**T.C.**

**İSTANBUL KÜLTÜR ÜNİVERSİTESİ**

**LİSANSÜSTÜ EĞİTİM ENSTİTÜSÜ**

# ANONİM ŞİRKETLERDE YURT DIŞINA KİŞİSEL VERİ AKTARIMLARININ HUKUKİ DAYANAĞI OLARAK STANDART SÖZLEŞMELER

**YÜKSEK LİSANS TEZİ**

**Merve Betül GÖKSU**

**2000006470**

**Anabilim Dalı: ÖZEL HUKUK**

**Programı: ÖZEL HUKUK**

**Tez Danışmanı: Dr. Öğr. Üyesi Muharrem TÜTÜNCÜ**

**Haziran 2025**

**T.C.**

**İSTANBUL KÜLTÜR ÜNİVERSİTESİ**

**LİSANSÜSTÜ EĞİTİM ENSTİTÜSÜ**

# ANONİM ŞİRKETLERDE YURT DIŞINA KİŞİSEL VERİ AKTARIMLARININ HUKUKİ DAYANAĞI OLARAK STANDART SÖZLEŞMELER

**YÜKSEK LİSANS TEZİ**

**Merve Betül GÖKSU**

**2000006470**

**Anabilim Dalı: ÖZEL HUKUK**

**Programı: ÖZEL HUKUK**

**Tez Danışmanı : Dr. Öğr. Üyesi Muharrem TÜTÜNCÜ**

**Jüri Üyeleri : Dr. Öğr. Üyesi Elif ALTINOK ÇALIŞKAN**

**Dr. Öğr. Üyesi Serkan SEYHAN**

**Haziran 2025**

# İÇİNDEKİLER

## KISALTMALAR

**AB** **:** Avrupa Birliği

**ABAD** **:** Avrupa Birliği Adalet Divanı

**ABD** **:** Amerika Birleşik Devletleri

**AB Direktifi** **:** "95/46/EC Sayılı Kişisel Verilerin İşlenmesi ve Serbest Dolaşımı Bakımından Bireylerin Korunmasına İlişkin Avrupa Parlamentosu ve Avrupa Konseyi Direktifi" ("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")

**AİHM** **:** Avrupa İnsan Hakları Mahkemesi

**AİHS** **:** Avrupa İnsan Hakları Sözleşmesi

**AK 108 No.lu Sözleşme** **:** Avrupa Komisyonu "Kişisel Verilerin Otomatik İşleme Tabi Tutulması Karşısında Bireylerin Korunması Sözleşmesi" ("Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data")

**Bknz.** : bakınız

**BM** : Birleşmiş Milletler

**BŞK** : Bağlayıcı Şirket Kuralları

**BCR** : Bağlayıcı Şirket Kuralları

**C** : Cilt

**E** **:** Esas Numarası

**E.T.** : Erişim Tarihi

**EDPB** **:** Avrupa Veri Koruma Kurulu (European Data Protection Board)

**GDPR** **:** General Data Protection Regulation

**GVKT** **:** Avrupa Birliği Genel Veri Koruma Tüzüğü (EU General Data Protection Regulation)

**K** : Karar Numarası

**KEP** : Kayıtlı Elektronik Posta

**Kurul** : Kişisel Verileri Koruma Kurulu

**Kurum** : Kişisel Verileri Koruma Kurumu

**KVKK** : 6698 sayılı Kişisel Verilerin Korunması Kanunu

**KVSYAY** : Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi Hakkında Yönetmelik

**KYC** : Know Your Customer/ Müşterini Tanı

**No** **:** Numara

**OECD** **:** Organisation For Economic Cooperation And Development (Ekonomik Kalkınma ve İş birliği Örgütü)

**OECD Rehber İlkeleri** **:** "Özel Yaşamın Korunması ve Kişisel Verilerin Sınır Ötesi Akışına İlişkin Rehber İlkeler" ("Guidelines on the Protection of Privacy and Transborder Flows of Personal Data")

**RG.** **:** Resmî Gazete

**s.** **:** Sayfa

**S.** **:** Sayı

**SCC** : Standart Sözleşme Maddeleri

**Sicil** : Veri Sorumluları Sicili

**T.** **:** Tarih

**TBK** **:** 6098 sayılı Türk Borçlar Kanunu

**TCK** **:** 5237 sayılı Türk Ceza Kanunu

**TMK** **:** 4721 sayılı Türk Medeni Kanunu

**TTK** **:** 6102 sayılı Türk Ticaret Kanunu

**TÜİK** **:** Türkiye İstatistik Kurumu

**VERBİS** **:** Veri Sorumluları Sicil Bilgi Sistemi

**VKED** **:** Veri Koruma Etki Değerlendirmesi

**VKS** **:** Veri kayıt sistemi

**VSBT** **:** Veri Sorumlusuna Başvuru Usul ve Esasları Hakkında Tebliğ

**VSSY** **:** Veri Sorumluları Sicili Hakkında Yönetmelik

**YHGK** **:** Yargıtay Hukuk Genel Kurulu

**Üniversite** : **İstanbul Kültür Üniversitesi**
**Enstitü** : **Lisansüstü Eğitim Enstitüsü**
**Anabilim Dalı** : **Özel Hukuk**
**Programı** : **Özel Hukuk**
**Tez Danışmanı** : **Dr. Öğr. Üyesi Muharrem TÜTÜNCÜ**
**Tezin Türü ve Tarihi** : **Yüksek Lisans Tezi – Haziran 2025**

## ÖZET

## ANONİM ŞİRKETLERDE YURT DIŞINA KİŞİSEL VERİ AKTARIMLARININ HUKUKİ DAYANAĞI OLARAK STANDART SÖZLEŞMELER

**Merve Betül Göksu**

6698 sayılı Kişisel Verilerin Korunması Kanunu'nun 9. maddesinde yapılan değişiklikler, kişisel verilerin yurt dışına aktarımı alanında köklü bir dönüşüm yaratmıştır. Bu dönüşümle birlikte, açık rıza istisnai bir yöntem haline gelmiş, veri aktarımında esas yöntem olarak "standart sözleşmeler" ön plana çıkmıştır. Söz konusu değişiklikler, özellikle büyük veri işleyen kuruluşlardan biri olan anonim şirketleri doğrudan etkilemiş; bu şirketlerin uluslararası veri aktarımı süreçlerindeki hukuki sorumluluklarını yeniden tanımlamıştır. Bu çalışmada, anonim şirketlerin yurt dışına veri aktarımı faaliyetleri çerçevesinde, güncel hukuki düzenlemelere nasıl uyum sağladığı, standart sözleşmelerin içerik ve işlevi ile birlikte detaylı biçimde incelenmiştir.

Tezin ilk bölümünde kişisel verilerin tanımı, hukuki niteliği, işlenme şartları ve temel ilkeler ele alınmış; ikinci bölümde 6698 sayılı Kanun ile Avrupa Birliği Genel Veri Koruma Tüzüğü (GDPR) karşılaştırmalı olarak incelenerek yurt dışına veri aktarımı için öngörülen hukuki mekanizmalar değerlendirilmiştir. Son bölümde ise, standart sözleşmelerin anonim şirketler tarafından nasıl uygulandığı, bu sözleşmelerin sağladığı hukuki güvenceler ve uygulamada karşılaşılan sorunlar analiz edilmiştir.

Araştırma sonucunda, standart sözleşmelerin yalnızca yurt dışı ile uyum sağlamaya değil, aynı zamanda veri sorumlularının yükümlülüklerini belirginleştirerek şeffaflık ve hesap verebilirliği artırmaya hizmet ettiği tespit edilmiştir. Ancak Türkiye'deki standart sözleşmelerin, Avrupa Birliği uygulamalarındaki "Standard Contractual Clauses" (SCC) ile tam uyumlu olmaması,

uygulamada bazı belirsizliklere yol açmaktadır. Bu kapsamda, standart sözleşmelerin sektörel rehberlerle ve denetim standartlarıyla desteklenmesi gerektiği ve veri koruma kültürünün risk temelli bir anlayışla geliştirilmesinin önem taşıdığı sonucuna ulaşılmıştır. Çalışma, anonim şirketlerin veri aktarım süreçlerinde karşılaştıkları hukuki ve pratik zorluklara dair çözüm önerileri sunarak, bu sürecin daha güvenli ve uyumlu biçimde yürütülmesine katkı sağlamayı amaçlamaktadır.

**Anahtar Kelimeler:** Kişisel Verilerin Korunması, Yurt Dışına Veri Aktarımı, Standart Sözleşmeler, Anonim Şirketler, KVKK, GDPR, Veri Güvenliği**.**

**University** : **İstanbul Kültür University**
**Institute** : **Institute of Graduate Studies**
**Department** : **Private Law**
**Programme** : **Private Law**
**Supervisor** : **Dr. Öğr. Üyesi Muharrem TÜTÜNCÜ**
**Degree Awarded and Date** : **Master's Thesis – June 2025**

## ABSTRACT

## STANDARD CONTRACTUAL CLAUSES AS THE LEGAL BASİS FOR CROSS-BORDER TRANSFERS OF PERSONAL DATA BY JOİNT STOCK COMPANİES

**Merve Betül Göksu**

The recent amendments to Article 9 of the Law on the Protection of Personal Data No. 6698 have led to a fundamental transformation in the transfer of personal data abroad. With these changes, explicit consent has been relegated to an exceptional mechanism, and "standard contractual clauses" have emerged as the primary legal basis for cross-border data transfers. These developments have significantly affected joint stock companies, which are among the largest data processors in Turkey, by redefining their legal responsibilities in international data transfers. This study comprehensively examines the updated legal framework, the structure and function of standard contractual clauses, and how these mechanisms are implemented by joint stock companies.

In the first part of the thesis, the concept of personal data, its legal characteristics, the conditions for processing, and fundamental principles are discussed. The second part compares the relevant provisions of the Turkish Data Protection Law and the European Union's General Data Protection Regulation (GDPR), focusing on the legal mechanisms for international data transfers. The final section analyzes how joint stock companies implement standard contractual clauses, the legal safeguards they provide, and the practical challenges encountered in their application.

The research concludes that standard contractual clauses not only facilitate compliance with international standards but also enhance transparency and accountability by clearly defining the obligations of data controllers. However, the lack of full alignment between Turkish standard clauses and the EU's Standard Contractual Clauses (SCC) has created certain legal ambiguities. Therefore, it is recommended that these clauses be supported by sector-specific guidelines and audit frameworks. Additionally, adopting a risk-based data protection approach would help joint stock companies establish more effective management and oversight mechanisms. By identifying the legal and practical challenges in data transfers, this study aims to contribute to the secure and compliant management of such processes by joint stock companies.

Keywords: Personal Data Protection, Cross-Border Data Transfer, Standard Contractual Clauses, Joint Stock Companies, KVKK, GDPR, Data Security.

# GİRİŞ

6698 sayılı Kişisel Verilerin Korunması Kanunu'nun 9. maddesinde yapılan son değişiklikler, kişisel verilerin yurt dışına aktarımını önemli ölçüde yeniden yapılandırmış ve bu süreçte "standart sözleşmeler" mekanizmasını merkezî bir konuma taşımıştır. Bu değişiklikler, özellikle anonim şirketlerin veri aktarım süreçlerini doğrudan etkilemiş ve şirketlerin yurt dışına veri aktarımlarındaki hukuki sorumluluklarını yeniden şekillendirmiştir. Anonim şirketlerin bu yeni düzenlemelere uygun hareket edebilmesi hem veri güvenliği hem de hukuki uyum açısından büyük önem taşımaktadır. Çalışmanın amacı, yurt dışına veri aktarımı konusunda uygulanan yeni hukuki çerçeveyi, standart sözleşmelerin yapısını ve bu sözleşmelerin pratikteki etkilerini ele almaktır.

