildiğine dair hatırlatma yapıldığını, ayrıca taahhütnamelere ilişkin olarak Kurum ile görüşmelerin devam ettiğini ifade etmiştir[519]. Kurul tarafından Amazon Türkiye'nin savunmasında yer alan bu ifadelere istinaden yapılan değerlendirmede rızanın zımni (örtülü) irade beyanı ile alınmış olması nedeniyle Kanun'a uygun olmadığına karar verilmiştir[520]. Ayrıca kararda, KVKK'da yer alan açık rızanın, kişinin kişisel verilerinin işlenmesine kendi isteği veya veri sorumlusundan gelen talep üzerine onay verilmesi şeklinde açıklandığı ve açık rızanın ilgili kişinin, işlenmesine izin verdiği kişisel verinin sınırlarını, kapsamını ve süresini de belirlemesini sağlayacağı ifade edilmiştir. Bu çerçevede, bütün işlemler için tek bir rıza verilmesi şeklinde alınan ve "battaniye rıza" olarak tanımlanan bu yöntemin KVKK'da yer alan açık rızanın şartlarına uygun olmadığı belirtilmiştir[521]. Kişisel verilerin yurtdışına aktarılması için açık rıza alınması gerekliliğine rağmen alınan rızanın hukuka uygun olarak alınmaması ve sadece Amazon hizmetleri kullanılarak Gizlilik Bildiriminin kabul edilmiş olması durumu, Kurul'a göre KVKK m.12 kapsamında veri güvenliği yükümlülüklerine uygun değildir[522].

İhbarın ardından Kurul, yaptığı inceleme neticesinde ve Amazon Türkiye'nin savunmasını aldıktan sonra, Amazon Türkiye'nin yurtdışına veri aktarımında ilgili kişilerin açık rızasını almadığını fakat açık rıza almak yerine ilgili kişilere verilerinin üçüncü taraflarla paylaşılmasına ilişkin izin vermeme veya paylaşmaktan vazgeçme hakkı verdiğini ancak ilgili kişilere "vazgeçme" ve "izin vermeme" hakkı sunmanın KVKK m.9'da yer alan açık rıza alınması hükmüne uygun olmadığına hükmetti. Vazgeçme hakkı tanıyarak ilgili kişilerin kişisel

[519] Kurul,"Amazon Turkey Karar Özeti".
[520] Kurul,"Amazon Turkey Karar Özeti".
[521] Kurul,"Amazon Turkey Karar Özeti".
[522] Dülger, "Yurtdışına Veri Aktarımında Milyonluk Ceza", s.9.

verilerinin yurtdışına aktarılmasını kabul etmelerini beklemek yerine ilgili kişilerin aktarımlara açık ve net bir şekilde açık rıza vermesi gerekmektedir[523].

Amazon Türkiye, aktarım öncesinde ilgili kişilerden açık rıza almadığından, yurtdışına yasal olarak veri aktarımını m.5(2) ve m.6(3)'de yer alan istisnalardan en az birinin var olması şartıyla m.9(2) kapsamındaki imkânları kullanarak gerçekleştirebilir. KVKK m.9(2)(b)'de yer alan taahhüt ve Kurul'dan izin alınması hükmüne istinaden veri sorumlusu olan Amazon Türkiye söz konusu taahhütnameyi daha önce Kurul'a iletmişti, fakat hem şikâyetin yapıldığı tarihte hem de kararın açıklandığı tarihte söz konusu taahhütname Kurul tarafından henüz onaylanmamıştı. Amazon'a taahhütname izni ise karardan yaklaşık bir yıl sonra 4 Mart 2021 tarihinde Kurul tarafından verilmiştir[524]. Kurul'un nihai kararına göre bu imkânın kullanılabilmesi için başvuru yapmış olmak yeterli olmamakla birlikte m.9(2)(b)'ye göre taahhütte bulunulması ve Kurul'un izin vermesi şarttır[525]. Kurul'un Amazon Türkiye'nin taahhütnamesini onaylamamış olması dikkate alındığında, Amazon Türkiye tarafından yurtdışına yapılan veri aktarımlarının KVKK'ya uygun olmadığına karar verilmiş ve tek hukuki dayanağın ilgili kişinin açık rızasının alınması olduğu belirtilmiştir[526]. Ayrıca, taahhütnamelerin beklemede olmasının da ceza indirimine sebep olmadığı da görülmektedir[527]. Kurul, hem başvuruda bulunulduğu halde taahhütnameleri sonuçlandırmamış olması hem de kişisel verilerin yurtdışına aktarılması konusunda KVKK'da yer alan imkânların sınırlandırılmış olmasına rağmen kısıtlayıcı bir yaklaşım göstererek Amazon Türkiye'ye ceza vermiştir[528].

Karar, açıklanmasının ardından bazı eleştirilere sebep olmuştur. Bu eleştirilerden birisi Amazon Türkiye'nin kişisel verileri AB ülkelerine aktarmakta olmasıdır. AB

[523] Asylegal, "Uluslararası Veri Aktarımı".
[524] Söz konusu taahhütname izni için bkz. https://www.kvkk.gov.tr/Icerik/6898/TAAHHUTNAME-BASVURUSU-HAKKINDA-DUYURU, Erişim Tarihi: 15.11.2021.
[525] Asylegal, "Uluslararası Veri Aktarımı".
[526] Dülger, "Yurtdışına Veri Aktarımında Milyonluk Ceza", s.9.
[527] Kızılırmak, "Cross-Border Transfer", s.67
[528] Dülger, "Kişisel Verileri Koruma", s.5.

ülkelerinin GDPR'a tabi olması sebebiyle yeterli korumanın bulunduğu ülkeler olarak tanımlanması gerektiği eleştirileri olmuştur[529]. Bir diğer eleştiri ise Amazon Türkiye'nin hâlihazırda taahhütname başvurusunda bulunduğu eleştirileridir. Fakat burada şunu belirtmek gerekir ki KVKK'da açık ve net şekilde belirtilmesine rağmen, Amazon Türkiye ilgili kişilerden açık rıza almamasının yanında taahhütnameler için onay almadan veri aktarımına devam etmiştir. Kurul verdiği kararla bu noktada gayet açık ve net olmuş, yurtdışına aktarım yapmak için ilgili kişilerden açık rıza alınması gerektiğini, açık rıza almadan veri aktarmak istiyorsa yeterli korumanın olduğu ülkelerin açıklanmasını veya taahhütte bulunarak Kurul'un onay vermesinin beklenmesi gerektiğini ifade etmiştir. Buradan anlaşılacağı üzere Kurulun, sürecin KVKK'ya uygun olması için taahhütname başvurunun sonuçlanmasını bekleyerek Amazon Türkiye'ye ek süre verme yolunu da seçmediği görülmektedir[530].

Açık rıza alınması konusuna değinmek gerekirse, Amazon Türkiye gibi uluslararası büyüklükte bir şirketin yurtdışıyla bağlantısı olması sebebiyle gerçekleştirdiği her veri aktarımında ilgili kişiden açık rıza almasının teknik olarak mümkün olup olmadığı akla gelmektedir. Daha az sayıda ve daha az sıklıkta kişisel verileri yurtdışına aktaran küçük şirketlerde açık rıza alınması mümkün olsa da uluslararası olan bir şirket açısından her ilgili kişiden her aktarım için açık rıza alma uygulaması mümkün olmayabilir[531]. Ayrıca, kararın alındığı tarihte kullanılabilir olmayan ve 10.04.2020 tarihinde Kurul tarafından açıklanan Bağlayıcı Şirket Kuralları yönteminin çok uluslu bir şirket olan Amazon Türkiye gibi şirketlerde daha kullanılabilir bir yöntem olduğu söylenebilir.

Verilen karar, KVKK'da yer alan mevcut durum kapsamında uygun görülmekle birlikte bu mevcut durumun veri sorumlularına zorluk çıkardığı da önemli gerçektir. KVKK'nın yürürlüğe girdiği tarihten itibaren bazı belirsizliklerin devam etmesi

[529] Asylegal,"Uluslararası Veri Aktarımı".
[530] Yılmaz, "Kişisel Verileri Hukuka Uygun".
[531] Dülger, "Kişisel Verileri Koruma", s.5.

veri sorumlularının yurtdışına kişisel veri aktarımı yöntemlerini oluşturamamasına sebep olmuştur[532]. Bununla birlikte sadece açık rıza alınıp alınmaması durumu göz önüne alınarak veri sorumlusunun yükümlülüğünü yerine getirmediği düşüncesiyle ihlal kararı vermenin uygun olmadığı düşünülmektedir[533].

4.2.2 22.07.2020 Tarih ve 2020/559 Sayılı Karar

Kurul, otomotiv sektöründe faaliyet gösteren ve veri sorumlusu olan şirketin kişisel verileri yurtdışına aktarırken Kanun'a uygun hareket etmediği gerekçesiyle söz konusu veri sorumlusuna 900.000 TL idarî para cezası vermiştir.

İlgili kişi veri sorumlusu hakkında Kurul'a şikâyette bulunmuştur. Söz konusu şikâyette, "*otomotiv sektöründe faaliyet gösteren veri sorumlusu tarafından reklam/bilgilendirme amaçlı bir kısa mesaj (SMS) gönderilmesi*[534]" yer almaktadır. Şikâyet üzerine Kurul inceleme başlatmış ve veri sorumlusundan savunma talep etmiştir.

Veri sorumlusu yapmış olduğu savunmada, şirketleri tarafından pazarlama amacıyla toplanan kişisel verilerin yurtdışındaki veri işleyene aktarılması ve yalnızca ilgili hizmetin yerine getirilmesi için verilerin işlenmesini, KVKK m.5(2)(f)'de yer alan veri sorumlusunun meşru menfaatleri için veri işlemesinin zorunlu olması durumuna istinaden gerçekleştirdiğini ifade etmiştir. Bununla birlikte, söz konusu savunmada şikâyette bulunan kişi tarafından şirketlerinin veri gizliliği metninin onaylandığı yani söz konusu aktarım için rıza alındığını belirtilmiştir. Savunmada geçen bu iki ifadenin birbiri ile çelişmekte olmasına istinaden Kurul, 08.07.2019 tarih ve 2019/203 sayılı Karar ve KVKK m.15(1) kapsamında resen inceleme başlatılması kararı almış ve yurtdışına kişisel veri

[532] Dülger, "Yurtdışına Veri Aktarımında Milyonluk Ceza", s.9.
[533] Dülger, "Yurtdışına Veri Aktarımında Milyonluk Ceza", s.9.
[534] Kurul," Kişisel verilerin 108 Sayılı Sözleşme dayanak gösterilerek yurt dışına aktarılması hakkında 22.07.2020 tarih ve 2020/559 sayılı Karar Özeti", https://kvkk.gov.tr/Icerik/6790/2020-559, Erişim Tarihi: 15.11.2021.

aktarımının hukuki dayanağının ne olduğuna dair açıklamalar ile konuya ilişkin tüm belge, bilgi ve kayıtları veri sorumlusundan talep etmiştir.

Kurul yapmış olduğu değerlendirmede, veri sorumlusunun savunmasında yer alan KVKK m.5(2)(f)'e göre aktarımın yapılabilmesi için iki aşamalı bir test yapılması ve meşru menfaatin varlığı ile söz konusu menfaatin ilgili kişinin temel hak ve özgürlüklerine zarar verip vermediğinin belirlenmesi gerektiğini ifade etmiştir. Ancak, veri sorumlusunun meşru menfaatinin ne olduğunu açıklamadığı ve menfaat ile temel hak ve özgürlükler arasında bir denge testi uyguladığına dair bilgi vermediği gerekçeleriyle söz konusu aktarımlar için geçerli bir menfaatin oluşmadığına karar vermiştir[535]. Kurul, veri sorumlusunun yurtdışından aldığı bulut hizmetini yerel bir hizmet sağlayıcıdan alma ihtimalinin olması sebebiyle veri sorumlusunun meşru menfaat gerekçesini uygun bulmamıştır[536].

Bu kapsamda, Karar'da da açıklandığı üzere KVKK m.5(2)(f)'de ifade edilen "meşru menfaat"in mevcut olup olmadığı belirlenmeli ve meşru menfaat varsa veri sorumlusu tarafından yapılacak denge testi ile ilgili kişinin temel hak ve özgürlüklerine zarar verip vermediği tespit edilmelidir. Veri sorumlusu söz konusu aktarımın meşru menfaat için mecburi olduğunu söylemişse de bu söylemi somut olarak açıklayamamıştır. Kurul'un kararı da bu yönde örtüşmektedir. Aslında veri sorumlusunun söz konusu aktarımının sebebi web tabanlı bir yazılım kullanması olsa da Kurul bu durumu şirketin meşru menfaati için zorunlu bir sebep olarak değerlendirmemiş yani web tabanlı yazılım kullanmanın bir tercih olduğunu ifade etmiştir[537]. Ayrıca, pazarlama ve reklam amaçlı müşterilere mesaj göndermek meşru menfaat olarak görülmemekte ve veri sorumlularının bu tür bildirimler için mutlaka açık rıza almaları gerekmektedir[538].

[535] Kurul, "22.07.2020 tarih ve 2020/559 sayılı Karar Özeti".
[536] Deniz Güngör, "Kişisel Verilerin Yurt Dışına Aktarımına İlişkin Güncel Kişisel Verileri Koruma Kurulu Kararı", *Mondaq*, 30 Eylül 2020, https://www.mondaq.com/turkey/data-protection/989552/ki351isel-verilerin-yurt-di351ina-aktarimina-304li351kin-gncel-ki351isel-verileri-koruma-kurulu-karari, Erişim Tarihi: 15.11.2021.
[537] Dülger, "Kişisel Verileri Koruma", s.10.
[538] Dülger, "Kişisel Verileri Koruma", s.10.