Özellikle, anonim şirketlerin sunduğu hizmetler, sözleşmelerin imzalanması, yükümlülüklerin yerine getirilmesi ve alacak tahsilatı gibi işlemler, büyük miktarda verinin işlenmesini zorunlu kılmaktadır. 6698 sayılı Kanun'un yürürlüğe girmesiyle, anonim şirketlerde kişisel verilerin işlenmesi, saklanması ve korunması sadece bir yasal zorunluluk değil, aynı zamanda sektörel bir mesele haline gelmiştir. Bu kanun, kişisel verilerin korunması hakkı ile ilgili önemli hukuki ve idari düzenlemelere zemin hazırlamış ve bu bağlamda anonim şirketlerin veri işleme faaliyetlerinin daha şeffaf ve güvenli bir şekilde yürütülmesi gerektiğini ortaya koymuştur. Günümüzde veri işleyen en büyük kuruluşlardan biri olan anonim şirketlerin hukuki açıdan detaylı bir şekilde incelenmesi ve bu şirketlerin sahip olduğu sorumlulukların ayrıntılı olarak ele alınması önem arz etmektedir. Özellikle, anonim şirketlerin yurt dışına veri aktarımındaki hukuki dayanağının belirlenmesi, bu şirketlerin uluslararası veri aktarım süreçlerinde karşılaştıkları sorunlara çözüm üretilmesi açısından kritik bir konu haline gelmiştir.

Bu tez, anonim şirketlerin veri işleme faaliyetleri çerçevesinde, kişisel verilerin hangi koşullar altında işlendiğini, bu verilerin türlerini, verilerin korunmasını sağlamak için alınması gereken önlemleri ve veri aktarımında standart sözleşme imzalama süreçlerini kapsamlı bir şekilde incelemeyi hedeflemektedir. Çalışmamızın ilk bölümünde kişisel veri kavramı ve unsurları, kişisel verilerin işleme süreçlerinde temel ilkeler ve işleme şartları ele alınacak; ikinci bölümde, 6698 sayılı Kişisel Verilerin Korunması Kanunu ve Avrupa Birliği Genel Veri Koruma Tüzüğü (GDPR) uyarınca kişisel verilerin yurt dışına aktarılmasındaki genel koşullar tartışılacak ve yurt dışına veri aktarımı için öngörülen hukuki mekanizmalar incelenecektir. Son bölümde ise, anonim şirketlerin yurt dışına veri aktarım süreçlerinde kullandıkları standart sözleşmelerin

hukuki dayanağı, bu sözleşmelerin gerekliliği ve uygulanması konusundaki pratik sorunlar ele alınacaktır. Bu şekilde, anonim şirketlerin veri aktarım süreçlerinde karşılaştıkları yasal ve pratik zorluklara ışık tutarak, bu süreçlerin güvenli ve yasal bir şekilde nasıl yönetilebileceğine dair bir analiz sunulması amaçlanmaktadır.

# BİRİNCİ BÖLÜM

## KİŞİSEL VERİLERİN KORUNMASI KAVRAMI VE HUKUKİ NİTELİĞİ

Bu bölümde, kişisel verilerin korunmasına ilişkin temel kavramlar ve hukuki nitelikleri ele alınacaktır. İlk olarak, kişisel veri tanımına ve türlerine ilişkin genel bir çerçeve sunulacak, ardından kişisel verilerin korunmasının önemine değinilecektir. Kişisel verilerin korunmasının hukuki temelleri, özellikle 6698 sayılı Kişisel Verilerin Korunması Kanunu çerçevesinde değerlendirilecek ve bu kanunun, verilerin işlenmesi, saklanması ve korunmasına dair getirdiği yükümlülükler incelenecektir. Ayrıca, kişisel verilerin korunmasıyla ilgili uluslararası düzenlemelere ve Avrupa Birliği'nin Genel Veri Koruma Tüzüğü (GDPR) gibi yasal çerçevelerine de yer verilecektir. Bu unsurlar, kişisel verilerin korunmasına dair hukuki bir temel oluşturacak ve sonraki bölümlere geçiş için zemin hazırlayacaktır.

### I. KİŞİSEL VERİ KAVRAMI ve UNSURLARI

#### A. KİŞİSEL VERİNİN ÖZÜ OLARAK BİLGİ KAVRAMI

Kişisel veri kavramı tanım olarak kişiye öz, sadece kişinin kendine has özelliklerini belirten, kişiye atfedebileceğimiz veridir. Kanunda, yönetmeliklerde, uluslararası kaynaklarda ve kişisel verileri ele alan tüm kitaplarda kişisel veri tanımı hemen hemen ortak olmakla birlikte KVKK madde 3 hükmüne göre kişisel veri, "kimliği belli ya da belirlenebilir gerçek kişiye ilişkin her türlü bilgidir[1]."

Avrupa Birliği Genel Veri Koruma Tüzüğü'nün 4. maddesi, kişisel veri tanımını açıklamaktadır. Bu maddeye göre, kişisel veri, belirli veya belirlenebilir bir gerçek kişiye ilişkin

[1] Kişisel Verilerin Korunması Kanunu (2016). R.G. Tarih: 07.04.2016 sayı: 29677.

her türlü bilgiyi ifade eder. Belirli bir kişi, bu bilgiyi direkt veya dolaylı olarak tanımlamak suretiyle bu bilgiyi kişiye atfeden birçok faktörle tanımlanabilir[2].

*"Kişisel veriden bahsedebilmek için; mevcut bir veri bulunmalı, mevcut veri gerçek bir kişiye ait olmalı ve bu gerçek kişinin kimliği belli ya da belirlenebilir olmalıdır. İlk olarak, ortada işlenebilir bir veri olmalıdır. Veri gerçek kişiye ait olmalıdır. Tüzel kişilere ait veriler, kişisel veri olarak kabul edilemez[3]."*

Kişisel Veri Koruma Kanunu'nun gerekçesi çerçevesinde kişisel verinin tanımında üç sac ayağı bulunduğu belirtilmektedir. Bu unsurlar şunlardır:

1. Gerçek kişiye ait olma: Kişisel verilerin yalnızca gerçek bireylere ait olması gerektiğini vurgulamakta olan 6698 sayılı Kişisel Verilerin Korunması Kanunu'nda, gerçek kişi tanımı doğumdan ölüme kadar olan süreçte hukuken bireyi ifade eden bir kavram olarak yer almaktadır. Bu bağlamda, bir kişinin ölümünden sonra kişilik hakları sona erdiği için o kişi, kişisel verilerin korunması kanununda tanımlanan kişisel veri öznesi olma özelliğini yitirir.
2. Kişiyi belirli veya belirlenebilir kılma: Kişisel verilerin, bireylerin kimliğini tanımlama ya da tanımlanabilir hale getirme özelliği taşır.
3. Her türlü bilgiyi içerme: Kişisel veriler, bireylerle ilgili her türlü bilgiyi kapsayabilir. Bu unsurlar, kişisel verilerin korunmasının önemli gerekçelerini oluşturur ve bireylerin mahremiyetinin sağlanmasına yönelik bir çerçeve sunar[4].

Kişisel veri tanımına çeşitli yargı kararlarında da yer verilerek, kişisel verilerin neler olabileceği hakkında çeşitli tasniflere gidilmiştir. Yargıtay Ceza Genel Kurulu'nun bir kararında belirtildiği üzere[5],

*"Kişisel veriler, bilimsel kaynaklar ışığında aşağıdaki şekilde gruplandırılabilir:*

a- Yaşam tarzına ilişkin kişisel veriler: Kişilerin üçüncü kişiler tarafından ayırımcılığa uğramaması ve haysiyetinin korunmasıyla ilişkili olarak, dini inançları, cinsel yönelim, etnik

---

[2] Avrupa Birliği Genel Veri Koruma Tüzüğü (2016) "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)" R.G. Tarih: 23.05.2018 sayı: OJ L 119, 04.05.2016; cor. OJ L 127.

[3] Beşir Orak, *Kişisel Sağlık Verilerin Korunması*, Ankara, Yetkin Yayıncılık, 1. Baskı, 2020. s.24.

[4] Mustafa Baysal, *KVKK Kişisel Verilerin Korunması Kanunu El Kitabı*, Ankara, Seçkin Yayıcılık, 7. Baskı, 2024, s.30.

[5] Yargıtay Ceza Genel Kurulu, E: 2012/12-1510, K: 2014/331, T.17.06.2014 https://www.lexpera.com.tr/ictihat/yargitay/ceza-genel-kurulu-e-2012-1510-k-2014-331-t-17-6-2014, (Erişim Tarihi: 18/04/2025).

kökeni, suç geçmişi, politik eğilimleri ve kişisel özel aktivitelere ilişkin bilgiler bu bağlamda sayılabilecektir.

b- Ekonomik ve finansal durumuna ilişkin kişisel veriler: Kişinin mali durumu, borçları, hesap bilgileri, alışveriş geçmişi gibi veriler suistimale açık olması nedeniyle önemlidir. Bu veriler dolaylı olarak kişinin konumu, ilişkileri ve sağlık durumu hakkında da bilgi verebilir.

c- Bilişim alanına ilişkin kişisel veriler: E-posta adresleri, şifreler ve internet üzerindeki faaliyetler mahrem kabul edilir. İnternetteki gezintiler sırasında toplanan kişisel bilgiler, hizmet sağlayıcılar ve sunucular tarafından kaydedilebildiği için bu verilerin gizliliği önemlidir.

d- Sağlıkla ilgili kişisel veriler: Kişinin iş güvencesi, toplumdaki konumu ve sigorta durumu üzerinde etkili olan bu bilgiler, aynı zamanda bireyin sosyal hayatı ve psikolojik durumu hakkında da ipuçları verir. Biyometrik veriler de bu kapsamdadır.

e- Siyasi tercihlerine yönelik veriler: Kişilerin siyasi tercihleri toplumda ayrımcılığa neden olabileceği için kişisel veri olarak kabul edilir."

Kişisel verilerin tanımı, uluslararası belgelerde benzer bir çerçevede ele alınmaktadır. OECD'nin 1980 yılında yayımlayıp 2013'te revize ettiği rehber ilkeleri ile Avrupa Birliği Genel Veri Koruma Tüzüğü, kişisel verileri bir gerçek kişi ile doğrudan veya dolaylı olarak ilişkilendirilip tanınmasına olanak sağlayan tüm bilgi türleri olarak tanımlamaktadır. Bu tanım, veri koruma standartlarının geliştirilmesi ve bireylerin gizliliğinin sağlanması açısından büyük önem taşımaktadır[6].

Kişisel verilerin işlenmesi, saklanması ve korunması süreçlerinde bu tanım, yasaların oluşturulması ve uygulanmasında kritik bir temel sunar. Örneğin, yalnızca açıkça tanımlanabilir bilgiler (isim, adres gibi) değil, aynı zamanda IP adresleri, çerez verileri (cookies) ve diğer dolaylı tanımlayıcı bilgiler de kişisel veri olarak kabul edilir[7]. Bu tür verilerin korunmasıyla ilgili düzenlemeler, bireylerin haklarının güvence altına alınmasına ve kuruluşların yasal yükümlülüklerinin belirlenmesine yardımcı olmaktadır. Bu çerçevede, kişisel verilerin ve bireylerin mahremiyetinin korunması, günümüzde veri güvenliği konusundaki en önemli önceliklerden biri haline gelmiştir.

[6] Bahri Öztürk, Elif Altınok Çalışkan, Serkan Seyhan, *Kişisel Verilerin Korunması Hukuku Teorik ve Pratik Çalışma Kitabı*, Ankara, Seçkin Hukuk, 3. Baskı, 2024, s. 17.

[7] Kişisel Verileri Koruma Kurumu, *Kişisel Verilerin Korunması Kanunu Hakkında Bilgi Notu*, https://www.kvkk.gov.tr/Icerik/6649/Kisisel-Veri-Nedir, (Erişim Tarihi: 24.10.2024).