Veri sorumlusunun ifade ettiği bir diğer savunma olan açık rıza alınması hakkında Kurul, KVKK m.3(1)(a)'da yer alan açık rıza tanımına istinaden, verilen açık rıza beyanının hangi verilerin hangi amaç ile işleneceğine ilişkin verilmesi gerektiğini belirtmiştir. Verilerin yurtdışına aktarılması gibi veri kullanımı sonrası gerçekleştirilecek ikincil işlemler için veri sorumlusunun ilgili kişiden ayrıca açık rıza alması gerekmektedir. Kişisel veri işleme faaliyeti için KVKK'da yer alan açık rıza alınması haricindeki şartlardan biri için hukuki dayanak mevcutsa ilgili kişiden açık rıza alınmasının uygun olmadığı yani açık rıza haricindeki bir hukuki dayanak ile işleme faaliyeti yapılacaksa açık rıza alınmasının aldatıcı olacağı ve hakkın kötüye kullanılması anlamına geleceğini tespit etmiştir[539].

Kurul'un tespitinde görüldüğü üzere veri işleme ve veri aktarımının hangi hukuki gerekçelere göre yapıldığı önemlidir ve verilerin hangi amaçla işlendiği ve aktarıldığı açık bir şekilde belli olmalıdır. Söz konusu karar da açıklandığı üzere veri sorumlusunun hangi veriyi hangi amaca ve hangi hukuki dayanağa istinaden işlediği belli değildir. Ayrıca, şirketin aydınlatma ve açık rıza metninde pazarlama amaçlı sms gönderilmesine rıza verilmesi durumunda kişisel verilerin yurtdışındaki bir firmaya aktarılacağına dair herhangi bir açıklama yer almadığından, veri aktarımının meşru menfaate istinaden mi yoksa açık rızaya dayanarak mı yapıldığının anlaşılmadığı ya da kişisel verilerin hangilerinin açık rızaya hangilerinin meşru menfaate dayanılarak işlendiğinin açıkça belirtilmediği tespit edilmiştir[540]. Burada belirtilmesi gereken önemli bir husus, veri sorumlusunun açık rıza metninde ilgili verilerin üçüncü taraflarla paylaşılacağının belirtilmiş olmasına rağmen üçüncü tarafların yurtdışında olduğuna dair herhangi bir bilginin verilmemiş olmasıdır. Bu noktada aydınlatma yükümlülüğü gerçekleştirilirken veri işlemenin hukuki dayanağının açıkça ifade edilmesi ve aydınlatmanın KVKK ile uyumlu olması gerektiği Kurul tarafından belirtilmiştir[541].

[539] Kurul, "22.07.2020 tarih ve 2020/559 sayılı Karar Özeti".
[540] Kurul, "22.07.2020 tarih ve 2020/559 sayılı Karar Özeti".
[541] Kurul, "22.07.2020 tarih ve 2020/559 sayılı Karar Özeti".

Kararın en önemli noktası Kurul'un 108 sayılı Sözleşme ile ilgili değerlendirmesidir. Kurul yapmış olduğu değerlendirmede, savunmada bahsedilen 108 sayılı Sözleşme m.12'nin sadece, özel hayatın korunması sebebiyle sözleşmeye taraf ülkelerin kendi aralarında kişisel veri aktarımlarının yasaklanamayacağını veya kısıtlanamayacağını düzenlediğini belirtmiştir. Sözleşmeye ilişkin Açıklayıcı Raporun 2. fıkrasında ise, söz konusu hükmün amacının taraf ülkelerin kişisel verilerin korunması açısından yeterli seviyede güvence verdiği hususunun kabul edilerek kendi aralarındaki veri akışını kolaylaştırmak olduğu belirtilmiştir.

Kurul yapmış olduğu değerlendirmede, 108 Sayılı Sözleşmenin taraf devletlerin gerek yurtiçi gerekse yurtdışı aktarımlarını yasaklamaya ilişkin düzenleme yapabilmesini engellemediğini, ayrıca hükmün AB uygulamasında Sözleşmeye taraf olan ülkelerin başka bir değerlendirme yapmadan yeterli korumayı sağlayan ülkeler olarak değerlendirilmediğini ve taraf olmanın sadece yeterlilik değerlendirmesinde dikkate alınacak bir kıstas olarak kabul edildiğini belirtmiştir[542]. Kurul, KVKK m.9(4)(a)'da yer alan "Türkiye'nin taraf olduğu sözleşmelerin dikkate alınması" hükmüne istinaden yapmış olduğu açıklamada, aktarım yapılacak ülkenin yeterli koruma sağladığına ilişkin yapılan değerlendirmede ülkenin 108 sayılı sözleşmeye taraf olmasının yanında kişisel verilerin özellikleri, ilgili ülkedeki veri koruma kanunu ve uygulaması, veri sorumlusu veya işleyenin taahhütte bulunacağı önlemler gibi hususlar ile Türkiye ve aktarım yapılacak ülke arasındaki karşılıklılık durumunun da değerlendirme de göz önünde bulundurulduğunu belirtmiştir[543]. Kurul, bu değerlendirmelere istinaden KVKK'da yer alan veri aktarım mekanizmasının 108 sayılı Sözleşme ile uyumluluk içinde olduğunu ifade etmiştir[544]. Kurul 108 sayılı sözleşmeye taraf olmanın yurtdışına kişisel verilerin aktarımı için tek başına yasal dayanak teşkil etmeyeceğini ve buna istinaden yurtdışına veri aktarımının KVKK m.9 kapsamında yer alan şartlara uygun olarak yapılabileceğini belirtmiştir.

[542] Kurul, "22.07.2020 tarih ve 2020/559 sayılı Karar Özeti".
[543] Kurul, "22.07.2020 tarih ve 2020/559 sayılı Karar Özeti".
[544] Kurul, "22.07.2020 tarih ve 2020/559 sayılı Karar Özeti".

Kurul vermiş olduğu kararla, 108 sayılı Sözleşme gerekçe gösterilerek KVKK m.9(2)(b) kapsamında yeterli korumanın olmadığı ülkelere yapılan veri aktarımlarında Kurul'dan izin alınması gerektiğini vurgulamıştır[545]. Bu kapsamda veri sorumlusunun yapmış olduğu açıklamalarda ve sunduğu bilgi ve belgelerde KVKK m.9(2)(b) uyarınca taahhütname hazırlandığı/hazırlanacağı bilgisinin yer almadığı ve Karar tarihine kadar Kurul'a herhangi bir taahhütname başvurusunda bulunmadığı belirtilmiştir.

Kurul, KVKK m.9(6)'da yer alan "diğer kanunlarda yer alan hükümlerin saklı tutulması" hükmüne dayanarak, T.C. Anayasası m.90'da yer alan usulünce yürürlüğe konulmuş uluslararası sözleşmelerin kanun hükmünde olduğunu ve bu çerçevede 108 sayılı sözleşmenin de kanun niteliğine haiz olduğunu belirtmiştir. Aynı maddenin gerekçesinde söz konusu anlaşma hükümlerinin kullanılabilmesi için uluslararası sözleşme hükümlerinin doğrudan uygulanabilmesi gerektiği yani "*yeterince açık, kesin, koşulsuz olması ve uygulaması için devletin ilave bir tedbir almasını gerektirmeyecek nitelikte*" olması gerektiğinin altını çizmiştir. Kurul bu bağlamda doğrudan uygulanabilir olmayan soyut ve genel bir sözleşme hükmü ile Kanun'un hükmü arasında oluşan uyuşmazlığın m.90(5)[546]'e göre çatışma teşkil etmeyeceğini ve bu nedenle Anayasa'nın bahsi geçen hükmünün uygulanamayacağına karar vermiştir. Buna bağlı olarak kanun hükmü ile uluslararası antlaşma hükmünün çelişmesi durumunda çelişen KVKK maddesinin esas alınması gerektiğini değerlendirmiştir[547].

Öte yandan Kurul, 108 sayılı Sözleşme m.4'e ve Açıklayıcı Rapora göre, sözleşme m.12'de yer alan hükmün taraf devletler için doğrudan bağlayıcı ve uygulanabilir olmadığını ve sözleşmede yer alan veri koruma hükümlerinin iç hukuka alınması

[545] Güngör, "Kişisel Verilerin Yurt Dışına".
[546] T.C. Anayasası m.90(5) uyarınca "*Usulüne göre yürürlüğe konulmuş Milletlerarası antlaşmalar kanun hükmündedir. Bunlar hakkında Anayasaya aykırılık iddiası ile Anayasa Mahkemesine başvurulamaz. Usulüne göre yürürlüğe konulmuş temel hak ve özgürlüklere ilişkin milletlerarası antlaşmalarla kanunların aynı konuda farklı hükümler içermesi nedeniyle çıkabilecek uyuşmazlıklarda milletlerarası antlaşma hükümleri esas alınır*".
[547] Kurul, "22.07.2020 tarih ve 2020/559 sayılı Karar Özeti".

yükümlülüğünün bulunduğunu belirtmiştir. Kurul, Sözleşme hükümlerinin sadece ulusal veri korumaya ilişkin düzenlemelerde olması gereken temel ilkeleri ve ilgili kişilere sağlanacak güvencelerin usul ve esaslarını belirlemekte olduğunu hatırlatmıştır.

Sonuç olarak, Kurul, veri sorumlusunun, açık rızanın şartlarına uygun bir metin düzenlemediği ve ilgili kişilere açık ve net olacak şekilde bildirmediği, meşru menfaat dayanağına ilişkin olarak denge testinin yapılmadığı ve veri sorumlusunun Kurul'a herhangi bir taahhütname başvurusu yapmadığı gerekçeleriyle kişisel verilerin yurtdışına aktarılması konusunda KVKK m.9'da belirtilen yurtdışına veri aktarımına ilişkin hükme uygun bir aktarım gerçekleştirmediğine karar vermiştir. Bu kapsamda veri sorumlusunun, hukuka aykırı bir şekilde yurtdışına aktardığı kişisel verilerin KVKK m.7 hükmüne uygun olarak silmesi veya yok etmesine ve söz konusu kişisel verilerin silindiğine veya yok edildiğine dair Kurul'a bilgi vermesine karar verilmiştir. Ayrıca, şirketin aydınlatma metni ve rıza metni olarak 2018 yılından beri güncellenmeyen metinler kullandığı ve metinlerin Aydınlatma Tebliği'ne göre hazırlanmasında gerekli dikkat ve özenin gösterilmediği tespit edilmiş ve bu çerçevede veri sorumlusunun aydınlatma yükümlülüğünü ve açık rıza alınması işlemlerini yerine getirmesine karar verilmiştir[548]. Ayrıca veri sorumlusu yukarda açıklanan sebeplerden ötürü KVKK m.18(1)(b) uyarınca 900.000 TL idarî para cezasına çarptırılmıştır.

Veri sorumlusunun, Kurul yeterli korumaya sahip ülkeler listesini henüz ilan etmediğinden 108 sayılı Sözleşme m.12'yi hukuki dayanak olarak göstermesi aslında aktarıma ilişkin başka bir dayanak arayışı içinde olduğunu göstermektedir[549]. Ancak, bu dayanağın öne sürülmesi Kurul'un KVKK m.9 kapsamındaki yükümlülüklerin yerine getirilmesi konusundaki değerlendirmesini değiştirmemektedir. Bu noktada Kurul'un yeterli korumayı sağlayan ülkeleri açıklamamasının da "karşılıklılık" ilkesine göre Türkiye'nin henüz AB veya diğer

[548] Kurul, "22.07.2020 tarih ve 2020/559 sayılı Karar Özeti".
[549] Dülger, "Kişisel Verileri Koruma", s.16.

ülkeler tarafından yeterli koruma sağlayan ülke listesine dâhil edilmemiş olması sebebine bağlamak mümkündür[550]. Kurul'un bu kararı yurtdışına veri aktarımlarının hangi kural ve düzenlemelere göre yapılabileceğini açık ve net bir şekilde belirlemiştir.

4.2.3 31.05.2019 Tarih ve 2019/157 Sayılı Karar

Gelişen teknoloji ve küreselleşmenin etkisiyle bulut hizmetlerin kullanımı giderek artmış ve kişisel verilerin aktarılmasında da gündeme gelmiştir. Kurul'un 31.05.2019 tarih ve 019/157 sayılı, kurumsal e-posta hizmetinin, Google (gmail) üzerinden yine aynı uzantıya sahip olarak kullanılıp kullanılamayacağına ilişkin kararı, kişisel verilerin aktarılmasında bulut hizmetlerinin kullanımı açısından önemlidir. Söz konusu kararda Kurul tarafından;

> *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 olacağına ve veri sorumlularının söz konusu uygulamayı 6698 sayılı Kişisel Verilerin Korunması Kanununun (Kanun) "Kişisel verilerin yurt dışına aktarılması" başlıklı 9 uncu maddesi hükümlerine uygun olarak gerçekleştirmesine ve server'ları yurt dışında bulunan veri sorumlularından/veri işleyenlerden temin edilen saklama hizmetlerinin de Kanunun 9 uncu maddesi hükümlerine uygun olarak gerçekleştirilmesine*[551]

karar verilmiştir. Karar, Google özelinde alınmış olsa da karar sonucunda aynı şekilde e-posta hizmeti sunan diğer şirketlerden (Amazon, Microsoft vb.) e-posta

[550] Dülger, "Kişisel Verileri Koruma", s.16.
[551] Bkz. Kurul, "Kurumsal e-posta hizmetinin, Google (Gmail) üzerinden yine aynı uzantıya sahip olarak kullanılıp kullanılamayacağına ilişkin 31.05.2019 tarihli ve 2019/157 sayılı karar özeti", https://www.kvkk.gov.tr/Icerik/5493/2019-157, Erişim Tarihi: 15.11.2021.

hizmeti alan veri sorumluları da KVKK m.9 kapsamında yükümlülük altına girmişlerdir.

4.3 KVKK ve GDPR Karşılaştırması

Kurul, Türkiye'nin AB üyeliği sürecine uyumlu olacak şekilde KVKK'nın gerek uygulanmasında gerekse yorumlanmasında GDPR'ı takip etmekte olsa da KVKK ve GDPR'da kişisel verilerin yurtdışına aktarılmasında farklı yaklaşımlar izlenmektedir. GDPR'da, kişisel verilerin yurtdışına aktarılması konusunda verilerin aktarılmasını daha kolay hale getirmek için alternatiflerin olduğu bir sistem kurulmuş, KVKK'da ise açık rızanın olmadığı durumda verilerin aktarılması için daha kontrollü bir yapı oluşturulmuştur[552]. GPDR'da yer alan kişisel verilerin yurtdışına aktarım mekanizmaları, veri alıcılarının GDPR'a uymasını sağlamaya ve kişisel verilerin aktarıldığı ülkede korunmasına yöneliktir. KVKK'da kişisel verilerin yurtdışına aktarılmasında temel kural olarak ilgili kişinin açık rızası alınması gerekirken, GDPR'da verilerin aktarımını aksatmadan kişisel veriler için yeterli bir koruma sağlamaya yönelik yaklaşım ile AB Hukuk kurallarının verilerin aktarıldığı ülkelere ihraç edilmesi amaçlanmıştır[553]. GDPR ayrıca, kısıtlayıcı olmak yerine veri akışını kolaylaştırmak için uygun bir yöntem sağlar[554]. KVKK ise yurtdışına aktarılan kişisel veriler için hem mevzuat açısından hem de mevzuatın uygulanması açısından kısıtlayıcıdır[555]. GPDR'da yeterlilik kararı alınmasında Avrupa Komisyonu'nun üstlendiği görev KVKK'da benzer şekilde Kurul'un yetkisindedir. KVKK'da yer alan Kurum'un GDPR'da karşılığı ise EDPB'dir.

Kurul'un açık rızada GDPR'da bulunan unsurları istemesi, açık rızaya dayanılarak Türkiye'den yurtdışına kişisel veri aktarımlarını zorlaştırmaktadır[556]. Bu durumun ilk sebebi, kişiye ürün veya hizmet sunulması ya da kişinin ürün veya hizmetten

[552] Bilgi IT Law Institute, "Kişisel Verilerin Korunmasına İlişkin Düzenlemeler", s.35.
[553] Aşıkoğlu ve Uzun, "Kişisel Verilerin Yurtdışına", s.935.
[554] Bilgi IT Law Institute, "Kişisel Verilerin Korunmasına İlişkin Düzenlemeler", s.35.
[555] Bilgi IT Law Institute, "Kişisel Verilerin Korunmasına İlişkin Düzenlemeler", s.46.
[556] Aşıkoğlu ve Uzun, "Kişisel Verilerin Yurtdışına", s.960.

yararlandırılması için açık rızanın ön şart olarak sunulamayacak olmasıdır. Diğer bir sebep ise ilgili kişinin vermiş olduğu açık rızasını her zaman geri çekme hakkının olmasıdır. Kişinin verdiği rızayı geri çekme hakkı, veri sorumlularının sunduğu ürün veya hizmetin sürekliliği bakımından önemli bir risk olarak görülmektedir. Açık rızanın geri çekilmesi, veri sorumlusunun yurtdışında gerçekleştirdiği tüm faaliyetlerini etkilemekle birlikte, kişiye ürün veya hizmetin sunulmasını imkânsızlaştırabilir[557].

Genel olarak bakıldığında yurtdışına veri aktarımlarında KVKK'nın çizdiği çerçevenin ve KVKK'da yer alan açık rıza kavramının, GDPR'da yer alan aktarım mekanizmaları karşısında yetersiz kaldığı düşünülmektedir[558]. Kişisel verilerin yurtdışına aktarılmasında GPDR m.49'da istisnalar altında yer alan ve katı gereklilikler getirilen açık rıza, GDPR'da yer alan diğer aktarım mekanizmalarının bulunmaması halinde hukuka uygunluk dayanağı olarak belirlenmiştir. GDPR'da yer alan aktarım mekanizmaları arasındaki hiyerarşik düzende yeterlilik kararı ve uygun güvenceler olmadığı zaman kullanılabilen ve istisna olarak düzenlenen ilgili kişinin açık rızasının alınması, KVKK'da yurtdışına veri aktarımında temel dayanak olmuştur. Bu anlamda, KVKK'da yer alan açık rızanın kişisel verilerin korunmasını sağlamadığı sadece hukuki bir dayanak oluşturduğu söylenebilir[559]. Öte yandan, GDPR'da yer alan açık rıza ilgili kişinin aktarımın olası risklerine karşı bilgilendirilmesini gerektirirken, KVKK'da yer alan açık rıza için bu yönde bir bilgilendirme zorunluluğu olduğu açıkça yer almamaktadır.

KVKK'da yer alan yeterli korumanın sağlanması ve GDPR'da yer alan yeterlilik kararı da birbirine benzemektedir. Bu noktada aralarındaki temel fark ise, bu mekanizmanın KVKK'nın aksine GDPR'da ana ilke olarak yer almasıdır. Çalışmanın ikinci bölümünde detaylı olarak anlatıldığı üzere GDPR'da, verilerin yurtdışına aktarılmasında ilk mekanizma yeterlilik kararı olarak düzenlenmiş ve

[557] Aşıkoğlu ve Uzun, "Kişisel Verilerin Yurtdışına", s.960.
[558] Kızılırmak, "Cross-Border Transfer", s.56.
[559] Kızılırmak, "Cross-Border Transfer", s.66.

Avrupa Komisyonu tarafından verilen yeterlilik kararları ile AB ile eşdeğer bir koruma sağlayan ülkelerin olduğu "beyaz liste" belirlenmiştir. KVKK'da da bu yönteme benzeyecek şekilde yeterli korumanın bulunduğu ülkelerin ilan edilebileceği hükmü yer alsa da Kurul tarafından henüz yeterli korumanın bulunduğu ülkelerin listesi yayınlamadığından bu hüküm hiçbir ülke için geçerli olmamaktadır[560].

KVKK'da yer alan açık rızanın özelliklerinin GDPR'ı takip etmesinin bir diğer sonucu da yurtiçinde ve yurtdışında bulunan veri sorumluları arasındaki eşitsizliktir[561]. Yurtiçinde bulunan veri sorumlusunun yurtdışına veri aktarabilmesi ve aktardığı verilerin yurtdışında işlenebilmesi için KVKK'ya göre açık rıza alması gerekirken, yurtdışında bulunan veri sorumlusu Türkiye'de yer alan kişisel verilerin işlenmesi veya aktarılması için ilgili kişilerden açık rıza almak zorunda değildir.

GDPR m.49'da yer alan bazı istisnalar, KVKK m.5(2)'de yer alan veri işleme şartlarıyla benzer olup aralarındaki temel fark ise GDPR'da düzenlenen istisnaların veri aktarımı için tek başına yeterli olmasıdır[562]. KVKK m.5(2)'de ki şartlar ise veri aktarımı için tek başına yeterli değildir. Söz konusu şartlar, bu şartlardan en az birinin varlığı ile veri aktarımının yeterli korumanın bulunduğu ülkelere yapıldığı veya yeterli korumanın olmadığı ülkelerde ise veri sorumlusu tarafından taahhütte bulunulması ve Kurul'un izninin alındığı durumlarda hukuki dayanak oluşturur.

Hem KVKK hem de GDPR'da üçüncü ülkede yeterli korumanın bulunduğuna dair dikkate alınacak kriterler benzer olsa da GDPR'da olup da KVKK'da yer almayan kriterler bulunmaktadır. Bu nedenle GDPR'ın kriterler açısından daha kapsamlı olduğu görülmektedir. Örneğin KVKK'da yeterli korumaya ilişkin değerlendirmede sadece üçüncü ülkenin sahip olduğu veri koruma ve işlemeye ilişkin mevzuat ve uygulaması dikkate alınırken, GDPR veri koruma mevzuatının

[560] Bilgi IT Law Institute, "Kişisel Verilerin Korunmasına İlişkin Düzenlemeler", s.110.
[561] Aşıkoğlu ve Uzun, "Kişisel Verilerin Yurtdışına", s.962.
[562] Bilgi IT Law Institute, "Kişisel Verilerin Korunmasına İlişkin Düzenlemeler", s.111.

yanında hukukun üstünlüğü, insan hakları ve temel özgürlüklere saygı, kamu güvenliği, savunma, milli güvenlik ve ceza hukuku ile kamu kuruluşlarının kişisel verilere erişimi de dâhil olmak üzere üçüncü ülke mevzuatının geniş kapsamlı olarak değerlendirilmesini gerektirir. Üçüncü ülke mevzuatının geniş kapsamlı olarak dikkate alınması ilgili kişilerin haklarının korunması bakımından oldukça önemlidir. Ayrıca, GDPR'da yer alan üçüncü ülkelerin küresel veya bölgesel kuruluşlara üye olması kriteri KVKK'da bulunmamaktadır. Küresel ve bölgesel kuruluşlara üye olan üçüncü ülke, üyesi olduğu kuruluşlara verdiği uluslararası taahhütler ve yasal bağlayıcılığa sahip onayladığı sözleşmeler bakımından daha fazla güvence sağlar. Öte yandan GDPR'dan farklı olarak KVKK'da yer almayan etkili ve uygulanabilir ilgili kişi hakları ve ilgili kişilere yönelik etkili idarî ve adli tazminat imkanlarının olması da yeterlilik değerlendirmesinde dikkate alınması gereken önemli bir kriter olacaktır.

KVKK m.9(2)(b)'de yer alan veri sorumlularının taahhüdü ve Kuruldan izin alınması koşulu GDPR'da yer alan iki mekanizma ile benzerdir. Standart sözleşme maddeleri mekanizması, Komisyon tarafından kabul edilen standart sözleşme maddelerinin bir bütün olarak ve üzerinde değişikliğe uğratılmadan kullanılması durumunda kişisel verilerin yurtdışına aktarılması durumudur[563]. Bu yöntemi KVKK'da yer alan benzer yöntemden ayıran özellik ise veri koruma otoritesinden izin alınmasına gerek olmamasıdır. GDPR'da yer alan diğer mekanizma ise veri aktaran ile veri aktarılan arasındaki sözleşmede yer alacak hükümlerle uygun güvencelerin sağlandığı yöntemdir ve bu yöntemde aktarımın yapıldığı ülkede bulunan veri koruma otoritesi tarafından sözleşme hükümleri için onay alınması gerekmektedir. KVKK'da ve GDPR'da düzenlenen bu benzer yöntemin en önemli farkı, KVKK'da yer alan taahhüt ve izin yöntemi, açık rıza ile her zaman yurtdışına veri aktarımının mümkün olmaması ve yeterli korumanın olduğu ülkelerin açıklanmamış olması sebebiyle ana yöntem iken GDPR'da ise söz konusu yöntemin bir alternatif olarak yer almasıdır[564].

[563] Bilgi IT Law Institute, "Kişisel Verilerin Korunmasına İlişkin Düzenlemeler", s.110.
[564] Bilgi IT Law Institute, "Kişisel Verilerin Korunmasına İlişkin Düzenlemeler", s.110.

GDPR'da, yeterlilik kararının olmadığı durumlarda verilerin aktarılabilmesine yönelik altı farklı uygun güvence yöntemi yer almaktadır. KVKK'da ise yeterli koruma bulunmadığında kullanılabilecek ve GDPR'da yer alan uygun güvence yöntemine benzer olan taahhüt ve izin yöntemi dışında farklı bir uygun güvence yöntemi bulunmamaktadır. Bu kapsamda KVKK'da da yeterli korumanın bulunmadığı durumlarda GDPR'da yer alan ve veri sorumluları tarafından sağlanacak uygun güvenceler gibi alternatif yöntemlerle yurtdışına veri aktarılabilir. Örneğin, GDPR'da yer alan standart sözleşme maddeleri benzeri olarak Kurul tarafından belirlenen standart hükümlerin yer aldığı taahhütname yoluyla Kurul'dan ilave bir izin almadan kişisel verilerin aktarılması sağlanabilir. Ayrıca, GDPR'da yer alan davranış kuralları ve sertifikasyon mekanizmaları ile aktarım hususu KVKK'da bulunmamaktadır. Standart sözleşme maddelerinin karmaşıklığı ve bağlayıcı şirket kurallarının sınırlı firmalar tarafından kullanılabilmesi davranış kuralları ve sertifikasyon mekanizmalarının kullanılabilmesini daha çok uygulanabilir hale getirmektedir. Anılan yöntemlerin KVKK'da da yer alması yurtdışına yapılacak aktarımlar için alternatifler oluşturacaktır.