## B. KİŞİSEL VERİ KAVRAMININ UNSURLARI

### 1.Kişi

6698 sayılı Kişisel Verilerin Korunması Kanunu, kişisel verilerin yalnızca gerçek bireylere ait olması gerektiği ilkesini benimsemektedir. Bu nedenle, Kanunda veri sahibi olan kişiyi tanımlamak için "ilgili kişi" terimi kullanılır ve bu kişi yalnızca gerçek kişiler olabilir (m.3/ç). Tüzel kişilere ait veriler ise doğrudan bu kapsamda değerlendirilmez. Ancak, bir tüzel kişiye ait veri, bir gerçek kişinin kimliğini ortaya koyuyor ya da ortaya koyabilir nitelikteyse, bu veri Kanun kapsamında korunur. Bu durumda da koruma altına alınan çıkar, tüzel kişiye değil, veriyle ilişkilendirilebilen gerçek kişiye aittir. Kanun, tüzel kişilere ait verilerin korunmasına yönelik bir düzenleme getirmemektedir. "*Kanunda yer alan kişisel verinin tanımı gereği, tüzel kişiye ait bir verinin herhangi bir gerçek kişiyi belirlemesi ya da belirlenebilir kılması halinde, bu veriler de Kanun kapsamında koruma altındadır. Ancak burada korunan menfaat tüzel kişiye değil, düzenlemenin temellendirdiği öncelik gereği belirlenen ya da belirlenebilecek gerçek kişiye ait olacaktır. Çünkü Kanun, tüzel kişilere ait verilerin korunmasını hiçbir şekilde düzenlememektedir*[8]*."*

Kişisel Verilerin Korunması Kanunu'nda "gerçek kişi" tanımı, bireyin doğumuyla başlayıp ölümüne kadar süren hayat döngüsünü kapsamaktadır. Bu bağlamda, kişi yaşamı boyunca kişisel verileriyle bağlantılı haklara sahiptir (KVKK m. 1 ve m. 2)[9]. Ölüm durumu, kişilik haklarının sona ermesiyle sonuçlanır. Bir kişinin vefatıyla birlikte, o kişinin hukuki olarak varlığı sona erer (TMK m.28) ve kişisel verileri, kanun kapsamındaki kişisel veri öznesi olma niteliğini kaybeder. Bu nedenle, öldükten sonra bireylerin kişisel verileri, veri koruma hukukunun dikkate aldığı bir konu olmaktan çıkar. Bu durum, kişisel verilerin korunması ilkesinin özel bir önemi olduğunu ve bireylerin yaşamları boyunca sahip oldukları hakların, ölümlerinden sonra geçerliliğini yitirdiğini göstermektedir. Böylece, Kişisel Verilerin Korunması Kanunu yalnızca yaşayan bireylerin mahremiyetini ve verilerini korumaya yönelik bir düzenleme olarak anlam kazanmakta ve bu kapsamda, gerçek kişilere ait verilerin korunmasına yönelik gerekli önlemlerin alınmasını teşvik etmektedir[10].

---

[8] Kişisel Verileri Koruma Kurumu, *https://www.kvkk.gov.tr/Icerik/2034/Ilgili-Kisi-Kimdir*, (Erişim Tarihi: 24/10/2024).

[9] Ayrıca bknz. Kişisel Verileri Koruma Kurumu, *6698 Sayılı Kanun'da Yer Alan Temel Kavramlar, https://www.kvkk.gov.tr/Icerik/4187/6698-Sayili-Kanun-da-Yer-Alan-Temel-Kavramlar (E.T.* 24/10/2024*)*.

[10] Baysal, *KVKK Kişisel Verilerin Korunması Kanunu El Kitabı*, s.31.

İlgili kişinin ölümü halinde ise, kişisel verilerin niteliği, sözleşmenin konusu ve veri işleme faaliyetinin amacı dikkate alınarak değerlendirme yapılmalıdır. 6698 sayılı Kişisel Verilerin Korunması Kanunu kapsamında yalnızca yaşayan gerçek kişilere ait veriler korunmakta ise de doktrinde, ölen kişilerin dijital verilerinin –örneğin sosyal medya hesapları veya dijital varlıkları– korunup korunmaması gerektiğine ilişkin görüş ayrılıkları bulunmaktadır[11]. Bu tartışmalar ağırlıklı olarak genel nitelikli veriler bağlamında yürütülmektedir.

Bu durum, anonim şirketlerin veri sorumlusu sıfatıyla yürüttüğü kişisel veri işleme faaliyetleri bakımından da geçerlidir. Şirket ile ilgili kişi arasında kurulmuş olan sözleşmeye veya hukuki ilişkiye dayanarak işlenen veriler, ilgili kişinin vefatıyla birlikte artık kişisel veri rejimi kapsamında korunmaz[12]. Ölüm, ilgili kişinin açık rıza verebilme ehliyetini sona erdirdiğinden, kişisel veri işleme faaliyeti açısından aranan rıza şartı da hukuken anlamını yitirir[13]. Bununla birlikte, verinin artık kişisel veri niteliği taşımaması, anonim şirketin elinde bulunan bu tür verileri herhangi bir yükümlülük olmaksızın serbestçe işleyebileceği anlamına gelmemektedir. Bu veriler, özellikle özel hayatın gizliliği, ticari sırlar ya da sektörel düzenlemeler kapsamında farklı hukuki rejimlerin konusu olabilir. Ayrıca, kamu güvenliği, kamu sağlığı veya adli süreçler gibi sebeplerle saklanması gereken veriler, ilgili mevzuat hükümlerine göre belirli sürelerle muhafaza edilmelidir.

Sağlık verileri bakımından ise, Kişisel Sağlık Verileri Hakkında Yönetmelik'in 11. maddesinde "Ölünün Sağlık Verilerine Erişim" başlığı altında, "ölmüş bir kimsenin sağlık verilerini almaya, veraset ilamını ibraz etmek suretiyle murisin yasal mirasçıları münferit olarak yetkilidir. Ölmüş bir kimsenin sağlık verileri, en az 20 yıl süre ile saklanır." hükmü yer almaktadır. Buna göre, ilgili kişi vefat etmiş olsa dahi, sağlık verileri anonim şirket veri sorumluları tarafından da en az 20 yıl süreyle muhafaza edilmelidir[14]. Bu bağlamda anonim şirketler ölüm sonrası veri muhafazası konusunda veri türü, işleme amacı ve sektörel düzenlemeler çerçevesinde ayrıca değerlendirme yapmakla yükümlüdür.

---

[11]Süleyman Yılmaz, Vehbi Umut Erkan; "Sosyal Medya Hesaplarının Miras Yoluyla İntikal Edip Edemeyeceği Sorusunun Kişisel Verileri Koruma Hukuku Kapsamında İncelenmesi", *İnönü Üniversitesi Hukuk Fakültesi Dergisi*, C. 11, S. 2, s. 574; Yasemin, Maraşlı Dinç, "Ölümden Sonra Sosyal Medya Hesaplarının Hukuki Akıbeti: Dijital Miras", *TBBD*, S. 142, 2019, s. 283. (Aktaran: Miray Özer Deniz, *Özel Nitelikli Kişisel Verilerin İşlenmesi ve Bundan Doğan Sorumluluk*, İstanbul, Oniki Levha Yayıncılık, 1. Baskı 2022, s.255. )

[12] GDPR 4/1, GDPR Gerekçesi (Recital 27: Not Applicable to Deceased Persons. Bu yönetmelik ölen kişilerin kişisel verilerine uygulanmaz. Üye Devletler, ölen kişilerin kişisel verilerinin işlenmesine ilişkin kurallar koyabilir.)

[13] Elif Beyza Akkanat Öztürk, *Karşı Edim Olarak Kişisel Veriler,* İstanbul, Oniki Levha Yayıncılık, 1. Baskı 2022, s.370.

[14] Miray Özer Deniz, *Özel Nitelikli Kişisel Verilerin İşlenmesi ve Bundan Doğan Sorumluluk*, İstanbul, On İki Levha Yayıncılık, 1. Baskı 2022, s.255.

Farklı hukuk sistemlerinde, ölen kişilere ait verilerin kişisel veri olarak kabul edilip edilmediği hususunda yeknesak bir yaklaşım bulunmamaktadır. Avrupa Birliği Genel Veri Koruma Tüzüğü, kapsamını yalnızca yaşayan gerçek kişilerle sınırlamakta[15] ve ölen kişilere ait verileri kişisel veri kapsamında değerlendirmediğinden bahsetmiştik. Ancak bazı üye devletler, ölüm sonrası veri işleme hususunu ulusal mevzuatlarında özel olarak düzenlemişlerdir. Bu bağlamda Fransa, Loi Informatique et Libertés adlı veri koruma yasasında bireylerin hayattayken ölüm sonrasına ilişkin verilerinin işlenmesine dair talimat verebilmesini öngörerek bu alanda özel bir hüküm getirmiştir[16]. Almanya ve İsviçre gibi ülkelerde ise ölen kişilere ait veriler doğrudan kişisel veri olarak değerlendirilmemekle birlikte, bu verilerin yaşayan üçüncü kişiler üzerindeki etkisi dolayısıyla dolaylı koruma sağlanabilmektedir[17]. Avrupa dışı hukuk sistemlerinde de benzer şekilde ölüm sonrası veri koruması gündeme gelmektedir. Örneğin Kanada'nın Québec eyaletinde kabul edilen Bill 64 ile bireylerin hayattayken ölüm sonrasına ilişkin veri tasarrufu konusunda talimat verebilmesi mümkün kılınmıştır[18]. Japonya'da ise kişisel verilerin korunması yalnızca yaşayan bireyleri kapsamakla birlikte, aile verileri, vasiyet işlemleri ve cenaze hizmetleri gibi özel durumlar kapsamında ölen kişilere ait verilerin işlenmesi belirli ilkelere tabi tutulmaktadır[19]. Bu durum, kişisel verilerin ölüm sonrası statüsüne ilişkin uluslararası düzeyde açık bir normatif bütünlük olmadığını, ancak bazı sistemlerin veri öznesinin ölümünü takiben de sınırlı koruma öngördüğünü göstermektedir.

### 2. Kişinin Belirli veya Belirlenebilir Olması

Kişisel veri, bir birey hakkında doğrudan veya dolaylı olarak bilgi veren her türlü veridir (m.3/d). Bireyi tanımlama ya da tanınabilir hale getirme özeliğine sahip olan bu tür veriler, isim, telefon numarası, adres gibi açık verilerle birlikte, IP adresleri, çerezler ve diğer dolaylı tanımlayıcı bilgilerdir[20]. Bu kapsamda, anonim şirketlerin faaliyetleri sırasında işledikleri verilerin önemli bir kısmı, kişiyi doğrudan ya da dolaylı olarak tanımlamaya elverişli nitelikte olabilir. Bir anonim şirket, faaliyetleri gereği birçok kişinin kişisel verisini işler. Bu veriler,

---

[15] Avrupa Parlamentosu ve Konseyi, Genel Veri Koruma Tüzüğü (GDPR) 2016/679, OJ L 119, 04.05.2016, m.1(1) ve m.4(1).

[16] Fransa, Loi Informatique et Libertés, Yasa No. 78-17, 06.01.1978, m.85, https://www.legifrance.gouv.fr/, (E.T. 28.06.2025).

[17] Murat Uçak, "Kişisel Verilerin Ölümden Sonra Korunması", *İMHFD*, C. VI, S. 10, 2021, s. 97-123; Almanya, Bundesdatenschutzgesetz (BDSG), 30.06.2017, yürürlük: 25.05.2018, §1(1); İsviçre, Datenschutzgesetz (DSG), 25.09.2020, Art. 2(1), https://www.fedlex.admin.ch/eli/cc/2022/491/fr, (E.T. 28.06.2025).

[18] Québec, Act to Modernize Legislative Provisions Respecting the Protection of Personal Information (Bill 64), 2021, https://www.cai.gouv.qc.ca/loi-modernisee/, (E.T. 28.06.2025).

[19] Japan, Act on the Protection of Personal Information (APPI), rev. 2020, https://www.ppc.go.jp/en/, (E.T. 28.06.2025).

[20] Kişisel Verileri Koruma Kurumu, *Kişisel Verilerin Korunması Kanunu Hakkında Bilgi Notu*, https://www.kvkk.gov.tr/Icerik/6649/Kisisel-Veri-Nedir, (Erişim Tarihi: 24.10.2024).

müşteriler, çalışanlar, tedarikçiler ve diğer paydaşlar hakkında olabilir. Örneğin, bir anonim şirketin web sitesinde ticaret unvanının, adresinin, iletişim bilgilerinin yer alması kişisel verileri belli ve belirlenebilir kılar. Bu sayede o veri, bir kişinin kimliğini doğrudan veya dolaylı yoldan tespit edebilecektir. Bu veriler arasında, bireyin kimliğini doğrudan ortaya koyan ve onu diğer kişilerden açıkça ayırt etmeye yarayan bilgiler ise, 'belli kılma' özelliği taşır. Verinin bir kişiyi "belli" kılması, bireyin kimliğinin doğrudan tanımlanması anlamına gelmekte ve bu veri bireyi açıkça tanımlamakta ve başka bireylerden ayırt etmektedir. Örneğin, bir kişinin adı, soyadı, kimlik numarası, doğum tarihi, e posta adresi, telefon numarası gibi bilgiler, o bireyi kesinlikle belirleyebildiği için "belli kılma" özelliğine haizdir[21]. GDPR'in gerekçesinin 26. Maddesi belirlenebilir kılma noktasında ölçütü "*İlgili kişinin eldeki mevcut verilerle ya da başka yerde bulunan verilerle birleştirilerek belirlenmesi makul biçimde olası ise kişinin belirlenebilir olduğu"* yönündedir[22].

Bir kişinin kimliğinin dolaylı yoldan tespit edilmesini ifade eden "belirlenebilir kılma" ise daha kapsamlı bir çerçeve sunar. Kişiye ait olan dolaylı tanımlayıcı veriler, belirli bir gruptan ya da çevreden gelen bilgilerle birlikte değerlendirildiği zaman o kişiyi tanımlamada etkili olabilir. Örneğin, yaş, cinsiyet, eğitim durumu gibi veriler, bir bireyi belirgin kılma amacıyla kullanılabilir. Belirli bir verinin hangi kişiye ait olduğunun ilk bakışta doğrudan anlaşılmadığı durumlar söz konusu iken başka verilerle ve bilgilerle birleştirildiğinde, kişinin kimliği net bir şekilde tespit edilebildiği durumlarda, bireyin verisinin dolaylı olarak belirlenmiş ya da belirlenebilir olduğu ifade edilebilir[23]. Örneğin, bir anonim şirketin yalnızca adresinin bir kısmını içeren bir veri parçası, kendi başına yeterli bilgi sağlamasa da belirli bir bağlamda veya ticaret unvanı gibi başka verilerle bir araya geldiğinde, o şirketin net kimliğine ulaşmayı mümkün kılabilir[24]. Bu tür verilerin bir araya getirilmesiyle, kişisel verilerin korunması açısından, dolaylı tanımlayıcıların da dikkate alınması büyük önem taşır. IP adresi, çerez bilgileri, cihaz kimliği, sosyal medya platformlarındaki profil bilgileri gibi bilgiler kişinin başka verileri ile birleştiğinde o bireyi belirleyebildiği için "belirlenebilir kılma" özelliğine haizdir[25].

---

[21] Murat Volkan Dülger, *Kişisel Verilerin Korunması Hukuku,* İstanbul, Hukuk Akademisi, 3. Baskı, 2020, s 163.
[22] Avrupa Parlamentosu ve Konseyi, *Genel Veri Koruma Tüzüğü (EU) 2016/679*, 27 Nisan 2016, Gerekçe m. 26. https://www.privacy-regulation.eu/en/recital-26-GDPR.htm, (Erişim Tarihi: 25.10.2024).
[23] Canan İmançlı, Kişisel Sağlık Verilerinin Korunamamasından Doğan Özel Hukuk Sorumluluğu, Sosyal Bilimler Enstitüsü, Özel Hukuk Anabilim Dalı, Yayınlanmamış Yüksek Lisans Tezi, İstanbul 2019, s. 40, (E.T.: 03.11.2024).
[24] Dülger, *Kişisel Verilerin Korunması Hukuku,* s 159.
[25] Avrupa Parlamentosu ve Konsey, *Genel Veri Koruma Tüzüğü (EU) 2016/679*, 27 Nisan 2016, Gerekçe 26: *"...doğrudan kimliği belirlemeyen verilerin, başka verilerle birleştirilerek bir gerçek kişiyi tanımlamaya elverişli hale gelmesi durumunda, bu veriler de kişisel veri olarak kabul edilmelidir."*

Verinin kullanıldığı bağlam da belirlenebilirlik ilkesi açısından kritik bir öneme sahiptir. Örneğin, belirli bir coğrafi konumda ve zamanda bir anonim şirkete ait veriler, bu şirkete ait bilgilerin tespit edilmesine olanak tanıyabilir. Bu noktada veri analizi ve büyük veri teknolojileri de bireylerin belirlenebilirliğini artırmakta ve bu durum hem bireylerin verilerine ait mahremiyetini korumak hem de yasal düzenlemelere uyum sağlamak açısından büyük önem taşır. Veri işleyicilerinin, kişisel bilgileri toplarken bunları göz önünde bulundurması gerekir. Özellikle çalışanların iş yerindeki faaliyetlerine ilişkin olarak işlenen biyometrik veriler ve çevrim içi izleme yoluyla elde edilen veriler, ilgili kişinin kimliğinin belirlenmesine olanak tanıyabildiğinden kişisel veri olarak değerlendirilmelidir[26].

Anonim şirketlerde sıklıkla kullanılan personel devam kontrol sistemleri kapsamında çalışanlardan parmak izi alınması uygulaması, kişinin biyometrik özelliklerine dayanarak tanınmasını sağlamaktadır. Parmak izi her bireye özgü biyometrik bir veri olması nedeniyle, kişinin doğrudan kimliğini ortaya koyan niteliktedir. Bu tür uygulamalarda çalışanın sisteme parmak izi ile giriş yapması, ilgili kişinin tanımlanabilirliğini doğrudan sağlar. Nitekim Kişisel Verileri Koruma Kurulu, 27.02.2020 tarihli ve 2020/167 sayılı kararında, spor salonu üyelerinin parmak iziyle giriş sistemini "kişiyi belirlenebilir kıldığı" için özel nitelikli veri görüp, ölçülülük ilkesine aykırı bulmuş ve ilgili veri işlemenin sonlandırılmasına karar vermiştir[27]. Şirket binalarına girişte yüz tanıma sistemlerinin kullanılması da kişinin belirlenebilirliğini temin eden bir diğer biyometrik veri işleme faaliyetidir. Bu sistemlerde kişinin yüz hatları belirli bir algoritma ile dijitalleştirilerek, sistemde kayıtlı biyometrik veri ile eşleştirilmek suretiyle kimlik doğrulama gerçekleştirilir. 04.08.2022 tarihli ve 2022/797 sayılı Kurul Kararı'nda yüz tanıma sistemlerinin, özel nitelikli kişisel veri olan biyometrik veriler kapsamında değerlendirilmesi gerektiği ve açık rıza olmaksızın işlenemeyeceği belirtilmiştir. Ayrıca, bu tür sistemlerin kullanılmasında alternatif, daha az müdahaleci çözümler mevcutsa, tercih edilmesi gerektiği vurgulanmaktadır[28].

İşyeri içerisindeki ortak alanlarda güvenlik amacıyla yerleştirilen kamera sistemleri aracılığıyla çalışanların görüntülerinin kaydedilmesi de ilgili kişilerin belirlenebilirliğini sağlayan veri işleme faaliyetlerinden biridir. Her ne kadar görüntü kaydında isim gibi tanımlayıcı bir bilgi bulunmasa da söz konusu görüntülerin işyeri kayıtları, vardiya çizelgeleri veya başka verilerle

[26] Dülger, *op. cit.,* s.161.
[27] KVKK, 27/02/2020 Tarihli ve 2020/167 Sayılı Kararı, https://www.kvkk.gov.tr/Icerik/6738/2020-167, (E.T.: 30/05/2025).
[28]KVKK, 04.08.2022 Tarihli ve 2020/797 Sayılı Kararı, https://www.kvkk.gov.tr/Icerik/7434/2022-797, (E.T.: 30/05/2025).

eşleştirilmesi halinde kişinin kimliğinin belirlenmesi mümkündür. Bu doğrultuda kamera kayıtları da kişisel veri olarak kabul edilmektedir. 24.11.2022 tarihli ve 2022/1249 sayılı Kurul Kararı'nda, kamera izleme uygulamasının, işyeri güvenliğinin sağlanması amacıyla sınırlı ve ölçülü şekilde yapılması, çalışanların önceden aydınlatılması koşuluyla hukuka uygun olabileceği belirtilmiştir[29].

Bir e-ticaret sitesinde kullanıcı adı girilmemiş olsa da IP adresi, tarayıcı çerezi (cookie), cihaz ID'si gibi verilerle kullanıcının kimliği belirlenebiliyorsa bu kullanıcı belirlenebilir kişi sayılır. Örneğin bir kullanıcının cihazına yerleştirilen benzersiz bir tanımlayıcı (örneğin user_id=4538721) sayesinde, o kullanıcının farklı zamanlarda ve platformlarda yaptığı işlemler takip edilebilir. Kullanıcı adı veya e-posta adresi olmaksızın, sadece bu tanımlayıcı ile kullanıcı profili çıkarılabilir. Bu profil, veri sorumlusu tarafından başka bilgilerle ilişkilendirilerek doğrudan kimliğe ulaşılabilir. Kişisel Verileri Koruma Kurulu, 10.03.2022 tarihli ve 2022/229 sayılı kararında, özellikle pazarlama ve hedefleme amaçlı kullanılan çerezlerin bireyin izlenmesine imkân tanıdığını ve bu bağlamda ilgili kişinin belirlenebilir kılındığını açıkça belirtmiştir. Kararda, şu tespitte bulunulmuştur: "Kullanıcıların açık rızası olmaksızın, analitik ve reklam çerezleri ile kullanıcı davranışlarının takibi yoluyla kişisel veri işlendiği ve bu veriler üzerinden kişi profili oluşturulabildiği görülmüştür."[30] Benzer şekilde 2022/1358 sayılı kararda da, kullanıcı rızası alınmaksızın çalışan izleme çerezlerinin devreye alınması, kişisel veri işleme faaliyeti olarak değerlendirilmiş ve kişisel profil çıkarmaya elverişli veri setleri üzerinden kişinin belirlenebilir hâle geldiği ifade edilmiştir[31].

Avrupa Birliği Genel Veri Koruma Tüzüğü uyarınca da çerezler, kullanıcının açık rızası olmaksızın yalnızca "kesinlikle gerekli" fonksiyonlar için kullanılabilir. Özellikle üçüncü taraf çerezleri (third-party cookies) ile farklı platformlarda kullanıcı hareketlerinin izlenmesi ve tekil kullanıcı profili oluşturulması, kişinin dolaylı şekilde tanımlanabilirliğini sağladığından kişisel veri işleme kapsamında değerlendirilir (GDPR Recital 30).

### 3. Bilginin Kişiye İlişkin Olması

Bir bilginin kişisel veri olarak değerlendirilmesi için o bilginin bireyle doğrudan bağlantılı olması gerekir. Bu durum, bireyin kimliği ve özellikleri hakkında bilgi sağlayan verilerin,

[29] KVKK, 24.11.2022 Tarihli ve 2022/1249 Sayılı Kararı, https://www.kvkk.gov.tr/Icerik/7586/2022-1249, (E.T.: 30/05/2025).
[30] KVKK, 10.03.2022 Tarihli ve 2022/229 sayılı Kararı, https://www.kvkk.gov.tr/Icerik/7275/2022-229, (E.T.: 30/05/2025).
[31] KVKK, 23.12.2022 Tarihli ve 2022/1358 sayılı Kararı, https://www.kvkk.gov.tr/Icerik/7595/2022-1358, (E.T.: 30/05/2025).

kişisel veri olarak kabul edilmesine olanak tanır. Yani, bu bilgi, hem ilgili kişi hakkında bilgi verip hem de o kişiyle de ilişkilendirilmelidir. Ancak bazı durumlarda, bir bilginin nesnelere, süreçlere ve olaylara dair olması da kişisel veri sınıfına girmesini sağlar.[32] Dolayısıyla, kişisel verilerin kapsamı yalnızca bireylerle ilgili doğrudan bilgilerle sınırlı değildir; dolaylı olarak bir kişiyi etkileyen veya onunla bağlantılı olan veriler de bu tanımın içine girebilmektedir.