İlaveten GDPR'da davranış kuralları ve sertifikasyon mekanizmasında olduğu gibi KVKK m.9(2)(b) uyarınca taahhütname yoluyla taahhütte bulunan ve bu taahhüde bağlı kalan veri sorumlusu ve veri işleyenlerin de bu bağlılığa ve taahhütlerine uyup uymadığını kontrol etmek, izlemek ve uyumu sağlamak için Kurul'un akredite edeceği özel bir organ atanabilir. Bu organın atanması uygulamada taahhütname yönetiminin etkin ve hızlı işlemesi ve taahhütnamelere uyumun sağlanması için önemli bir adım olacaktır. Söz konusu organın taahhütnameler konusunda uzmanlaşmış ve bağımsız olması, yerine getirdiği görevlerin çıkar çatışmasına sebep olmaması, kural ihlallerine ilişkin şikâyetleri değerlendirecek şeffaf prosedür ve yapıya sahip olması gibi kriterleri taşıması gerekmektedir. Akredite edilen organlar, gelecekte veri aktarımının artacağı ve daha karmaşık hale geleceği düşünüldüğünde veri akışını kolaylaştırmak ve veri korumasına uyumun sağlanması adına etkin bir rol üstelenmiş olacaklardır.

KVKK ile GDPR arasındaki bir benzer aktarım yöntemi de Bağlayıcı Şirket Kurallarıdır. KVKK'da tanımlanmamış ve ismen yer almamış olsa da Kurul'un Bağlayıcı şirket kurallarına ilişkin olarak yayınladığı belgelerde görüldüğü üzere, KVKK kapsamında geçerli olan Bağlayıcı Şirket Kuralları hükümlerinin GDPR'da düzenlenen Bağlayıcı şirket kurallarının temelini oluşturan ve WP29'un yayınladığı belgelerde yer KVKK kapsamında oluşturulan bağlayıcı şirket kurallarının AB'den örnek alınarak benzer şekilde yapılması, özgün bir düzenleme olmaması bakımından öğretide eleştirilere sebep olmuştur. Zira başka mevzuatlardan neredeyse birebir alınarak yapılan düzenlemeler başlangıçta problemleri çözmek için uygun bir yol gibi görünse de sonrasında farklı sorunlar ortaya çıkabilmektedir[565].

Kişisel verilerin yurtdışına aktarılması hususunda KVKK'da GDPR'da olduğu gibi iki aşamalı bir yaklaşım izlendiği görülmektedir. İlk aşamada KVKK'da yer alan genel kurallar, ikinci aşamada ise yurtdışına aktarım özelinde 9. madde de yer alan hükümler dikkate alınmaktadır[566]. Zira m.9'da yer alan kurallar m.5(2) ve m.6(3)'de yer alan genel şartların tamamlayıcısı niteliğindedir[567]. İkinci aşamada, aktarım yapılacak ülkenin yeterli koruma sağlayıp sağlamadığına göre veri sorumlusu gerekli tedbirleri alacaktır. GDPR'da ise aktarımlara ilişkin genel ilkeleri düzenleyen GDPR m.44'de benimsenen yaklaşıma göre kişisel verilerin, GDPR ile gerçek kişilere yönelik sağlanan koruma düzeyi zarar görmeden AB dışına aktarılabilmesi için, aktarımın hem GDPR 5. Bölümdeki hükümlere hem de GDPR'ın diğer tüm hükümlerine uygun olarak yapılması gerekmektedir. Ayrıca KVKK'da kişisel verilerin ileriye dönük aktarımları ve transit aktarımları kısıtlanmamıştır. GDPR m.44'de yer alan bu düzenleme de KVKK'nın eksik kaldığı bir husustur.

[565] Dülger ve Kahraman, "KVKK'dan Kişisel Verilerin Yurt Dışına", s.6.
[566] Bekir Gürses, "AB ve Türk Hukukunda Kişisel Verilerin Korunması- Mevzuat Uyumuna Yönelik Bir Değerlendirme", Yüksek Lisans Tezi, Marmara Üniversitesi, 2019, s.56.
[567] Mesut Serdar Çekin, *Avrupa Birliği Hukukuyla Mukayeseli olarak 6698 Sayılı Kişisel Verilerin Korunması Kanunu,* İstanbul: On iki Levha Yayıncılık, 2018, s. 87.

GDPR 5. Bölümde yer alan veri aktarım kuralları, üçüncü ülkelerin yanında aktarımların uluslararası kuruluşlara yapılması durumunda da geçerli olacak şekilde düzenlenmiştir. Uluslararası kuruluşlara aktarım hususu KVKK'da yer almamaktadır. Uluslararası kuruluşlarla olan gerek ticari gerekse diplomatik ilişkiler ve bu kuruluşlarla birlikte çalışma gerekliliği dikkate alındığında aktarım kurallarına uluslararası kuruluşların da dâhil edilmesi önemli bir ihtiyaca cevap verecektir. Ayrıca, GDPR'da yer alan üçüncü ülke içerisindeki belirli bir sektörün yeterli koruma sağladığına ilişkin verilen kısmi yeterlilik kararı benzeri bir uygulamanın KVKK'ya eklenmesi, önemli sektörlerde üçüncü ülkeler ile Türkiye arasındaki ticari ilişkilerin gelişmesine katkıda bulunarak uygulamada kolaylık sağlayacaktır.

KVKK kapsamında her ne kadar yeterli korumanın bulunduğu ülkeler ilan edilmemiş olsa da, yeterli korumanın bulunduğu ülkelerin ilan edilmesi durumunda söz konusu korumaya ilişkin yeterliliğin periyodik olarak gözden geçirilmesi veri korumanın sürekliliği açısından bir gerekliliktir. Nitekim ABAD'ın Schrems I kararının bir gerekliliği olarak Komisyon'un aldığı bir yeterlilik kararının periyodik olarak gözden geçirilmesi gerektiği GDPR m.45(3)'de düzenlenmiştir. KVKK'da da periyodik gözden geçirme süresinin yer alması ile Kurul tarafından yeterli korumanın bulunduğu ülkeler, bu ülkelerin tespitinde dikkate alınması gereken kriterlere göre revize edilebilir.

GDPR'da yeterlilik kararı ve uygun güvence olmadığında aktarıma yasal dayanak olarak istisnai durumlar düzenlenmiştir. Bu düzenleme KVKK'da yer almamış ve GDPR'da yer alan açık rıza istisnası da KVKK'da aktarımın ilk koşulu olmuştur. Bu kapsamda aktarımlara yasal dayanak olması ve istisnaların GDPR'daki gibi dar yorumlanacak şekilde KVKK'da da düzenlenmesi, veri sorumlusunun bazı sınırlı durumlarda istisnalara dayanarak veriyi hukuka uygun olarak aktarabilmesinin önünü açacaktır. Ancak belirtmek gerekir ki istisnaların, istisnaların doğasına aykırı olamayacak şekilde sürekli ve düzenli olmayan ve ara sıra gerçekleşen aktarımlar

için kullanılması ve bir kural haline gelmemesi gerekmektedir. Zira bu gereklilik GDPR'da özellikle belirtilerek istisnalara dayalı aktarımlar sınırlandırılmıştır.

SONUÇ

GDPR, AB Hukukunda kişisel verilerin üçüncü ülkelere aktarılmasına ilişkin en önemli düzenlemedir. GDPR, kişisel verilerin aktarımına ilişkin içerdiği hükümler ile kişisel verilerin korunması hakkı temelinde verilerin aktarılmasını kısıtlayarak kontrollü bir aktarım gerçekleşmesini sağlamaktadır.

GDPR'da, kişisel verilerin AB dışına aktarımına ilişkin olarak hiyerarşik bir yapıda olan ve çalışmanın önceki bölümlerinde detaylı olarak incelenen meşru aktarım mekanizmalarının en üst basamağında bulunan yeterlilik kararının tasarlanma amacı temelde, AB'de bulunan ilgili kişiler için veri koruma düzeyini garanti etmek ve AB veri koruma standardını tüm dünya ülkeleri için teşvik etmektir. Komisyon bir yeterlilik kararı alırken GDPR'a uyarak ve üçüncü ülkede AB ile eşdeğer seviyede koruma sağlamaya yönelik yaklaşımı dikkate alarak hareket etmektedir. Güvenli Liman ve Gizlilik Kalkanı kapsamında Komisyonun almış olduğu yeterlilik kararlarının, temel haklara müdahale edilmesine imkân vermesi ve Şart'ın gerekliliklerini taşımaması nedenleriyle ABAD tarafından geçersiz kılınması da AB'nin üçüncü ülkelerde AB ile eşdeğer seviyede koruma sağlamaya yönelik yaklaşımı ile bu yeterlilik kararlarının tutarsız olduğunu göstermiş ve yeterlilik kararlarının eksiklerini ortaya çıkarmıştır[568]. Bu da gösteriyor ki bir yeterlilik kararının temel görevi olan AB'de bulunan ilgili kişilere sağlanan koruma düzeyinin üçüncü ülkelerde de garanti edilmesi yeterlilik kararına rağmen yerine getirilemeyebilir. Şunu da belirtmek gerekir ki dünya üzerinde iki yüzü aşkın ülke olduğu ve yeterlilik kararı verilen toplam ülke sayısının on beş olduğu düşünüldüğünde yeterlilik kararı ile AB dışına veri aktarımının diğer aktarım yöntemlerine göre sınırlı sayıda kaldığı söylenebilir[569].

[568] Chen, s.46.
[569] W. Gregory Voss, "Cross-Border Data Flows, the GDPR, and Data Governance", *Washington International Law Journal*, 29/3 (2020), s.507.

Öte yandan yeterlilik kararlarının barındırdığı ve AB'nin şart koştuğu veri korumaya ilişkin taahhütleri üçüncü ülkelerin kabul etmeleri, ülkelerin ticareti kolaylaştırması çıkarlarını da içermektedir. Örneğin Japonya'ya yönelik alınan yeterlilik kararı, Japonya'nın AB veri koruma standardına yaklaşması ve GDPR'a uyum sağlayarak veri koruma rejiminde reform yapmasının yanında, AB ve Japonya'nın karşılıklı ticari çıkarları bakımından da bir zorunluluk olmuştur. Zira Komisyon 2017 yılında yayınladığı bir kararda, hangi üçüncü ülkelere yönelik yeterlilik kararı alınacağını belirlerken, AB'nin söz konusu üçüncü ülke ile olan ticari ilişkilerinin de dikkate alınacağını ifade etmiştir[570]. Ayrıca, 17 Aralık 2021 tarihinde Kore Cumhuriyeti'ne yönelik verilen yeterlilik kararının, kişisel veri akışının sürekliliğinin sağlanması açısından AB ve Kore Cumhuriyeti arasındaki Serbest Ticaret Anlaşmasının tamamlayıcısı olduğu ve dijital dünyada gizlilik ve kişisel veri korumasının sağlanması ile uluslararası ticareti kolaylaştırmanın birlikte yürüyebileceği taraflar tarafından ifade edilerek[571] yeterlilik kararı ve ticari ilişkiler arasındaki öneme dikkat çekilmiştir.

AB'den üçüncü ülkelere kişisel veri aktarımının ekonomik etkilerine rağmen, GDPR 5. Bölümde yer alan aktarıma ilişkin hükümlerin yeterli şekilde açıklanmadığı görülmektedir. Özellikle, yeterlilik kararı alınırken üçüncü bir ülkenin veri koruma düzeyinin AB ile eşdeğer olarak kabul görecek kadar yeterli olup olmadığının nasıl değerlendirilebileceğine ilişkin net şartlar GDPR'da yer almamaktadır. EDPB'nin GDPR'da yer alan hükümlerin kullanımına ilişkin rehberler yayınlaması da GDPR'da yer alan hükümlerin yeterli açıklanmadığının bir göstergesidir. Veri sorumlusu veya veri işleyenlerin, üçüncü ülkeye yönelik yeterlilik kararı alınırken değerlendirilen kriterlerin tam olarak neler olduğunu bilmeleri şirketlerin iş süreçlerini planlamaları bakımından önemlidir.

[570] European Commission, "Exchanging and Protection Personal Data", s.8-9.
[571] Bkz. https://ec.europa.eu/commission/presscorner/detail/en/statement_21_6915, Erişim Tarihi: 30.12.2021

ABAD, almış olduğu Schrems I kararı ile Güvenli Limanı geçersiz kılmasının yanında, AB Hukuku çerçevesinde veri aktarımları için yeterli koruma düzeyini tanımlamış ve AB Hukukundaki temel veri koruma hakkının AB'den üçüncü ülkelere aktarılan kişisel verilerin işlenmesine yönelik yol gösterici olarak kullanılması için bir içtihat oluşturmuştur[572]. Ayrıca ABAD, üçüncü ülkelere aktarılan kişisel veriler açısından veri koruma otoritelerinin korumanın yeterliliğini inceleme hakkına destek vermiş ve ulusal denetim makamlarının rolünü güçlendirmiştir.

Kişisel veri aktarımları Schrems I kararından 4 yıl sonra bu sefer ABAD'ın Schrems II kararı ile gündeme gelmiştir. Gizlilik Kalkanı Anlaşmasını geçersiz kılan ve standart sözleşme maddeleri için yeni gereklilikler getiren Schrems II kararı, Gizlilik Kalkanı kapsamında ve standart sözleşme maddeleri ile AB'den ABD'ye aktarım yapan şirketler açısından ilk etapta belirsiz bir ortam oluşturmuştur. Bir tarafta AB Hukukunun veri koruma gereklilikleri diğer tarafta şirketlerin iş yapabilmeleri için küresel düzeyde veri aktarımı gereklilikleri düşünüldüğünde, AB'nin veri koruma standardını yükseltmesinin bu şirketlerin iş yapmalarını zorlaştıracağı aşikârdır. Facebook'un Küresel İşler ve İletişimden Sorumlu Başkan Yardımcısı Nick Clegg'in "*Hâlihazırda kurulmuş olan Facebook ile ortak ve benzer birçok şirketin, artık dünyanın bir ucundan diğerine verileri aktarabilmek için yasal bir dayanağı yoksa hizmet sağlaması zorlaşacaktır*[573]" şeklindeki açıklaması bu ikilemi göstermektedir.