Doğrudan Belirleyen öğeler[33];

- *Adı, soyadı, T.C. kimlik numarası gibi doğrudan kişinin kimliğini belirten bilgiler,*
- *Doğum tarihi, doğum yeri gibi bilgiler,*
- *Biyometrik veriler (parmak izi, yüz tanıma verileri gibi),*
- *İletişim bilgileri (telefon numarası, e-posta adresi),*
- *Adres bilgileri,*
- *Sağlık bilgileri,*
- *Finansal bilgiler (banka hesap numarası, kredi kartı bilgileri vb.).*

Dolaylı şekilde belirleyen öğeler[34];

- *Bir web sitesini ziyaret etme sırasında bırakılan IP adresi ve çerez bilgileri,*
- *Sosyal medya hesaplarında paylaşılan bilgiler (fotoğraflar, konum bilgileri),*
- *Bir ürün veya hizmet satın alırken verilen kişisel bilgiler,*
- *Bir ankete verilen cevaplar gibi.*

Örneğin, Bir şirketin web sitesini ziyaret eden kişilerin IP adresleri, tarayıcı bilgileri gibi verileri otomatik olarak toplanır veya bir alışveriş sitesindeki üyeliğe ait kullanıcı adı ve sipariş geçmişi, başka bir platformdan elde edilen veya bir anket sonucu elde edilen bilgilerle birleştirildiğinde kişinin kimliğini belirleyebilir.

Anonim şirketler için kişisel veri bilgilerinin bireye ilişkin olması, iş süreçlerinin yürütülmesi, müşteri ilişkilerinin yönetilmesi ve yasal yükümlülüklerin yerine getirilmesi açısından oldukça önem taşımaktadır.

---

[32] Nur Buğçe Bakırel, *Veri Sorumlusu ve Veri İşleyen Arasındaki Sorumluluk Paylaşımı Avrupa Birliği Genel Veri Koruma Tüzüğü ve Kişisel Verilerin Korunması Kanunu Çerçevesinde Değerlendirilmesi,* Ankara, Seçkin Hukuk, 1. Baskı, 2021, s 19.

[33] Kişisel Verileri Koruma Kurumu, *Kişisel Verilerin Korunması Kanunu Hakkında Bilgi Notu*, https://www.kvkk.gov.tr/Icerik/4186/6698-Sayili-Kanunda-Yer-Alan-Terimler, (Erişim Tarihi: 24.11.2024).

[34] *Ibid.*

## C. ÖZEL NİTELİKLİ KİŞİSEL VERİLER

Özel nitelikli veriler, kişiye sıkı sıkıya bağlı, kişi nezdinde hassas unsurları barındıran, kişiye özgü, karşı taraflarca öğrenilmesi halinde kişinin mağduriyetine sebep olabilecek verilerdir. Bu nedenle kanunda ve uluslararası düzenlemelerde bu veriler özel olarak korunmuştur. KVKK madde 6'da özel nitelikli veriler numerus clausus yoluyla sayılmıştır. Buna göre,

*"Kişilerin ırkı, etnik kökeni, siyasi düşüncesi, felsefi inancı, dini, mezhebi veya diğer inançları, kılık ve kıyafeti, dernek, vakıf ya da sendika üyeliği, sağlığı, cinsel hayatı, ceza mahkûmiyeti ve güvenlik tedbirleriyle ilgili verileri ile biyometrik ve genetik verileri özel nitelikli kişisel veridir[35]."*

Yasa koyucu kanun değişikliği öncesinde açık rıza olmaksızın verilerin işlenebileceği haller bakımından farklı düzenlemeler, belirli ayrımlar yapmıştı. Sağlık ve cinsel hayata ilişkin kişisel verilerin işlenmesi ile diğer özel nitelikli kişisel verilerin işlenebileceği halleri farklı düzenlemelere tabi tutmuştu. Değişiklik öncesindeki düzenlemeye göre özel nitelikli kişisel verilerin işlenmesi, ilgili kişinin açık rızası dışında aşağıdaki hallerde mümkündü: "*Sağlık ve cinsel hayat dışındaki özel nitelikli kişisel veriler, ancak kanunlarda öngörülen hallerde, sağlık ve cinsel hayata ilişkin kişisel veriler, 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 işlenebilir.*" ifadesi yer almaktaydı (KVKK m.6/3).

12.02.2024 tarihinde 32487 sayılı Resmi Gazetede yayımlanan 7499 s. Kanunun 33. Maddesi baştan düzenlenerek 6698 sayılı KVKK'nın GDPR'a uyumlu hale getirilmesi amaçlanmıştır. Yapılan değişiklik ile birlikte, kanunun 6. Maddesinin 3. Fıkrasında düzenlenen "Özel Nitelikli Kişisel Verilerin İşlenmesi" yasağı temel düstur olarak benimsenmiş ve bu yasağa ilişkin istisnai durumlar şu şekilde belirlenmiştir[36]:

*"(3) Özel nitelikli kişisel verilerin işlenmesi yasaktır. Ancak bu verilerin işlenmesi;*

*a) İlgili kişinin açık rızasının olması,*

*b) Kanunlarda açıkça öngörülmesi,*

*c) 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,*

*ç) İlgili kişinin alenileştirdiği kişisel verilere ilişkin ve alenileştirme iradesine uygun olması,*

---

[35] Kişisel Verilerin Korunması Kanunu (2016). R.G. Tarih: 07.04.2016 sayı: 29677.

[36] Öztürk, Bahri, Elif Altınok Çalışkan, Serkan Seyhan, *Kişisel Verilerin Korunması Hukuku Teorik ve Pratik Çalışma Kitabı*, Ankara, Seçkin Hukuk, 3. Baskı, 2024, s. 101-102.

*d) Bir hakkın tesisi, kullanılması veya korunması için zorunlu olması,*

*e) Sır saklama yükümlülüğü altında bulunan kişiler veya yetkili kurum ve kuruluşlarca, kamu sağlığının korunması, koruyucu hekimlik, tıbbi teşhis, tedavi ve bakım hizmetlerinin yürütülmesi ile sağlık hizmetlerinin planlanması, yönetimi ve finansmanı amacıyla gerekli olması,*

*f) İstihdam, iş sağlığı ve güvenliği, sosyal güvenlik, sosyal hizmetler ve sosyal yardım alanlarındaki hukuki yükümlülüklerin yerine getirilmesi için zorunlu olması,*

*g) Siyasi, felsefi, dini veya sendikal amaçlarla kurulan vakıf, dernek ve diğer kâr amacı gütmeyen kuruluş ya da oluşumların, tâbi oldukları mevzuata ve amaçlarına uygun olmak, faaliyet alanlarıyla sınırlı olmak ve üçüncü kişilere açıklanmamak kaydıyla; mevcut veya eski üyelerine ve mensuplarına veyahut bu kuruluş ve oluşumlarla düzenli olarak temasta olan kişilere yönelik olması, halinde mümkündür.*

*(4) Özel nitelikli kişisel verilerin işlenmesinde, ayrıca Kurul tarafından belirlenen yeterli önlemlerin alınması şarttır."*

Önemle belirtilmelidir ki, hassas veriler kanunda açıkça ve sınırlı olarak belirlenmiş olup, yorum yoluyla hassas veriler kategorisini genişletilemez. Özel nitelikli kişisel verilerin işlenmesi kural olarak yasak olmakla birlikte, kanunda belirtilen istisnai haller bu kuralın dışındadır. Hassas nitelikli verilerin işlenmesinde, veri sorumlusunun yalnızca hukuki işleme şartına değil, aynı zamanda veri işleme ilkelerine de uygun hareket etmesi gerekmektedir. Bu ilkelerden biri olan veri minimizasyonu, işleme faaliyetinin amacıyla sınırlı, ilgili ve ölçülü verilerin işlenmesini zorunlu kılar[37]. Başka bir deyişle, yalnızca işleme amacının gerçekleştirilmesi için gerekli olan veriler toplanmalı; gereksiz, fazladan ya da konu dışı veri işleme pratiklerinden kaçınılmalıdır. Bu ilkenin doğal sonucu olarak işlenen veri hacminde bir sınırlama söz konusu olmalıdır. Avrupa Birliği Adalet Divanı'nın Norra Stockholm v. Per Nycander kararında da vurgulandığı üzere, veri minimizasyonu ilkesi yalnızca niceliksel bir sınırlama getirmemekte; aynı zamanda orantılılık denetimini de zorunlu kılmaktadır[38]. Bu bağlamda, özel nitelikli verilerin işlenmesinde hem kapsam hem de içerik bakımından titiz bir değerlendirme yapılmalı ve yalnızca açıkça gerekli olan verilerle sınırlı kalınmalıdır. Bu

[37] Gürbüz Yüksel, ''Kişisel Sağlık Verilerinin Hukuki Korunması*", Sağlık Akademisyenleri Dergisi*, Ankara, 2019, s.2.

[38] Avrupa Birliği Adalet Divanı, C-268/21, Norra Stockholm Bygg AB v. Per Nycander AB, karar tarihi: 04.05.2023, para. 45, https://curia.europa.eu/juris/document/document.jsf?text=&docid=270823&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=2078240 >, (E.T.: 28/06/2025); aktaran: Ahmet Demirtaş, ChatGPT'nin Gölgesinde Kişisel Verilerin Korunması, Kişisel Verileri Koruma Dergisi, C.6, S.1, s.20.

kapsamda, özellikle meşru menfaat temelinde gerçekleştirilen veri işleme faaliyetlerinde, "gereklilik testi" (necessity test) özel bir önem taşır[39]. ICO[40] tarafından ortaya konulan bu test üç aşamadan oluşmaktadır: (i) Amaç testi – veri işleme faaliyeti meşru bir menfaati gerçekleştirmeye yönelik midir? (ii) Gereklilik testi – bu kişisel veriler işleme amacı için gerçekten gerekli midir? (iii) Denge testi – veri sorumlusunun meşru menfaati ile ilgili kişinin temel hak ve özgürlükleri arasında adil bir denge var mıdır? Bu çerçevede, veri minimizasyonu ilkesi yalnızca veri sayısını azaltmakla sınırlı bir teknik ilke değil; işlenen her bir verinin neden gerekli olduğuna dair açık bir gerekçe sunma yükümlülüğünü de kapsar. Zira gereksiz veri toplamak, ilgili kişinin haklarını ihlal etmenin yanı sıra, veri sorumlusunun yükümlülüklerini de ağırlaştırmakta ve veri ihlali riskini artırmaktadır. Bu nedenle hem GDPR hem de 6698 sayılı Kanun'un 4. maddesinde düzenlenen "işleme amacıyla bağlantılı, sınırlı ve ölçülü olma" ilkesi gereğince, her bir veri kategorisi ayrı ayrı gereklilik denetimine tabi tutulmalı ve yalnızca işin doğası bakımından zorunlu olan veriler işlenmelidir.

GDPR çerçevesinde, kişilerin ticari birliklere üyeliklerine ilişkin bilgiler özel nitelikli kişisel veriler olarak kabul edilir. Yani, bu tür bilgiler, diğer kişisel verilerden farklı bir şekilde ele alınmakta ve daha fazla koruma gerektirmektedir[41]. Özel nitelikli kişisel veriler, daha hassas bilgiler olarak kabul edilir ve bu nedenle, bunların işlenmesi, saklanması ve paylaşılması konusunda daha katı kurallar ve düzenlemeler uygulanır. Bu bağlamda, kişilerin ticari birliklere üyelik bilgileri, bireylerin mahremiyetini korumak amacıyla özel bir koruma gerektiren hassas nitelikteki veriler sınıfına girmektedir.

Kişisel Verilerin Korunması Kanunu'nun 6. maddesinin 3/a bendinde, özel nitelikli kişisel verilerin işlenmesinde ilgili kişinin açık rızasının bulunması temel hukuka uygunluk şartı olarak öngörülmektedir. Genel Veri Koruma Tüzüğü'nde ise rıza, madde 6/1-a kapsamında genel veri işleme şartı olarak düzenlenmiş, özel nitelikli kişisel verilerin işlenmesi bakımından ise madde 9/2-a'da yer alan açık rıza şartı getirilmiştir. Bu düzenlemeler, GDPR'ın özel nitelikli verilere

[39] Ayşe Nida Günal, İş İlişkilerinde Kişisel Verilerin İşlenmesinde Hukuka Uygunluk Sebebi Olarak "Meşru Menfaat", *Kişisel Verileri Koruma Dergisi,* C.4, S.2, s. 1-18.
[40] UK Information Commissioner's Office (ICO), "Legitimate Interests", Guide to the General Data Protection Regulation (GDPR), https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/legitimate-interests/, (E.T. 28.06.2025).
[41] Tüze Yılmaz, *Avrupa Birliğinde Kişisel Verilerin Korunması Hukuku*, Adalet Yayınevi, Ankara, 1. Baskı, 2022, s.27.

ilişkin daha katı koruma mekanizmaları öngördüğünü ve bu bağlamda daha yüksek bir rıza standardı benimsediğini göstermektedir[42].

Avrupa Veri Koruma Kurulu, 05/2020 sayılı rıza rehberinde de açıkça belirttiği üzere, rızanın geçerli bir hukuki dayanak oluşturabilmesi için öncelikle GDPR madde 4/11'de tanımlanan rıza unsurlarını taşıması ve madde 7'de yer alan usulî yükümlülüklere uygun olarak verilmiş olması gerekmektedir[43]. EDPB'ye göre, özel nitelikli verilerin işlenmesi açısından, ilgili kişinin rızasının sadece açık ve özgür iradeye dayanması yetmemekte, aynı zamanda belirli, bilinçli ve açık bir beyanla ifade edilmesi gerekmektedir. Bu doğrultuda, örneğin yalnızca bir kutucuğun önceden işaretlenmiş olması ya da varsayılan rıza halleri geçerli kabul edilmemektedir (EDPB, Guidelines 05/2020, par. 93-96).

Kişisel Verileri Koruma Kurulu da benzer yönde değerlendirmelerde bulunmuş ve özellikle sağlık verileri gibi özel nitelikli verilerin işlenmesinde, kişilerin yeterince bilgilendirilmeden verdikleri rızaların geçersiz olacağına hükmetmiştir (Örn. KVK Kurulu, 31.05.2018 tarihli ve 2018/63 sayılı Karar[44]). Kurul, ilgili kişinin rızasını açıkça ve tereddüte mahal bırakmayacak biçimde beyan etmesinin şart olduğunu, bu nedenle rıza metinlerinin genel, belirsiz ve muğlak ifadeler içermemesi gerektiğini vurgulamıştır.

Kurul kararları incelendiğinde, anonim şirketlerin özel nitelikli kişisel veri işlerken genellikle açık rıza alınmaksızın veya Kanun'un öngördüğü istisna halleri dışında işlem yaptıkları ve bu durumun hukuka aykırı bulunduğu görülmektedir. 2019/162 sayılı Kurul kararında, bir anonim şirketin ilgili kişinin açık rızası bulunmaksızın sağlık ve ceza mahkûmiyeti verilerini işlemesi değerlendirilmiştir[45]. Kurul, özel nitelikli kişisel verilerin işlenmesinin ancak Kanun'un 6. maddesinde yer alan istisna hallerinden birine dayanması hâlinde mümkün olabileceğini vurgulamış; aksi durumda veri işlemenin hukuka aykırı olacağı sonucuna varmıştır. Özellikle işveren sıfatıyla faaliyet gösteren anonim şirketlerin çalışanlara ait özel nitelikli verileri işlemesi sırasında m.6/2 (açık rıza) veya m.6/3 (sır saklama yükümlüsü sağlık personeli aracılığıyla işleme) hükümlerine titizlikle riayet etmesi gerekmektedir.

---

[42] Öztürk, Bahri, Elif Altınok Çalışkan, Serkan Seyhan, *op. cit.,* s.103.
[43] EDPB, "Guidelines 05/2020 on consent under Regulation 2016/679", https://www.edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-052020-consent-under-regulation-2016679_en, (E.T.: 30/05/2025).
[44] KVKK, 31.05.2018 Tarihli ve 2018/63 sayılı Kararı, https://www.kvkk.gov.tr/Icerik/5248/2018-63, (E.T.: 30/05/2025).
[45] 31.05.2019 Tarihli ve 2019/162 Sayılı Kararı, https://www.kvkk.gov.tr/Icerik/5495/2019-162, (E.T.: 10.06.2025).

Benzer şekilde, 2020/404 sayılı Kurul kararında da işveren sıfatıyla hareket eden bir anonim şirketin, çalışanlarından açık rıza almaksızın ve aydınlatma yükümlülüğünü yerine getirmeksizin özel nitelikli verileri (örneğin sağlık verisi) işlemesi değerlendirilmiştir. Kurul, ilgili şirketin veri işleme faaliyetinin hem aydınlatma yükümlülüğü bakımından hem de özel nitelikli verilerin işlenmesine ilişkin hukuka uygunluk şartları bakımından eksik olduğunu tespit etmiş ve veri işlemenin hukuka aykırı olduğuna karar vermiştir[46]. Bu bağlamda özel hukuk tüzel kişisi olan anonim şirketler, veri sorumlusu sıfatıyla özel nitelikli kişisel verileri işlerken, yalnızca ilgili kişinin açık rızasına veya Kanun'da sınırlı şekilde sayılan diğer istisnai işleme şartlarına dayanabilirler.

Anonim şirket statüsünde faaliyet gösteren özel hastaneler, hastaların tıbbi verilerini (örneğin HIV durumu, genetik analiz sonuçları, psikiyatri teşhisleri) yalnızca mücbir sağlık sebepleriyle ilgili hizmet sunumunda görevli sağlık personeline aktarabilir. Bu tür aktarım, KVKK m.6/3 kapsamında açık rıza aranmaksızın meşru kabul edilir. Ancak, bu verilerin hastanın veya şirketin açık rızası olmadan gazeteler, medya kuruluşları veya pazarlama amaçlı üçüncü taraflarla paylaşılması hukuka aykırıdır ve Kurul tarafından 2019/372 sayılı kararla açıkça ihlal sayılmıştır[47].

Sonuç olarak hem GDPR hem de KVKK uyarınca özel nitelikli verilerin işlenmesinde "açık rıza", yalnızca formel bir onay beyanı olarak değil, açık, belirli, bilinçli ve özgürce verilmiş bir irade açıklaması olarak değerlendirilmekte; bu da veri sorumlularının rıza alma süreçlerinde hem içerik hem de yöntem bakımından daha yüksek bir dikkat ve şeffaflık standardına uymasını zorunlu kılmaktadır.

## II. KİŞİSEL VERİLERİN HUKUKİ NİTELİĞİ

Kişisel verilerinin kişinin kendine özgü veriler olması nedeniyle kendine has bir mevzuat çerçevesinde ve sıkı şekil kuralları ile gerek ulusal gerek uluslararası alanda korunması amaçlanmıştır. Doktrinde kişisel veri kavramının hukuki niteliği açısından farklı görüşler mevcuttur:

[46] KVKK, 20/05/2020 tarihli ve 2020/404 sayılı Kararı, https://www.kvkk.gov.tr/Icerik/6913/2020-404, (E.T.: 10.06.2025).
[47] KVKK, 09/12/2019 tarih ve 2019/372 sayılı Kararı, https://www.kvkk.gov.tr/Icerik/6663/2019-372, (E.T.: 10.06.2025).

## A. MÜLKİYET HAKKI GÖRÜŞÜ

Kişisel verilerin hukuki niteliği, günümüzde teknolojinin hızla gelişmesiyle birlikte sıkça tartışılan bir konudur. Özellikle Amerika Birleşik Devletleri'nde, kişisel verilerin eşya hukuku kapsamında bir "şey" olarak görüldüğü ve bireylere bu veriler üzerinde mülkiyet hakkı tanındığı yönünde genel bir görüş vardır[48]. Bu görüş, bireylerin kişisel verileri üzerindeki kontrolünü güçlendirmeyi, etkinleştirmeyi amaçlasa da ekonomik, mülkiyet hakkının doğası, pazar gücü asimetrisi, etik sorular gibi birçok eleştirileri de beraberinde doğurur. Kişisel verilerin "mülkiyet hakkı" çerçevesinde değerlendirilmesi yaklaşımı, özellikle ABD'de bazı eyaletlerde yürürlüğe giren modern veri koruma yasalarıyla birlikte geri planda kalmış ve yerini kişisel veriler üzerinde "kontrol hakkı" (right to control) anlayışına bırakmıştır[49]. Nitekim California Consumer Privacy Act (CCPA) ve onu izleyen California Privacy Rights Act (CPRA) ile bireylere tanınan haklar — örneğin veriye erişim, düzeltme, silme, veri paylaşımını engelleme gibi — verinin sahibi olma değil, üzerinde hak kullanma perspektifini esas almıştır[50]. Bu yasa kapsamında, bireyler verileri üzerinde fiilî ve hukuki denetim yetkileri kullanabilmekte, ancak veri üzerinde klasik anlamda mülkiyet hakkı tanınmamaktadır.

Söz konusu görüşe göre, kişisel veriler de eşya hukukundaki bir mal gibi kişinin bir araba, ev veya toprak üzerindeki mülkiyeti gibi bireyin mülkiyetindedir ve birey bu veriler üzerinde tasarruf hakkına sahiptir[51]. Bu hak kapsamında birey, kişisel verilerini kullanabilir, başkalarına devredebilir, serbestçe tasarruf edebilir veya bu veriler üzerinden gelir elde edebilir.

"Ekonomik değerleri ön planda tutarak kişisel verileri açıklayan bu görüş en çok ABD'de savunulmaktadır. Bu görüşü savunanlara göre kişisel veri, eşya hukukunda kişinin mülkiyeti üzerinde serbestçe tasarrufta bulunabilmesinden yola çıkılarak, kişisel verilerinin üzerinde de aynı hak ve yetkileri serbestçe eşya hukuku kuralları çerçevesinde kullanabilecektir. Bu görüşün eleştirisi ise, kişisel verilerin hukuki niteliğinde mülkiyet hakkı görüşü kabul edilirse, bu seferde ekonomik olarak mülkiyet hakkının amacına aykırılık oluşturacağı, bireylere daha fazla özgürlük sunacağı, hakimiyeti kişiye vermenin Amerikan ekonomisine zarar vereceği, hakkın kullanım amacına aykırılık oluşturacağı düşünülmektedir. Kaldı ki mülkiyet hakkı

---

[48] Saadet Kartalcı, "Kişisel Verilerin Korunması Hakkı ve Hukuki Niteliği", *Hukuk ve Bilişim Dergisi*, https://hukukvebilisim.org/kisisel-verilerin-korunmasi-hakkinin-hukuki-niteligi, (E.T: 04.05.2025).

[49] CALIFORNIA CONSUMER PRIVACY ACT (CCPA), Cal. Civ. Code § 1798.100 et seq., yürürlük: 01.01.2020, https://oag.ca.gov/privacy/ccpa, (E.T. 28.06.2025).

[50] CALIFORNIA PRIVACY RIGHTS ACT (CPRA), Cal. Civ. Code § 1798.100-1798.199.100, yürürlük: 01.01.2023, https://cppa.ca.gov/regulations/, (E.T. 28.06.2025).

[51] Rabia Özkan, *Kişisel Veri Koruma Hukukunun Kişilik Hakkının Korunması Çerçevesinde Değerlendirilmesi,* Ankara Sosyal Bilimler Üniversitesi Hukuk Fakültesi Dergisi, Cilt 3, Sayı:2, s. 683-685.

sahibine sahip olduğu şey üzerinde kullanma, yararlanma ve tasarruf yetkilerinin tümünü verirken, kişisel verilerin eşya hukukundaki gibi tasarruf edilebilir veriler olmadığı, kanun lafzından da çıkarıldığı üzere hassas niteliğe sahip oldukları ve korunması gerekmekte olduğudur. Hal böyleyken kişisel verileri, eşya hukukundaki mal üzerinde tasarruf yetkisi kullanılarak devir işlemi gerçekleştirmek veya feragat etmek kanun lafzına, koruma amacına uygun olmayacaktır[52]".