Veri aktarım mekanizmalarına etkisi açısından bir dönüm noktası olarak görülen Schrems II kararı sonrasında kişisel verilerin AB dışına aktarımına ilişkin kurallar standart sözleşme maddeleri özelinde farklı şekillenmiştir. Schrems II kararı ile standart sözleşme maddeleri, yeterlilik kararı bulunmayan üçüncü ülkelere veri aktarımında meşru bir aktarım aracı olarak onaylanmıştır. Bunun yanında yeterlilik

[572] Kuner, "Reality and illusion", s.884.
[573] Congressional Research Service,"U.S.- EU Privacy Shield", s.15; Mark Scott, " Facebook's Clegg: Stopping Data Transfers Would Have 'Profound Consequences", *Politico Pro,* 2021.

kararı için benimsenen eşdeğer koruma seviyesinin standart sözleşme maddeleri için de gerekli olduğu Schrems II kararının bir sonucudur.

Bu kapsamda Schrems II kararı sonrasında yaşanan en önemli gelişmelerden birisi Komisyonun Direktif kapsamında önceden hazırlanmış standart sözleşme maddelerini Schrems II kararının getirdiği yüksek gerekliliklere göre güncellemesidir. Yeni standart sözleşme maddeleri ile AB'nin uluslararası veri aktarımlarında yüksek olan veri koruma çıtası daha da yükselmiştir. Nitekim bu yeni standart sözleşme maddelerine uyum tarafların organizasyonel ve teknik önlemleri almasını ve veri aktaran ve veri aktarılanların işbirliği içinde olmasını gerektirmektedir. Veri aktarım değerlendirmesi ile belirlenen veri aktarımlarına ilişkin alınacak ilave önlemlerin uygulamasının zor ve maliyetli olması da kaçınılmazdır. Veriye dayalı ticaretin önemi, küresel veri akışının artması ve veri aktarımını daha az kısıtlayıcı düzenlemelerin uluslararası rekabete olumlu yansımalarını göz önünde bulundurarak, AB'nin veri koruması standardından ödün vermeden ticari olarak güçlü olabilmeyi ve sürdürülebilir rekabet avantajı sağlamayı ne kadar mümkün kılacağı gelecekte belli olacaktır.

Schrems II kararı, sadece AB'den ABD'ye kişisel veri aktarımları üzerine değil GDPR'da yer alan veri aktarımlarına ilişkin birçok hüküm üzerine etki ederek genel geçerliliği olacak bir çerçeve sağlamıştır. Karara göre veri aktarımı için yeni gereklilikler arasında veri sorumlularından verilerin aktarıldığı üçüncü ülkedeki korumanın yeterliliği hakkında inceleme ve doğrulama yapılması beklenmektedir. Bu durum, GDPR m.45'de yer alan Komisyonun üstlendiği rolün veri sorumlularına da yüklenmesi ve standart sözleşme maddelerinin uygulamada "mini yeterlilik kararı" olarak kullanılması sonucunu doğurmuştur[574]. Bu sorumluluğu yerine getirmenin güvenlikle ilgili mevzuatlara ulaşılması zor olan ülkelerde kolay olmayacağı ve dolayısıyla aktarımları daha da zorlaştıracağı düşünülmektedir.

[574] Bkz. Christopher Kuner, "The Schrems II Judgment of the Court of Justice and the Future of Data Transfer Regulation", *European Law Blog*, 17.07.2020, https://europeanlawblog.eu/2020/07/17/the-schrems-ii-judgment-of-the-court-of-justice-and-the-future-of-data-transfer-regulation/, Erişim Tarihi: 25.11.2021.

Ayrıca AB'nin veri aktarımında esas aldığı ve ABAD'ın ifade ettiği "esasen eşdeğerlilik" kavramı, ulusal denetim makamları ve ulusal mahkemeler üzerine de yükler yüklemektedir. ABAD'ın ulusal denetim makamlarına yüklediği üçüncü ülkelerde veri koruma düzeyini değerlendirme rolü düşünüldüğünde, bu görev ulusal denetim makamlarına kaynak yetersizliğinden dolayı üstesinden kalkamayacakları bir yük getirebilir[575].

Schrems II kararı sonrasında EDPB yayınlamış olduğu tavsiyelerle, işletmelerin üçüncü ülkedeki veri koruma seviyesini değerlendirmesine ve buna bağlı olarak ek önlemleri uygulamalarına ilişkin rehberlik sağlamış olsa da söz konusu tavsiyelere uyumun özellikle küçük ve orta büyüklükteki işletmeler için kolay olmayacağı aşikârdır. Bu durum uygulamada, GDPR 5. Bölüme uymak zorunda kalmamak adına veri sorumlusu ve veri işleyenleri veri yerelleştirme uygulamaları ile verileri AB içinde tutmaya zorlayacaktır[576]. Veri aktarım rejimi olarak veri yerelleştirmenin uygulanması hem küresel ekonomik düzenin devam etmesi hem de GDPR kapsamında kişisel veri aktarımlarının kolaylaştırılması amacına uygun olmadığı için tercih edilmeyen bir uygulamadır. Bu nedenle EDPB'nin ileriye dönük hazırlayacağı yeni tavsiye metinleri ile Schrems II kararı sonrasında veri sorumluları ve veri işleyenlerin aktarım hükümlerine uymasına ilişkin ortaya çıkan belirsizlikleri ve karmaşıklığı açıklığa kavuşturması gerekmektedir.

Son beş yılda ABAD'ın (Güvenli Liman ve Gizlilik Kalkanı kapsamında alınan) iki yeterlilik kararını geçersiz kılması ve bir uluslararası anlaşmayı (AB - Kanada PNR anlaşması) daha yürürlüğe girmeden iptal etmesi, AB'nin benimsediği veri aktarım kurallarının üçüncü ülkelerde makul bir şekilde uygulanma düşüncesi ile büyük ölçüde ters düşmüştür[577]. Ayrıca mahkemenin kararları uygulamada, üçüncü ülke yasalarının AB veri koruma kurallarında esas alınan esasen eşdeğerliğe uyum sağlamasını zorlaştırmıştır.

[575] Kuner, "Reality and illusion", s.894.
[576] Caroline Moen Rasmussen, "Transfer of Personal Data to Third Countries in a Post-Schrems II World", Master Thesis, University of Oslo, 2021, s.55.
[577] Kuner, "The Schrems II Judgment".

Gizlilik Kalkanının geçersiz kılındığı düşünüldüğünde, Komisyonun yüksek veri koruma standardını mevcut kılmak için GDPR m.45(2)'de yer alan koşulları tam olarak dikkate almadığı görülmektedir. Nitekim Kararın 164. Paragrafında Mahkemenin, Gizlilik Kalkanı Anlaşmasının ABD'nin ulusal güvenlik gereksinimlerine Gizlilik Kalkanının sağlaması gereken korumadan daha çok öncelik vermesine ve bu korumayı sınırlandırmasına ilişkin yaptığı eleştiri, Komisyonun aldığı yeterlilik kararının GDPR m.45(2)'de yer alan koşullara uyum sağlamadığının veya bu koşulları dikkate almadığının bir göstergesi sayılabilir.

Gizlilik Kalkanının geçersiz kılınması AB ve ABD arasında yapılacak transatlantik veri aktarımına ilişkin yasal bir boşluk meydana getirmiştir. Bu nedenle AB ve ABD arasında veri aktarımına izin veren bir anlaşmanın bir an önce yürürlüğe girmesi oldukça önemlidir. Bu bağlamda, Bölüm 2.1.5.3'de değinildiği üzere AB ile ABD arasında veri aktarımı için yetkili taraflar arasında yeni bir anlaşma için müzakereler yapılmaktadır. ABD'nin uluslararası ticaret açısından giderek daha hayati bir konu olan sınır ötesi veri aktarımlarının ekonomik faydalarından yararlanmaya devam etmesi için veri koruma yasalarında reformlar gerçekleştirmesi aciliyet göstermektedir[578]. ABD'nin veri korumaya ilişkin yapacağı reformlar, AB ve ABD arasında kişisel veri aktarımına ilişkin yapılacak yeni anlaşmanın Güvenli Liman ve Gizlilik Kalkanının uğradığı akıbete uğramaması için son derece önemli ve belirleyici olacaktır.

AB - ABD veri aktarımlarında yeterlilik kararı yerine davranış kuralları ve sertifikasyon mekanizmaları gibi GDPR ile getirilen yeni aktarım mekanizmalarının geliştirilmesi ve aktif hale getirilmesiyle daha uygulanabilir bir sonuç elde edebilir. Zira standart sözleşme maddeleri ile aktarımlarda Schrems II kararı ile zorlaşmıştır. Şuana kadar henüz onaylanmış bir davranış kuralı ve sertifikasyon mekanizması bulunmasa da, potansiyel bir aktarım seçeneği olarak gelecekte kullanılması muhtemeldir.

[578] Skahill, "Trans-Atlantic data flows".

AB'nin üçüncü ülkelere yönelik yeterlilik kararı alması, kendi veri koruma standardını küresel düzeyde kabul ettirmesi için uygun bir yol olarak görülmektedir. Fakat küresel dünyanın büyük bir aktörü olan ABD'nin bu standarda uyum sağlamaması, AB veri koruma standardının küresel düzeyde benimsenmesine engel olmaktadır. Komisyonun, Güvenli Liman ve Gizlilik Kalkanı Anlaşmaları ile ABD'de veri korumasına ilişkin yeterliliği bulma girişimleri, söz konusu anlaşmaların ABAD tarafından geçersiz kılınmaları ile başarısızlığa uğramıştır. Komisyonun ticaret gücünün de zorlamasıyla AB'den ABD'ye veri aktarımları için yeterlilik kararı alma isteğinin devam etmesi halinde, yeterlilik kararının bir formalite olarak algılanması durumu ortaya çıkacaktır[579]. Ayrıca, üçüncü ülkelerin AB veri koruma standardını örnek alması için yoğun bir şekilde uğraşarak AB ile müzakereler yapması, yapılan anlaşma ve yeterlilik kararlarının mahkeme tarafından iptal edilme akıbetine uğraması riski de düşünüldüğünde söz konusu ülkeler tarafından sorgulanacak ve üçüncü ülkelerin GDPR'ı örnek alma isteklerini önemli derecede etkileyecektir.

Öte yandan GDPR ile veri aktarımı ihlallerine karşı getirilen yüksek cezalar göz önünde bulundurulduğunda şirketlerin veri aktarımlarını GDPR'da yer alan mekanizmalara uygun olarak gerçekleştirmeleri ve bunu gerçekleştirebilmek için uygun teknik ve organizasyonel tedbirleri uygulamaları gerekmektedir. Bu kapsamda şirketlerin, Komisyon tarafından aktarım mekanizmalarının periyodik incelemesi sonucu oluşabilecek değişikliklere dikkat etmeleri ve ortaya çıkacak değişikliklere karşı kendilerini güncellemelerinin önemli olduğu görülmektedir.

AB dışına veri aktarabilmenin bir yolu da uluslararası anlaşmalar düzenlemektir. Bu kapsamda AB'nin Kanada ile yaptığı PNR anlaşmasına ilişkin ABAD'ın 1/15 sayılı görüşünde yüksek veri koruma düzeyini gerekli görmesi ve AB Hukukuna tam uygunluk istemesi, AB'nin kişisel verilerin aktarımını kapsayan küresel veri paylaşımı ve uluslararası ticaret gibi konularda uluslararası anlaşma yapma

[579] Chen, s.48.

imkânını kısıtlamıştır. Ayrıca, GDPR'da uluslararası anlaşmalara sadece Gerekçe 102'de yer verilmesi uluslararası anlaşma yapma imkânını kısıtlamaktadır. Günümüz dünyasında kişisel verilerin aktarımı uluslararası ticaretin önemli bir yapıtaşı ve olmazsa olmazı olarak görülmektedir. Kişisel verilerin aktarımı için uluslararası anlaşma düzenlemek veya bu anlaşmalara taraf olmak, veri aktarımını daha kolay hale getirmesinin yanında ticari olarak da avantaj sağlayabilir. ABAD'ın 1/15 sayılı görüşü, üçüncü ülkelerin AB ile veri aktarımına ilişkin anlaşma yapmak için kaynak harcamaları konusunda tereddütler doğurmuş ve AB'nin gelecekte üçüncü ülkelerle veri paylaşımına ilişkin yapmak istediği anlaşmalar için müzakerelerde elini zorlaştırmıştır[580].

AB'nin veri koruması için küresel bir referans noktası olarak konumlandırdığı GDPR, bir başarı hikâyesi olarak birçok ülke tarafından benimsenerek örnek alınmıştır. Şüphesiz ABAD'ın kişisel veri aktarımına ilişkin almış olduğu kararlar da veri aktarımlarının geleceği ve mevzuatın uygulanması bakımından belirleyici olmuştur. AB veri koruma standartlarını örnek alan birçok üçüncü ülke olduğu düşünüldüğünde, özellikle Schrems II kararının dünyanın çoğunu etkileyebileceği ve AB ve ABD arasındaki transatlantik veri aktarımına yeni bir boyut kazandırdığı söylenebilir. ABAD, aktarılan kişisel verilere AB Hukukuna eşdeğer bir koruma sağlanması standardını tanımlamasıyla veri koruma seviyesini küresel olarak oldukça yükseltmiştir. AB Hukukunun sağladığı veri koruma standardı, örnek alınacak bir model olması için elbette yüksek düzeyde olmalıdır. Ancak uygun dengeyi sağlamak için bu yüksek standardın üçüncü ülkelerin uygulayabileceği düzeyde olması gerektiği de unutulmamalıdır.