Bu görüşe yönelik birçok eleştiri bulunmaktadır:

Mülkiyet hakkının doğası gereği kişisel veriye mülkiyet hakkı atfetmek birçok sorunu beraberinde getirir. Öncelikle kişisel veri somut ve bölünebilir maddi bir eşya değildir. Mülkiyet hakkı, bir kişinin bir şeye sahip olma, kullanma ve tasarruf etme yetkisini, fiziksel varlıklar üzerindeki hakları ifade ederken, kişisel veriler soyut ve sürekli değişen bir niteliktedir. Bu nedenle, kişisel verilere mülkiyet hakkı isnat etmek hukuki ve felsefi olarak sorunlu bulunmakta, kişisel verinin niteliği ile bağdaşmamaktadır[53].

Kişisel verilerin mülkiyet hakkı olarak kabul edilmesinin birçok ekonomik etkisi olacaktır. Bu durum büyük teknoloji şirketlerinin iş modellerini ciddi şekilde etkileyebilir, veri toplama ve işleme maliyetlerinin artması sonucu inovasyonu yavaşlatabilir ve ekonomik büyümeyi olumsuz etkileyebilir[54]. Bu sonuç anonim şirketler için de birçok olası sonucu doğurur. Örneğin kişisel verilerin mülkiyet hakkı olarak kabul edilmesi sonucu anonim şirketlerde veri toplama ve işleme süreçleri için daha sıkı hukuki düzenleme getirilmesini gerektirebilir. Anonim şirketler, veri sahiplerinin açık rızalarını almak zorunda kalabilir ve veri kullanım amaçlarını daha şeffaf bir şekilde açıklamak durumunda kalabilirler. Ayrıca bu düzenlemeler daha yüksek maliyetlere sebep olabilir. Bu görüş kabul edilirse anonim şirketlerin veri toplama ve işleme süreçlerine daha çok kaynak ayırmaları gerekebilir. Şirketlerin veri güvenliği önlemlerini artırması, veri sahiplerine daha fazla bilgi verme ve rızalarını alma gibi işlemler ek maliyetlere neden olabilir.

[52] Sinan Sami Akkurt, *Kişisel Veri Kavramının Hukuki Niteliğine İlişkin Yaklaşımlara Mukayeseli Bir Bakış,* T.C. Selçuk Üniversitesi Hukuk Fakültesi, Kişisel Verileri Koruma Dergisi, Cilt: 2, Sayı: 1, s. 21-23.
[53] Furkan Kaan Yüksek, AİHM İçtihatlarında Kişisel Verilerin Korunması, *Dokuz Eylül Üniversitesi Hukuk Fakültesi Dergisi,* Cilt: 25, Sayı: 1, 2023, s.386, https://dergipark.org.tr/tr/download/article-file/3056573, (E.T: 04.05.2025).
[54] Zehra Yürük, *Kişisel Verilerin İhlalinden Doğan Özel Hukuk Sorumluluğu*, İstanbul Ticaret Üniversitesi Sosyal Bilimler Enstitüsü Özel Hukuk Anabilim Dalı, Yüksek Lisans Tezi, 2021, s.45.

Bu yaklaşım kabul edilirse kişinin verilerini satarak gelir elde etmesi ve şirketlerin bu verileri satın alarak yeni ürün ve hizmetler geliştirmeleri mümkün olacak ve veri pazarları oluşacaktır. Şirketler için başka bir konu da veri güvenliği ve şeffaflık gibi konularda rekabet ederek birbirlerinden farklılaşarak rekabette birbirlerine üstünlük sağlayabilirler. Müşterilerinin güvenlerini kazanmak, şirket imajlarını korumak ve güçlendirmek için veri koruma ilkelerine daha fazla önem vermeleri gerekecektir. Kişisel verileri izinsiz kullanan, sızdıran veya veri koruma düzenlemelerine uymayan şirketler de hem veri sahiplerine tazminat ödemek hem de idari para cezaları ödemek durumunda kalacaktır. Kısacası kişisel veriler mülkiyet hakkı olarak kabul edilirse anonim şirketler için hem fırsatlar hem de riskler oluşacaktır. Şirketler, bu yeni düzenlemelere uyum sağlayarak ve veri güvenliği konusunda yatırım yaparak uzun vadede başarılı olabilse de şirketlerin iş modellerini ve stratejilerini yeniden gözden geçirmeleri gerekebilir.

Kişisel verilerin mülkiyet hakkı olarak kabul edilmesinin diğer bir sonucu da pazar gücü asimetrisi oluşmasına sebep olmasıdır[55]. Kişiler ve büyük teknoloji şirketleri arasında pazarlık gücü arasındaki dengesizlik, bireylerin kişisel verileri üzerinden haklarını etkin bir şekilde savunmalarını zorlaştıracaktır. Kişisel verileri mülkiyet hakkı ile birlikte metalaştırmak, insan onurunu zedeleyebilir ve mahremiyet hakkını ihlal edebilir. Bu da etik sorunlara yol açacaktır.

Zannımca mülkiyet hakkı görüşü yerine, kişisel verilerin korunması için daha kapsamlı ve çok boyutlu bir yaklaşım benimsenmesi ve bu yaklaşımın hem bireylerin haklarını koruyacak hem de teknolojik gelişmelere ayak uyduracak şekilde tasarlanması gerekmektedir.

Mülkiyet hakkı görüşünün Türk hukukundaki karşılığı konusuna gelecek olursak; hukukumuzda, kişisel verilerin mülkiyet hakkı olarak görüldüğü yönünde net bir yaklaşım bulunmamaktadır. 6698 sayılı Kişisel Verilerin Korunması Kanunu, kişisel verileri bir "şey" olarak değil, bireyin kişilik hakkının bir parçası olarak değerlendirmektedir ancak, kişisel verilerin ekonomik bir değeri olduğu ve bununda ticari amaçlarla kullanıldığı da gerçektir. Ancak, mevcut yasal düzenlemeler çerçevesinde kanunumuz, bireylerin kişisel verileri üzerindeki haklarını, mülkiyet hakkı yerine, mahremiyet hakkı ve diğer temel haklar bağlamında ele almaktadır.

[55] Rabia Özkan, *op. cit.* s.685.

Avrupa Birliği Genel Veri Koruma Tüzüğü, kişisel veriler üzerinde mülkiyet hakkı tanımamakta; bunun yerine, bireylere temel hak ve özgürlükler kapsamında koruma sağlamaktadır. Nitekim GDPR m.1 ve m.4 çerçevesinde kişisel verilerin işlenmesi, "kişinin kimliğine ilişkin" ve "kişisel mahremiyeti etkileyen" bir alan olarak görülmektedir. AB Adalet Divanı da kararlarında verilerin mülkiyet nesnesi değil, kimlikle doğrudan bağlantılı hak konusu olduğunu açıkça vurgulamaktadır[56]. Bu bağlamda hem GDPR hem de Avrupa Konseyi'nin 108 No.lu Sözleşmesi'nde kişisel verilerin "ekonomik değer taşısa bile mülkiyete konu edilemeyeceği" temel prensip hâline gelmiştir. Bu yaklaşım, veri özerkliğini ve bireyin kendisi üzerindeki denetimini esas alan "veri öznesi merkezli" bir sistemin benimsendiğini göstermektedir[57].

### B. FİKRİ HAK GÖRÜŞÜ

Kişisel verilerin hukuki niteliği tartışmalarında öne çıkan yaklaşımlardan biri de kişisel verilerin fikri mülkiyet hakları kapsamında değerlendirilmesi gerektiği yönündeki bu görüştür. Bu görüşte yine Amerikan hukuku tarafından benimsenmiştir. Bu görüşün, kişisel verilerin bir tür "fikri eser" olarak kabul edilmesini ve bu nedenle fikri mülkiyet hukukunun korumasına alınması gerektiğini destekler. Aynı zamanda bu görüşün savunucuları telif hakkıyla kişisel veri arasında bağlantı kurarak kişisel verileri fikri mülkiyet hakkı kapsamında değerlendirme amacı güder[58].

Fikri mülkiyet hakkı yaklaşımının temel savı olarak bu yaklaşımın savunucuları, kişisel verilerin fikri mülkiyet hukukunun koruması altına alınması gerektiğini ileri sürerek, kişisel verilerin de tıpkı bir kitap, tablo veya müzik parçası gibi bir "eser" olduğunu savunurlar. Bu görüşün temel dayanakları olarak; amaçsal benzerlik (hem fikri mülkiyet hem de kişisel

---

[56] Bknz. CJEU, Nowak v. Data Protection Commissioner, Case C-434/16, ECLI:EU:C:2017:994; ayrıca bkz. Avrupa Konseyi, Convention 108+, Modernised Convention for the Protection of Individuals with Regard to the Processing of Personal Data, 2018.

[57] Kaliforniya dışında da birçok Amerikan eyaleti kişisel verilerin işlenmesine dair mevzuatlar yürürlüğe koymuştur. Virginia, Colorado, Connecticut ve Utah eyaletlerinin 2023 itibarıyla yürürlüğe giren veri koruma yasaları, kişisel veriler üzerinde mülkiyet hakkını tanımamış; bunun yerine veri sahiplerine sınırlı, denetlenebilir ve devredilemez kişisel kontrol hakları tanımıştır. Bu düzenlemeler, verinin kişiliğe sıkı sıkıya bağlı bir değer olduğu yönündeki modern anlayışla örtüşmektedir. Bknz. Virginia Consumer Data Protection Act (VCDPA), Code of Virginia § 59.1-575 et seq., yürürlük: 01.01.2023, https://law.lis.virginia.gov/vacode/title59.1/chapter53/, Colorado Privacy Act (CPA), Colo. Rev. Stat. § 6-1-1301 et seq., yürürlük: 01.07.2023, https://coag.gov/resources/colorado-privacy-act/, Connecticut Data Privacy Act (CTDPA), Public Act No. 22-15, yürürlük: 01.07.2023, https://www.cga.ct.gov/2022/ACT/PA/PDF/2022PA-00015-R00SB-00006-PA.PDF, Utah Consumer Privacy Act (UCPA), Utah Code Ann. § 13-61-101 et seq., yürürlük: 31.12.2023, https://le.utah.gov/~2022/bills/static/SB0227.html, (E.T. 28.06.2025).

[58] Elif Küzeci**,** *Kişisel Verilerin Korunması,* Ankara, Turhan Kitabevi, 3. Baskı, 2019, s.66.

verilerin korunmasının temel amacının yaratıcı çalışmaları ve kişisel bilgileri korumak[59], inovasyonu teşvik etme); üretim benzerliği (kişisel verilerin bir bakıma bireyin zihinsel faaliyetlerinin bir ürünü olması ve bu nedenle fikri bir eser olarak kabul edilebilir olması); hakların benzerliği (fikri mülkiyet sahiplerin ortak yönü olarak kişisel veri sahiplerinin eserleri veya verileri üzerinde kullanım, çoğaltma ve kamuya sunma gibi hakları elinde bulundurması) örnek verilebilir[60].

Benzerliklere rağmen bu görüş birçok eleştiri de almaktadır. Her ne kadar kişisel verilerin fikri mülkiyet hakkı olduğu yönünde değerlendirilmeler cazip gibi gelse de bu yaklaşımın da birçok sakıncası bulunmaktadır. Kişisel verilerin somut bir varlık olmadığı, fikri mülkiyet haklarının daha kesin bir hukuki çerçeveye sahip olduğu unutulmamalı ve kişisel verilerin kolaylıkla çoğaltılabilmesinin oluşturacağı mahremiyet ihlallerinin, hukuki belirsizliklerin, değer kaybı sorununun ve kontrolsüz yayılım riski oluşturabileceği gerçeği göz ardı edilmemelidir[61].