AB'de üçüncü ülkelere veri aktarımı konusu her geçen gün daha çok önem kazanmaktadır. ABAD'ın bu konuya ilişkin davalarda aldığı kararlarda aktarımların geleceğinin şekillenmesinde etkili olmaktadır. İnternetin gelişmesine paralel olarak gelecekte aktarımların daha karmaşık hale geleceği gerçeğine binaen

[580] Kuner, "Data Protection, Data Transfers".

veri koruması için GDPR'da yer alan aktarıma ilişkin hükümlerin yetersiz kalabilmesi muhtemeldir. Nitekim ABAD, GDPR'ı dikkate alarak hazırlanan Gizlilik Kalkanı Anlaşmasını geçersiz kılarak daha çok veri koruma ve ilave önlem içeren yeni bir AB-ABD anlaşmasının gerekli olduğunu belirlemiş ve veri aktarımında kuralları baştan yazmıştır. Komisyonun standart sözleşme maddelerini güncellemesi de bu gerekliliğinin bir işaretidir. AB'nin veri aktarımlarında hangi yöntemi kullanmayı uygun görürse görsün, tutarlı bir yaklaşım benimsemesi ve ilgili kişilerin kişisel verilerinin korunması düzeyinin zarar görmemesi ilkesine uyması önemli olacaktır.

GDPR ile KVKK'nın yurtdışına kişisel veri aktarımına ilişkin yaklaşımlarında benzerlikler olsa da KVKK'da aktarıma ilişkin esas alınan ana ilkenin GDPR'dan farklı olduğu ve aktarım mekanizmalarının yetersiz kaldığı görülmektedir. KVKK'da aktarıma ilişkin ana ilke olan ilgili kişiden açık rıza alınarak aktarım yapıldığında, aktarılan veriler için koruma sağlanmamakta sadece aktarım için yasal dayanak sağlanmış olmaktadır. Bu noktada KVKK'nın uygulamada kişisel veriler için yeterince koruyucu bir yaklaşıma sahip olmadığı ve veri akışını kolaylaştırmadığı söylenebilir.

Bir tarafta teknolojinin gün geçtikçe gelişmesi diğer tarafta kişisel verilerin korunması düşünüldüğünde teknoloji ve veri koruması arasında uygun bir dengenin sağlanması gerekmektedir. Bu noktada KVKK'da hem veri korumasının hem de veri akışının sağlanması için model alınabilecek olan düzenleme de GDPR'da yer alan aktarım mekanizmalarıdır. GDPR'da kişisel veri aktarımlarında esas alınan anlayış, AB içinde verilere sağlanan korumanın verilerin aktarıldığı üçüncü ülkede de devam etmesidir. Bu anlayışın KVKK'da da yer alması, Türkiye'deki bireylerin kişiler verilerinin üçüncü ülkelerde korunmasının devam etmesi bakımından KVKK'nın GDPR ile uyumunu sağlayacaktır. Bu amaçla KVKK'da GDPR'da olduğu gibi aktarımlarda ilk yöntemin, ilgili kişilerden açık rıza alınması yöntemine göre değil verilerin aktarılacağı ülkede yeterli korumanın bulunup bulunmamasına göre düzenlenmesi uygun olacaktır. Kişisel verilerin korunmasına ilişkin

KVKK'nın gelişimi ve GDPR'a uyumu, Türkiye'nin AB ile olan ekonomik, hukuki ve siyasi ilişkileri bakımından oldukça önemlidir.

Yeterli koruma olmadığında ise, standart sözleşme maddeleri, davranış kuralları ve sertifikasyon mekanizmaları gibi uygun güvenceler kullanılarak aktarım yapılabilir. Özellikle sertifikasyon mekanizması yöntemiyle, veri aktarılanlar sahip olduğu sertifika ile kişisel veriler için yeterli koruma sağladıkları konusunda uygun güvence sağlarlar. Günümüzde birçok şirketin kullandığı bulut depolama hizmeti sağlayıcıları olan veri sorumlusu ve veri işleyenlerin böyle bir sertifikaya sahip olması, bu sağlayıcıların depoladıkları veriler için aldıkları güvenlik önlemlerinin sürekli güncel ve yeterli olması konusunda denetlenmelerine imkân verecektir. KVKK'da yer alacak sertifikasyon mekanizmasında sertifikanın geçerli olduğu azami sürenin GDPR'dan farklı olarak daha kısa olması, gittikçe zorlaşan veri korumasının sürekliliğini sağlayabilir.

KVKK'da yer alan taahhütname yöntemi standart sözleşme maddeleri ile benzerdir. Aralarındaki fark ise taahhütname için Kurul'dan izin alınması gerektiğidir. Bu noktada taahhütnameler, GDPR m.46(2)(b)'de yer alan Komisyon tarafından yayınlanan standart sözleşme maddeleri gibi düzenlenip tekrardan Kuruldan spesifik bir izin alınmadan kullanılabilir hale getirilebilir. Bunun haricinde taahhütnameler için yapılabilecek başka bir öneri ise, GDPR'da yer alan davranış kuralları ve sertifikasyon mekanizmasında olduğu gibi KVKK m.9(2)(b) uyarınca taahhütte bulunan veri sorumlusu ve veri işleyenlerin söz konusu taahhütlere uyup uymadığını kontrol etmek, izlemek ve uyumu sağlamak için Kurul'un akredite edeceği özel bir organ atanmasıdır. Uygulamada taahhütname yönetiminin etkin ve hızlı işlemesi ve taahhütnamelere uyumun sağlanması için bu organın atanması önemli bir adım olacaktır.

KAYNAKÇA

KİTAP, MAKALE VE TEZLER

Aşıkoğlu, Şehriban İpek, Fatih Burak Uzun. "Kişisel Verilerin Yurtdışına Aktarımının Açık Rızaya Dayandırılmasının Yarattığı Sorunlar ve Çözüm Önerileri". *Prof. Dr. Türkan Rado'nun Anısına Armağan,* İstanbul: On İki Levha Yayıncılık, 2020:921-968.

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,* Ankara: Ocak 2009:19-21.

Bilgi Information Technology Law Institute "Kişisel Verilerin Korunmasına İlişkin Düzenlemeler Çerçevesinde Uluslararası Veri Aktarımı Yeni Gelişmeler ve Uygulamaya İlişkin Hukuki Değerlendirmeler". İstanbul: 2020. https://itlaw.bilgi.edu.tr/media/2020/3/30/Final%20Veri_Aktarimi_Raporu_30.03.2020.pdf. Erişim Tarihi: 15.11.2021.

Chen, Siyuan. "Cross-border Data Transfer After Schrems II: The Globalization of EU Standards of Data Protection Through Adequacy Decisions or Trade Agreements?". Master Thesis, Lund University, Spring 2021.

Compagnucci, Marcelo Corrales, Mateo Aboy, Timo Minssen. "Cross-Border Transfers of Personal Data after Schrems II: Supplementary Measures and New Standard Contractual Clauses (SCCs)". October 27, 2021. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3951085. Erişim Tarihi: 30.11.2021.

Çekin, Mesut Serdar. *Avrupa Birliği Hukukuyla Mukayeseli olarak 6698 Sayılı Kişisel Verilerin Korunması Kanunu*. İstanbul: On iki Levha Yayıncılık, 2018.

Dülger, Murat Volkan, "Yurtdışına Veri Aktarımında Milyonluk Ceza: Kişisel Verileri Koruma Kurulunun Amazon Kararı". 24 Şubat 2021. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3792388. Erişim Tarihi: 13.11.2021.

Dülger, Murat Volkan, Cansu Ceren Kahraman. "KVKK'dan Kişisel Verilerin Yurt Dışına Aktarımında Önemli Bir Adım: Bağlayıcı Şirket Kuralları". 24 Şubat 2021. https://ssrn.com/abstract=3792375. Erişim Tarihi: 14.10.2021.

Dülger, Murat Volkan, Cansu Ceren Kahraman. "GDPR ve KVKK Ekseninde Bağlayıcı Şirket Kuralları". *Hukuk ve Daha Fazlası*. 26 Mayıs 2021. https://ssrn.com/abstract=3853724. Erişim Tarihi: 14.10.2021.

Dülger, Murat Volkan. "Kişisel Verileri Koruma Kurulu'nun 108 Sayılı Sözleşme Hakkındaki Kararı ve Yurt Dışına Veri Aktarımı Sorunu". 24 Şubat 2021. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3792396. Erişim Tarihi: 01.12.2021.

Dülger, Murat Volkan. *Kişisel Verilerin Korunması Hukuku*. İstanbul: Hukuk Akademisi, 2020.

Giakoumopoulos, Christos, Giovanni Buttarelli ve Michael O'Flaherty. *Handbook on European Data Protection Law*. Luxembourg: Publications Office of the European Union, 2018.

Gür, Berna Akçalı. "Uluslararası Hukuk ve AB Hukuku Boyutuyla Kişisel Verilerin Yurt Dışına Aktarılması". *Marmara Üniversitesi Hukuk Fakültesi Hukuk Araştırmaları Dergisi,* 25/2 (Aralık 2019):850-872.

Gürses, Bekir. "AB ve Türk Hukukunda Kişisel Verilerin Korunması- Mevzuat Uyumuna Yönelik Bir Değerlendirme". Yüksek Lisans Tezi, Marmara Üniversitesi, 2019.

Kızılırmak, Baran."Cross-Border Transfer of Personal Data Under GDPR Regime and Turkish Legal Framework". Master Thesis, University Of Hamburg, September 2020.

Kuner, Christopher. "Reality and Illusion in EU Data Transfer Regulation Post Schrems". *German Law Journal*. 18 /04 (2017):882-919.

Kuner, Christopher. "Data Protection, Data Transfers, and International Agreements: The CJEU's Opinion 1/15". 26.07.2017. https://verfassungsblog.de/data-protection-data-transfers-and-international-agreements-the-cjeus-opinion-115/. Erişim Tarihi: 15.10.2021.

Kuner, Christopher. "Schrems II Re-Examined", 25.10.2020. https://verfassungsblog.de/schrems-ii-re-examined/. Erişim Tarihi: 19.10.2021.

Kuner, Christopher. *Transborder Data Flows and Data Privacy Law*. Oxford Scholarship Online, September 2013.

Kuner, Christopher, Lee Bygrave ve Christopher Docksey.*The EU General Data Protection Regulation (GDPR): A Commentary*. Oxford University Press, 2020.

Kuner, Christopher, Lee Bygrave ve Christopher Docksey. *The EU General Data Protection Regulation (GDPR): A Commentary / Update of Selected Articles*. Oxford University Press, 2021.

Küzeci, Elif. *Kişisel Verilerin Korunması*. 3. Baskı, Ankara: Oniki Levha Yayınları, 2019.

Özkan, Oğulcan. "Kişisel Verilerin Korunması". Yüksek Lisans Tezi, Ankara Üniversitesi, 2019.

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*. 8/04 (2018): 318-337.

Toparlak, Rüya Tuna. "Veri Koruması Hukukunda Bağlayıcı Şirket Kuralları: 2016/679 Sayılı Genel Veri Koruma Tüzüğü ve 6698 Sayılı Kişisel Verilerin Korunması Kanunu Karşılaştırması". Yüksek Lisans Tezi, Türk Alman Üniversitesi, İstanbul: Şubat 2021.

Theodorakis, Nikolaos I. "Cross Border Data Transfers Under the GDPR: The Example of Transferring Data from the EU to the US". *TTLF Working Papers*, 39/1 (2018).

Türkiye Bilişim Derneği. "1. Çalışma Grubu Raporu: Sınır Aşan Veri*". Kamu Bilgi İşlem Merkezleri Yöneticileri Birliği Kamu Bilişim Platformu XXII*. Aralık 2019.

Rasmussen, Caroline Moen."Transfer of Personal Data to Third Countries in a Post-Schrems II World". Master Thesis, University of Oslo, 2021.

Weber, Rolf H., Dominic Staiger, *Transatlantic Data Protection in Practice*. Springer, 2017.

Van den Bulck, Paul. "Transfers of Personal Data to Third Countries". *ERA Forum.* 18/ 02 (2017):229-247.

Voss, W. Gregory. "Cross-Border Data Flows, the GDPR, and Data Governance". *Washington International Law Journal*. 29/3 (2020): 485-531.

BELGE, GÖRÜŞ, RAPOR VE REHBERLER

Article 29 Working Party. "Adequacy Referential". 06.02.2018, ("WP254", rev 1), https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=614108 , Erişim Tarihi: 28.06.2021.

Article 29 Working Party. "Guidelines on Consent under Regulation 2016/679", ("WP 259" rev.1). 7.06.2018, https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=623051 , Erişim Tarihi: 30.11.2021.

Article 29 Working Party. "Transfers of personal data to third countries; Applying Articles 25 and 26 of the EU data protection directive ("WP12")". 24.07.1998. https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/1998/wp12_en.pdf, Erişim Tarihi: 1.10.2021.

Article 29 Working Party. "Working document on a common interpretation of Article 26 (1) of Directive 95/46 of 24 October 1995 ("WP 114")". 25 November 2005. https://www.pdpjournals.com/docs/88080.pdf, Erişim Tarihi: 11.10.2021.

Article 29 Working Party. “Working Document on Binding Corporate Rules for Controllers (WP256 rev.01)”. 09.02.2018. https://ec.europa.eu/newsroom/article29/items/614109. Erişim Tarihi: 26.10.2021.

Article 29 Working Party. “Working Document on the approval procedure of the Binding Corporate Rules for controllers and processors (WP 263 Rev.01)”.16 Nisan 2018, https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=623056, Erişim Tarihi: 26.10.2021.

Congressional Research Service. “U.S.-EU Privacy Shield and Transatlantic Data Flows”. September 22,2021.

European Data Protection Board. “Guidelines 2/2018 on derogations of Article 49 under Regulation 2016/679”. 25.05.2018. https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_2_2018_derogations_en.pdfs . Erişim Tarihi: 16.12.2021.

European Data Protection Board. “Guidelines 03/2020 on the processing of data concerning health for the purpose of scientific research in the context of the COVID-19 outbreak”. 21.04.2020. https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_202003_healthdatascientificresearchcovid19_en.pdf. Erişim Tarihi: 01.01.2022.

European Data Protection Board. “Guidelines 04/2021 on codes of conduct as tools for transfers”. 7.07.2021. https://edpb.europa.eu/system/files/2021-07/edpb_guidelinescodesconducttransfers_publicconsultation_en.pdf, Erişim Tarihi: 21.11.2021.

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. https://edpb.europa.eu/our-work-tools/documents/public-consultations/2021/guidelines-052021-interplay-between-application_en. Erişim tarihi: 22.12.2021.

European Data Protection Board. "Information note on BCRs for companies which have ICO as BCR Lead Supervisory Authority". 12.02.2019. https://edpb.europa.eu/sites/default/files/files/file1/edpb-2019-02-12-infonote-bcrs-brexit_en_0.pdf. Erişim Tarihi: 26.10.2021.

European Data Protection Board. "Opinion 24/2020 on the draft decision of the Norwegian Supervisory Authority regarding the Controller Binding Corporate Rules of Jotun". 31.07.2020. https://edpb.europa.eu/sites/default/files/files/file1/edpb_opinion202024_bcrcontrollerjotun_en.pdf. Erişim Tarihi: 14.10.2021.

European Data Protection Board. "Opinion 25/2020 on the draft decision of the Swedish Supervisory Authority regarding the Controller Binding Corporate Rules of Tetra Pak". 31.07.2020. https://edpb.europa.eu/sites/default/files/files/file1/edpb_opinion202025_bcr-c_tetrapak_en.pdf. Erişim Tarihi: 14.10.2021.

European Data Protection Board. "Recommendations 01/2020 on measures that supplement transfer tools to ensure complaince with the EU level of protection of personel data". 18.06.2021.

European Data Protection Supervisor. "The transfer of personal data to third countries and international organisations by EU institutions and bodies". Position Paper. 14.07.2014, https://edps.europa.eu/sites/edp/files/publication/14-07-14_transfer_third_countries_en.pdf. Erişim Tarihi: 01.01.2022.

European Data Protection Supervisor. “Strategy for Union institutions, offices, bodies and agencies to comply with the Schrems II Ruling”. 29.01.2020. https://edps.europa.eu/data-protection/our-work/publications/papers/strategy-union-institutions-offices-bodies-and_en. Erişim Tarihi: 21.10.2021.

Kişisel Verileri Koruma Kurumu. “Doğru Bilinen Yanlışlar Dokümanı”. https://kvkk.gov.tr/SharedFolderServer/CMSFiles/ca752cda-c3df-4645-8d5e-e2a507e63200.pdf. Erişim Tarihi: 8.10.2021.

Kişisel Verileri Koruma Kurumu. “Açık Rıza Rehberi”. https://kvkk.gov.tr/yayinlar/A%C3%87IK%20RIZA.pdf. Erişim Tarihi: 14.10.2021.

Kişisel Verileri Koruma Kurumu. “Yurtdışına Aktarım”. https://www.kvkk.gov.tr/Icerik/2053/Yurtdisina-Aktarim. Erişim Tarihi: 16.12.2021.

Kişisel Verileri Koruma Kurumu. “Madde Ve Gerekçesi İle Kişisel Verilerin Korunması Kanunu (Bilgi Notu) Ve Kişisel Verilerin Korunmasına İlişkin Terimler Sözlüğü”. https://www.kvkk.gov.tr/Icerik/5388/Madde-ve-Gerekcesi-ile-Kisisel-Verilerin-Korunmasi-Kanunu-Bilgi-Notu-ve-Kisisel-Verilerin-Korunmasina-Iliskin-Terimler-Sozlugu. Erişim Tarihi: 13.11.2021.

Kişisel Verileri Koruma Kurumu. “Açık Rıza Alırken Dikkat Edilecek Hususlar”. https://www.kvkk.gov.tr/Icerik/2037/Acik-Riza-Alirken-Dikkat-Edilecek-Hususlar. Erişim Tarihi: 01.01.2022.

Information Commissioner’s Office. “Guide to the General Data Protection Regulation (GDPR)”, https://ico.org.uk/media/for-organisations/guide-to-

data-protection/guide-to-the-general-data-protection-regulation-gdpr-1-1.pdf. Erişim Tarihi: 28.11.2021.

PwC. "Binding Corporate Rules". https://www.pwc.com/m1/en/publications/documents/pwc-binding-corporate-rules-gdpr.pdf. Erişim Tarihi: 26.11.2021.

KARARLAR

Court of Justice of European Union. *Opinion of Advocate General Saugmandsgaard Øe in Case C-311/18", Data Protection Commissioner v. Facebook Ireland Limited and Maximilian Schrems, delivered on 19 December 2019*. ECLI:EU:C:2019:1145.

Court of Justice Of European Union. *Opinion 1/15 of the Court of Justice (Grand Chamber)*, ECLI:EU: C:2017:592.

Court of Justice of the European Union. C-362/14, *Maximilian Schrems v. Data Protection Commissioner [GC] ("Schrems I"*). 6 October 2015.

Court of Justice of the European Union. Case C-101/01, *Bodil Lindqvist.* 2003 E.C.R. I-12971.

Court of Justice of the European Union. *Case C-311/18, Data Protection Commissioner v. Facebook Ireland Limited and Maximilian Schrems [GC] ('Schrems II')*. 16 July 2020.

Court of Justice of the European Union. *Opinion of Advocate General Bot in Case C- 362/ 14 Schrems I*, EU:C:2015:627.

Irish High Court. *Data Protection Commissioner v. Facebook Ireland Limited and Maximilian Schrems.*

Joined Cases C-317/04 and C-318/04, European Parliament v Council and Commission, EU:C:2006:346.

Kişisel Verileri Koruma Kurulu. "Amazon Turkey Perakende Hizmetleri Limited Şirketi hakkındaki başvuru ile ilgili 27.02.2020 Tarihli ve 2020/173 Sayılı Kararı Özeti". https://www.kvkk.gov.tr/Icerik/6739/2020-173. Erişim Tarihi: 15.11.2021.

Kişisel Verileri Koruma Kurulu. "Kişisel verilerin 108 Sayılı Sözleşme dayanak gösterilerek yurt dışına aktarılması hakkında 22.07.2020 tarih ve 2020/559 sayılı Karar Özeti". https://kvkk.gov.tr/Icerik/6790/2020-559. Erişim Tarihi: 15.11.2021.

Kişisel Verileri Koruma Kurulu. "Yeterli korumanın bulunduğu ülkelerin tayininde kullanılmak üzere oluşturulan form" hakkında 02.05.2019 tarihli ve 2019/125 sayılı karar Özeti". https://www.kvkk.gov.tr/Icerik/5469/-Yeterli-korumanin-bulundugu-ulkelerin-tayininde-kullanilmak-uzere-olusturulan-form-hakkindaki-02-05-2019-tarihli-ve-2019-125-sayili-Kurul-Karari. Erişim Tarihi: 01.01.2022.

Kişisel Verileri Koruma Kurulu. "Kurumsal e-posta hizmetinin, Google (Gmail) üzerinden yine aynı uzantıya sahip olarak kullanılıp kullanılamayacağına ilişkin 31.05.2019 tarihli ve 2019/157 sayılı karar özeti". https://www.kvkk.gov.tr/Icerik/5493/2019-157. Erişim Tarihi: 15.11.2021.

Norwegian Data Protection Authority."Decision of the Norwegian Data Protection Authority Approving Binding Corporate Rules of Jotun Group".

18.08.2020. https://edpb.europa.eu/sites/default/files/bcr_decision_sa/no_final_decision_bcr-c_jotun20200818.pdf. Erişim Tarihi: 12.10.2021.

Swedish Data Protection Authority."Decision Approving the Binding Corporate Rules of Tetra Pak Group".17 August 2020. https://edpb.europa.eu/sites/default/files/bcr_decision_sa/se_sa_final_decision_bcr-c_tetra-pak_2020081_7_en.pdf. Erişim Tarihi: 12.10.2021.

MEVZUAT

Asia Pacific Economic Cooperation (APEC). "Privacy Framework" (2005). https://www.apec.org/publications/2005/12/apec-privacy-framework. Erişim Tarihi: 9.10.2021.

Accession Partnership Document for Turkey. "Council Decision of 8 March 2001 on the principles, priorities, intermediate objectives and conditions contained in the Accession Partnership with the Republic of Turkey". 2001/235/EC. https://www.ab.gov.tr/files/AB_Iliskileri/Tur_En_Realitons/Apd/Turkey_APD_2001.pdf. Erişim Tarihi: 9.10.2021.

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, OJ L 34.

Commission Implementing Decision (EU) 2016/2297 of 16 December 2016 amending Decisions 2001/497/EC and 2010/87/EU on standard contractual clauses for the transfer of personal data to third countries and to processors

established in such countries, under Directive 95/46 of the European Parliament and of the Council, OJ 2016/ L344.

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. https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/standard-contractual-clauses-scc/standard-contractual-clauses-international-transfers_en. Erişim Tarihi: 21.10.2021.

Commission Implementing Decision (EU) 2021/914 of 4.6.2021, Annex Section I. https://eurlex.europa.eu/eli/dec_impl/2021/914/oj?uri=CELEX%3A32021D0914&locale=en. Erişim Tarihi: 30.11.2021.

Commission Implementing Decision (EU) 2021/914 of 4.6.2021, Annex Section II. https://eurlex.europa.eu/eli/dec_impl/2021/914/oj?uri=CELEX%3A32021D0914&locale=en, Erişim Tarihi: 30.11.2021.

Commission Implementing Decision of 28.6.2021 pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council on the adequate protection of personal data by the United Kingdom".

Commission Implementing Decision of 28.6.2021 pursuant to Directive (EU) 2016/680 of the European Parliament and of the Council on the adequate protection of personal data by the United Kingdom".

Consolidated version of the Treaty on the Functioning of the European Union, (2012), OJ C 326/47.

Council Decision 2010/412/ of 13 July 2010 on the conclusion of the 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 the purposes of the Terrorist Finance Tracking Program 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 the purposes of the Terrorist Finance Tracking Program. [2010] OJ L195/3

Council of Europe. "Convention on Cybercrime". ETS No. 185. https://www.coe.int/en/web/conventions/full-list?module=treaty-detail&treatynum=185. Erişim Tarihi: 9.10.2021.

Council of Europe."Modernised Convention for the Protection of Individuals with Regard to the Processing of Personal Data". https://rm.coe.int/convention-108-convention-for-the-protection-of-individuals-with-regar/16808b36f1. Erişim Tarihi: 9.10.2021.

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". ETS No.181. https://rm.coe.int/1680080626. Erişim Tarihi: 9.10.2021

Council of Europe. "Convention for the protection of individuals with regard to automatic processing of personal data". ETS No.108. https://rm.coe.int/16808ade9d. Erişim Tarihi: 9.10.2021.

Decision of the Council and the Commission of 13 December 1993 on the conclusion of the Agreement on the European Economic Area between the European Communities, their Member States and the Republic of Austria, the Republic of Finland, the Republic of Iceland, the Principality of

Liechtenstein, the Kingdom of Norway, the Kingdom of Sweden and the Swiss Confederation, OJ 1994 L 1.

Decision of the EEA Joint Committee No 154/2018 of 6 July 2018 amending Annex XI (Electronic communication, audiovisual services and information society) and Protocol 37 (containing the list provided for in Article 101) to the EEA Agreement [2018/1022].

European Commission. "Commission Decision 2000/520 of 26 July 2000 Pursuant to Directive 95/46 of the European Parliament and of the Council on the Adequacy of the Protection Provided by the Safe Harbour Privacy Principles and Related Frequently Asked Questions Issued by the US Department of Commerce". 2000 OJ/L 215.

European Commission. "Commission Decision 2001/497/EC of 15 June 2001 on standard contractual clauses for the transfer of personal data to third countries under Directive 95/46". OJ 2001/L 181.

European Commission. "Commission Decision 2002/2/EC of 20 December 2001 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequate protection of personal data provided by the Canadian Personal Information Protection and Electronic Documents Act". OJ 2001/ L213.

European Commission. "Commission Decision 2004/915/EC of 27 December 2004 amending Decision 2001/497/EC as regards the introduction of an alternative set of standard contractual clauses for the transfer of personal data to third countries". OJ 2004 / L 385.

European Commission."Commission Decision 2010/87 of 5 February 2010 on standard contractual clauses for the transfer of personal data to processors

established in third countries under Directive 95/46 of the European Parliament and of the Council". OJ 2010/ L 39.

European Commission. "Communication from the Commission to the European Parliament and the Council, Exchanging and Protection Personal Data in a Globalised World". COM(2017)final. 10.01.2017. http://ec.europa.eu/newsroom/document.cfm?doc_id=41157. Erişim Tarihi: 23.12.2021.

European Commission. "Standard Contractual Clauses for controllers and processors in the EU". 4 June 2021. https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/standard-contractual-clauses-scc_en. Erişim Tarihi: 21.10.2021.

European Union. "Charter of Fundamental Rights of the European Union". OJ 2012/C 326.

European Union."Agreement between the European Community and the Government of Canada on the processing of Advance Passenger Information and Passenger Name Record data". OJ/L82. 21.3.2006. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A22006A0321%2801%29. Erişim Tarihi: 9.12.2021.

European Union. "Agreement between the European Union and Australia on the processing and transfer of Passenger Name Record (PNR) data by air carriers to the Australian Customs and Border Protection Service". OJ L 186. 14.7.2012. https://eur-lex.europa.eu/legal content/EN/TXT/?uri=CELEX%3A22012A0714%2801%29&qid=1638794233250 , Erişim Tarihi: 12.10.2021.

European Union. "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 [2016]". OJ L336/3. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:22016A1210(01)&rid=3. Erişim Tarihi: 9.10.2021.

European Union. "Agreement between the United States of America and the European Union on the use and transfer of passenger name records to the United States Department of Homeland Security", OJ L 215. 11.8.2012. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A22012A0811%2801%29. Erişim Tarihi: 12.10.2021.

European Union. "Agreement between the European Community and the United States of America on the processing and transfer of PNR data by air carriers to the United States Department of Homeland Security, Bureau of Customs and Border Protection". OJ/L183.20.5.2004. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A22004A0520%2801%29&qid=1639127925151. Erişim Tarihi: 12.10.2021.

European Union. "Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (1995) OJ L281/31".

European Union. "Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such

data, and repealing Council Framework Decision 2008/977/JHA, OJ 2016 L119".

European Union."Directive (EU) 2016/681 of the European Parliament and of the Council of 27 April 2016 on the use of passenger name record (PNR) data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime, OJ 2016 L 119/132".

European Union. "Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (2016)". L 119/1.

European Union. "Regulation (EU) No.182/2011 of the European Parliament of the Council of 16 February 2011 Laying down the rules and general principles concerning mechanism for control by Member States of the Commissions exercise of implementing Powers".OJ 2011 L 55/13.

Hague Evidence Convention. "Convention of 18 March 1970 on the Taking of Evidence Abroad in Civil or Commercial Matters. https://www.hcch.net/en/instruments/conventions/full-text/?cid=82 Erişim Tarihi: 9.10.2021.

Organisation For Economic Co-Operation and Development (OECD), "The OECD Privacy Framework(2013)".https://www.oecd.org/sti/ieconomy/privacy-guidelines.htm . Erişim Tarihi: 9.10.2021.

Trade and Cooperation Agreement between the European Union and the European Atomic Energy Community, of the One Part, and the United Kingdom of Great Britain and Northern Ireland, of the Other Part, OJ 2020 L 444/14.

Türkiye Cumhuriyeti Anayasası, Kanun Numarası: 2709, Kabul Tarihi: 18.10.1982, Resmi Gazete: 9.11.1982/ 17863.

İNTERNET KAYNAKLARI

Agencia İspanola Proteccion Datos (AEPD). https://www.aepd.es/es/documento/ps-00059-2020.pdf. Erişim Tarihi: 23.10.2021.

Amazon Turkey için verilen taahhütname izni için bkz. https://www.kvkk.gov.tr/Icerik/6898/TAAHHUTNAME-BASVURUSU-HAKKINDA-DUYURU. Erişim Tarihi: 01.01.2022.

Asylegal. "Uluslararası Veri Aktarımı & KVKK Amazon Türkiye Kararı". https://www.asylegal.com/tr/uluslararasi-veri-aktarimi-kvkk-amazon-turkiye-karari. Erişim Tarihi: 15.11.2021.

Braun, Martin and others. "European Commission adopts and publishes new Standard Contractual Clauses for international transfers of personal data". 7 June 2021. https://www.wilmerhale.com/en/insights/blogs/wilmerhale-privacy-and-cybersecurity-law/20210607-european-commission-adopts-and-publishes-new-standard-contractual-clauses-for-international-transfers-of-personal-data. Erişim Tarihi: 30.11.2021.

Data Protection Commission. "Transfers of Personal Data to Third Countries or International Organisations". https://www.dataprotection.ie/en/organisations/international-transfers/transfers-personal-data-third-countries-or-international-organisations. Erişim Tarihi: 20.11.2021.

European Commission. “European Commission Calls on the U.S. To Restore Trust in EU-U.S. Data Flows”. Press Release, 27.11.2013.

European Commission. “Intensifying Negotiations on transatlantic Data Privacy Flows: A Joint Press Statement by European Commissioner for Justice Didier Reynders and U.S. Secretary of Commerce Gina Raimondo”. 25 March 2021. https://ec.europa.eu/commission/presscorner/detail/en/STATEMENT_21_1443. Erişim Tarihi: 26.11.2021.

European Commission. “Statement by Commissioner Věra Jourová on the European Parliament consent vote on the conclusion of the EU-U.S. data protection Umbrella Agreement". 1 December 2016. https://ec.europa.eu/commission/presscorner/detail/en/STATEMENT_16_4182.Erişim Tarihi: 9.10.2021.

Gordon, Philip, Zoe Argento ve Kwabena Appenteng. “The European Union’s New Standardized Data Transfer Agreement: Implications for Multinational Employers”. 9 June 2021. https://www.littler.com/publication-press/publication/european-unions-new-standardized-data-transfer-agreement-implications. Erişim Tarihi: 30.11.2021.

Güngör, Deniz. “Avrupa Birliği'nden ABD'ye Yapılacak Veri Aktarımlarına İlişkin Gizlilik Kalkanı Anlaşmasının İptali”. *Mondaq*. September 30,2020. https://www.mondaq.com/turkey/privacy-protection/989728/avrupa-birli287i39nden-abd39ye-yapilacak-veri-aktarimlarina-304li351kin-gizlilik-kalkani-anla351masinin-304ptali-. Erişim Tarihi:7.10.2021.

Güngör, Deniz. “Kişisel Verilerin Yurt Dışına Aktarımına İlişkin Güncel Kişisel Verileri Koruma Kurulu Kararı”. *Mondaq.*September 30,2020. https://www.mondaq.com/turkey/data-protection/989552/ki351isel-

verilerin-yurt-di351ina-aktarimina-304li351kin-gncel-ki351isel-verileri-koruma-kurulu-karari. Erişim Tarihi: 15.11.2021.

Kişisel Verileri Koruma Kurulu. "Bağlayıcı Şirket Kuralları Hakkında Duyuru". https://www.kvkk.gov.tr/Icerik/6728/YURT-DISINA-KISISEL-VERI-AKTARIMINDA-BAGLAYICI-SIRKET-KURALLARI-HAKKINDA-DUYURU. Erişim Tarihi: 16.11.2021.

Kişisel Verileri Koruma Kurulu. "Kişisel Verilerin Korunması Kanunu Hakkında Sıkça Sorulan Sorular". https://www.kvkk.gov.tr/Icerik/4196/Kisisel-Verilerin-Korunmasi-Kanunu-Hakkinda-Sikca-Sorulan-Sorular. Erişim Tarihi: 8.10.2021.

Kişisel Verileri Koruma Kurulu. "Yurt Dışına Kişisel Veri Aktarımında Hazırlanacak Taahhütnamelerde Dikkat Edilmesi Gereken Hususlara İlişkin Duyurusu". https://www.kvkk.gov.tr/Icerik/6741/YURT-DISINA-KISISEL-VERI-AKTARIMINDA-HAZIRLANACAK-TAAHHUTNAMELERDE-DIKKAT-EDILMESI-GEREKEN-HUSUSLARA-ILISKIN-DUYURU. Erişim Tarihi: 13.10.2021.

Kişisel Verileri Koruma Kurulu tarafından verilen taahhütname izni için bkz. https://www.kvkk.gov.tr/Search?keyword=taahh%C3%BCtname&langText=tr. Erişim Tarihi: 16.11.2021.

Kuner, Christopher. "The Schrems II judgment of the Court of Justice and The Future of Data Transfer Regulation". *European Law Blog*. July.2020,17. https://europeanlawblog.eu/2020/07/17/the-schrems-ii-judgment-of-the-court-of-justice-and-the-future-of-data-transfer-regulation/. Erişim Tarihi: 25.11.2021.

Kuner. Christopher. “Data Protection, Data Transfers, and International Agreements: The CJEU’s Opinion 1/15”. 26.07.2017. Data Protection, Data Transfers, and International Agreements: the CJEU’s Opinion 1/15 – Verfassungsblog. Erişim Tarihi: 12.10.2021.

Lee, Phillip. “The Updated Standard Contractual Clauses:A New Hope?”. June 7, 2021. https://iapp.org/news/a/the-updated-standard-contractual-clauses-a-new-hope/. Erişim Tarihi: 30.11.2021.

Masoch, Daniela Fábián. “Why Should Companies Invest in Binding Corporate Rules?”. *Data Protection 2019*. 03.07.2019: 12-16. https://www.cuatrecasas.com/resources/publication-5f686d84f0d23.pdf?v1.6.0.202110071014. Erişim Tarihi: 01.01.2022.

Protokole taraf olan ülkelerin güncel listesi için bkz. https://www.coe.int/en/web/conventions/full-list?module=treaty-detail&treatynum=181. Erişim Tarihi: 01.01.2022.

Scott, Mark. “ Facebook’s Clegg: Stopping Data Transfers Would Have Profound Consequences”. *Politico Pro*, 2021.

Skahill, Emily. “Trans-Atlantic data flows: What’s Next After the EU-U.S. Privacy Shield?”. July 29, 2021. https://www.brookings.edu/events/transatlantic-data-flows-whats-next-after-the-eu-u-s-privacy-shield/. Erişim Tarihi: 24.11.2021.

Şimşek, Nilgün Serdar, İpek Okucu Taftalı ve Mert Taşkın. “Kişisel Verilerin Korunması Kanunu Kapsamında Yurt Dışına Veri Aktarımlarında Çözümler”. https://www.gsghukuk.com/tr/bultenler-yayinlar/makale-yazilar/kisisel-verilerin-korunmasi-kanunu-kapsaminda-yurt-disina-veri-aktarimlarinda-cozumler.html. Erişim Tarihi: 01.01.2022.

Tess Blair et al. “Appropriate Safeguards in the GDPR”. *Morgan Lewis*. February 2019,14. https://www.morganlewis.com/pubs/2019/02/appropriate-safeguards-in-the-gdpr. Erişim Tarihi: 11.10.2021.

WP29 tarafından oluşturulan güncel belgeler için bkz. https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/binding-corporate-rules-bcr_en#howistheleadauthoritychosen. Erişim Tarihi: 8.10.2021.

Yeterlilik kararına sahip ülkelerin güncel listesi için bkz. https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en. Erişim Tarihi: 24.08.2021.

Yılmaz, Damla. “Kişisel Verileri Hukuka Uygun Şekilde Yurt Dışına Aktarabilmek Ne Kadar Mümkündür?. https://www.sistemglobal.com.tr/makaleler/kvkk-makaleler/kisisel-verileri-hukuka-uygun-sekilde-yurt-disina-aktarabilmek-ne-kadar-mumkundur/. Erişim Tarihi: 15.11.2021.

https://www.coe.int/en/web/conventions/full-list?module=signatures-by-treaty&treatynum=108. Erişim Tarihi: 01.01.2022.

https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/standard-contractual-clauses-scc_en. Erişim Tarihi: 20.10.2021.

https://edpb.europa.eu/our-work-tools/documents/public-consultations/2018/guidelines-12018-certification-and-identifying_en. Erişim Tarihi: 21.11.2021.

https://edpb.europa.eu/our-work-tools/documents/public-consultations/2020/recommendations-012020-measures-supplement_en. Erişim Tarihi: 21.11.2021.

https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-12019-codes-conduct-and-monitoring-bodies-0_en. Erişim Tarihi: 21.11.2021.

https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-22020-articles-46-2-and-46-3-b-regulation_en. Erişim Tarihi: 10.10.2021.

https://www.cnil.fr/fr/responsables-de-traitement-comment-identifier-et-traiter-des-transferts-de-donnees-hors-ue. Erişim Tarihi: 21.11.2021.

https://www.datatilsynet.no/contentassets/7121f4f2de614186bc535823c9da7102/20_01727-3vedtak-om-overtredelsesgebyr---ferde-as.pdf. Erişim Tarihi: 23.11.2021.

https://www.enforcementtracker.com/. Erişim Tarihi: 12.10.2021.

https://www.legifrance.gouv.fr/cnil/id/CNILTEXT000039419459/. Erişim Tarihi: 23.10.2021.

https://www.liberties.eu/en/stories/european-court-of-justice-to-decide-on-pnr-directive/18148. Erişim Tarihi: 08.01.2022.

https://tietosuoja.fi/en/transfers-of-personal-data-out-of-the-eea, Erişim Tarihi: 12.01.2022.

https://edpb.europa.eu/about-edpb/about-edpb_en, Erişim Tarihi: 17.12.2021.

https://www.kvkk.gov.tr/Icerik/2053/Yurtdisina-Aktarim, Erişim Tarihi: 17.12.2021.

https://www.sistemglobal.com.tr/makaleler/kvkk-makaleler/kisisel-verileri-hukuka-uygun-sekilde-yurt-disina-aktarabilmek-ne-kadar-mumkundur/, Erişim Tarihi: 15.11.2021.

https://ec.europa.eu/commission/presscorner/detail/en/statement_21_6915, Erişim Tarihi: 30.12.2021