Doktrinde yazarlar[62], kişisel verilerin korunması hakkı ile fikri mülkiyet haklarını her ne kadar birlikte ele alsalar da fikri mülkiyet hakkı eser sahibinin eseri üzerindeki haklarını korurken, kişisel verilerin korunması hukukunda kişinin kendi verileri üzerindeki tasarruflarını korur. Kanaatimce, benzer yönleri bulunsa bile kişisel veriler fikri mülkiyet haklarından farklı olarak ele alınmalıdır. Bir eser sahibi, eserini özgün bir şekilde oluşturabilirken, biz kişisel verilerimizi iradi olarak seçme kuvvetinde değiliz. Örneğin bir ressam bir insan figürü resmederken, istediği

[59] Furkan Kaan Yüksek, AİHM İçtihatlarında Kişisel Verilerin Korunması, *Dokuz Eylül Üniversitesi Hukuk Fakültesi Dergisi,* Cilt: 25, Sayı: 1, 2023, s.386, https://dergipark.org.tr/tr/download/article-file/3056573, (E.T: 04.05.2025).

[60] Sinan Sami Akkurt, ‘‘Kişisel Veri Kavramının Hukuki Niteliğine İlişkin Yaklaşımlara Mukayeseli Bir Bakış’’, *Kişisel Verileri Koruma Dergisi,* Cilt 2, Sayı 1, 2020, s.20-32.

[61] Furkan Kaan Yüksek, *op. cit.,* s.386.

[62] Görüş hakkında ayrıca bkz. Sinan Sami Akkurt, *op. cit*. s. 24; Jonathan Zittrain, “What the Publisher Can Teach the Patient: Intellectual Property and Privacy in an Era of Trusted Privication*”, Stanford Law Review*, Cilt 52, 2000, s. 1203; Ann Bartow, “Our Date, Ourselves: Privacy, Propertization and Gender”, *USFL. Review,* C. 34, s. 685-693; Lawrence Lessig, “Privacy as Property”, *Social Research*, C. 69, S. 1, 2002, s. 201; Ahmet M. Kılıçoğlu, “Fikri Hakların İhlalinde Hukuksal Koruma Yolları (Sınai Haklarla Karşılaştırmalı Olarak)”, *Türkiye Barolar Birliği Dergisi*, S. 54, 2004, s. 54; Dülger, *op. cit.,* 2019, s. 4; Furkan Güven Taştan, *Türk Sözleşme Hukukunda Kişisel Verilerin Korunması,* İstanbul, On İki Levha Yayıncılık, 2017.s. 57-60; Hüseyin Can Aksoy, *Medeni Hukuk ve Özellikle Kişilik Hakkı Yönünden Kişisel Verilerin Korunması*. Ankara, Çakmak Yayınevi, 2010, s. 60, Corien Prins, “When Personal Data, Behavior and Virtual Identities Become a Commodity: Would a Property Rights Approach Matter?”, *Script – ed*, C. 3, S. 4, 2006, s. 279; Pamela Samuelson, “Privacy as Intellectual Property?”, *Stanford Law Review*, C. 52, 2000, s. 1134; Aydın Akgül, *Danıştay ve Avrupa İnsan Hakları Mahkemesi Kararları Işığında Kişisel Verilerin Korunması,* İstanbul, Legal Yayıncılık, 2010, s. 74; A. Çiğdem Ayözger Öngün, *Elektronik Haberleşme Sektörüne İlişkin Özel Düzenlemeler Dahil Kişisel Verilerin Korunması Hukuku*. İstanbul, Beta Yayıncılık, 2019, s. 17; Küzeci, *op. cit.,* s. 66.

gibi göz rengini, saç rengini vs. seçebilirken, bizim saç veya göz rengimiz, parmak izimiz gibi kişisel verilerimiz doğuştan genetik olarak gelir.

Eğer kişisel verileri fikri hak olarak kabul edersek bu durum anonim şirketler için birçok sonuç doğuracaktır. Bunlardan ilki kişisel verinin sahibinin kim olacağı sorusudur. Verileri toplayan şirket mi, yoksa veriye konu olan birey mi kişisel verinin sahibi olacaktır? Bu sorunun net bir cevabı olmadığı sürece, şirketler hukuki belirsizliklerle karşı karşıya kalabilir ve süreç zorlaşabilir. Ayrıca şirketlerin kişisel verileri kullanabilmeleri için veri sahiplerinden telif hakkı almalarını gerektirebilir. Bu durum sonucunda, şirketlerin maliyetlerini artıracak ve yeni iş modelleri geliştirilmesini zorlaştıracaktır. Bir diğer sonuç olarak, kişisel verilerin aktarım süreçleri karmaşık hale gelebilir. Her ülkenin farklı fikri hak koruma düzenlemeleri olduğu için, anonim şirketler uluslararası veri transferlerinde kısıtlamalar doğabilir ve önemli engellerle karşılaşabilirler. Veri güvenliği ve şeffaflık konusunda daha iyi uygulamaları olan şirketler, rekabette avantaj sağlayarak rakiplerinden farklılaşabilirler.

### C. KİŞİLİK HAKKI GÖRÜŞÜ

Öğretide tartışılan diğer bir görüş ise kişisel verilerin şahıs varlığı haklarından olduğu görüşüdür. Bu görüş genelde kıta Avrupası hukuk ekolü tarafından benimsenmiş olup, kişisel verilerin korunmasını insan hakları çerçevesinde ele alır[63]. Bu görüşe göre, kişisel veriler sadece bir bilgi yığını olarak görülmez. Kişisel veriyi bireyin kimliğini, özel hayatını ve hatta geleceğini şekillendiren değerli bir varlık olarak ele alır[64]. Kişisel verilerin şahıs varlığı haklarından olduğu bu görüş, bireylerin mahremiyet hakkı, onur ve haysiyet hakkı gibi temel haklarının korunması için önemlidir. Kişisel verilerin korunması konusunda daha kapsamlı ve etkili düzenlemelerin yapılmasına katkı sağlar. Yapay zeka ve büyük veri gibi teknolojilerin gelişmesiyle birlikte kişisel verilerin önemi daha da artmaktadır bu nedenle bu yaklaşım, bu teknolojilerin geliştirilmesi ve kullanılması sürecinde bireylerin haklarının korunmasını sağlar. Elbette bu görüş için de eleştiriler mevcuttur. Kişisel verilerin somut bir varlık olmadığı ve mülkiyet hakkı gibi bir hakla korunmasının zor olduğu iddiaları başlıca eleştiriler arasındadır[65].

[63]Sinan Sami Akkurt, "Kişisel Verilerin Korunması Hakkının Hukuki Niteliği." Hukuk ve Bilişim Dergisi, https://hukukvebilisim.org/kisisel-verilerin-korunmasi-hakkinin-hukuki-niteligi (E.T: 04.05.2025).
[64] Dilek Yüksel Civelek, Kişisel Verilerin Korunması ve Bir kurumsal Yapılanma Önerisi, Bilgi Toplumu Dairesi Başkanlığı, Ankara, 2011, s.14, https://www.sbb.gov.tr/wp-content/uploads/2022/08/Kisisel-Verilerin-Korunmasi-ve-Bir-Kurumsal-Yapilanma-Onerisi-Dilek-Yuksel-Civelek.pdf, (E.T: 04.05.2025).
[65] Aydın Akgül, Danıştay ve Avrupa İnsan Hakları Mahkemesi Kararları Işığında Kişisel Verilerin Korunması, Beta Yayınları, Ankara, 2016, s.73.

Bu görüş Anonim Şirketler içinde birtakım sonuçlar doğuracaktır. Şirketin veri sorumluları ve veri işleyenleri, kişisel verileri toplama, işleme ve saklama süreçlerinde daha dikkatli olmak zorunda kalacak ve veri güvenliği önlemlerini güçlendirmek için yatırım yapmaları gerekecektir. Kişisel verilerin şahıs varlığı hakkı olarak kabul edilmesi, hukuki anlamda birçok belirsizliği beraberinde getirebilir ve bu görüş, özellikle veriye dayalı iş modelleri üzerine kurulu şirketlerin faaliyetlerini sınırlayabilir ve ekonomik büyümeyi olumsuz etkileyebilir.

Kişilik hakkı, bir bireyi diğerlerinden ayıran ve bireyi kendisi yapan maddi ve manevi özelliklerin toplamıdır. Kişisel veriler de bireyin özünü oluşturan ve kişiliğini tanımlayan önemli bir unsurdur. Avrupa İnsan Hakları Sözleşmesi madde 8[66]'de yine kişisel verileri koruma altına almak için düzenlenmiştir. AİHM kararları, kişisel verilerin izinsiz işlenmesinin, bireyin kimliğine ve özel hayatına müdahale olarak değerlendirilmesi gerektiğini vurgulamakta; AİHS Madde 8'de, kişisel verilerin yalnızca bir bilgi yığını değil, bireyin ayrılmaz bir parçası olduğunu ve bu nedenle özel hayat hakkı kapsamında korunması gerektiğini vurgulamaktadır[67]. Böylece, bireylerin mahremiyeti, kimliği ve özgürlükleri daha iyi korunacaktır. Görüşün en büyük eleştirilerinde biri de kişilik hakkı kapsamında her türlü verinin korunmasının mümkün olmaması, bazı verilerin kamuya açık olduğu ve bunun da özel hayatın gizliliğini kapsamında değerlendirilemeyeceği, daha sınırlı bir koruma sağlanabileceği yönündedir.

Bu eleştiriler anonim şirketler bakımından önemli sonuçlar doğurmaktadır. Birçok anonim şirket, sosyal medya kanallarındaki kamuya açık profilleri analiz eder ve potansiyel müşterileri hakkında bilgi toplar. Bu sosyal medya platformlarındaki profillerde yer alan ad-soyad, yaş, ilgi alanları, beğeniler gibi bilgiler, aslında kişisel veri olsa da kullanıcılar tarafından gönüllü olarak paylaşıldığı, alenileştirildiği için özel hayatın gizliliği kapsamında tam koruma altında olmayabilir.

Anonim şirketler, bir web sitesini ziyaret eden kullanıcıların IP adresleri, tarayıcı türleri, ziyaret ettikleri sayfalar gibi bilgileri; web sitesinin performansını iyileştirmek ve kullanıcı deneyimini kişiselleştirmek için kullanılabilir. Ancak, bu verilerin tamamı bireyin özel hayatına dair

[66] https://fra-europa-eu.translate.goog/en/law-reference/european-convention-human-rights-article-8-0?_x_tr_sl=en&_x_tr_tl=tr&_x_tr_hl=tr&_x_tr_pto=tc, (E.T:04.05.2025).
[67] Avrupa İnsan Hakları Sözleşmesi 8. Madde Rehberi, https://inhak.adalet.gov.tr/Resimler/Dokuman/482020115014Guide%20Art%208-TUR.pdf, (E.T:04.05.2025).

derinlemesine bilgi vermeyebilir ve özel hayatın gizliliği kapsamında tam koruma altında olmayabilir.

Anonim şirketlerin işe alım sürecinde, iş başvurularında yer alan ad-soyad, eğitim bilgileri, deneyim gibi bilgiler, kişisel veri olarak kabul edilse de şirkete işe alım süreci için başvuran adayları değerlendirmek için bu bilgilere ihtiyaç duyulacaktır. Bu tür verilerin, potansiyel adayın rızası ile işveren tarafından işlenmesi, özel hayatın gizliliği ile bağdaşabilir. Özetle, anonim şirketler, bu örneklerde olduğu gibi kişisel verilerin tamamını değil yalnızca özel hayatın gizliliğini ihlal edebilecek nitelikteki verileri koruma yükümlülüğü altındadır. Kamuya açık bir şekilde paylaşılan veya iş amaçlarıyla gerekli olan veriler, daha sınırlı korumaya tabi olabilir. Kaldı ki KVKK'nın 5. Maddesi bu konuda düzenlemeler getirmiştir. Bu husus ileri ki bölümlerde ayrıntılı olarak açıklanacaktır.

## III. KİŞİSEL VERİLERİN İŞLENMESİNDE TEMEL İLKELER

### A. GENEL OLARAK

Kişisel verilerin işlenmesi için dikkat edilmesi gereken ilke ve esaslar hem iç hukukumuzda hem uluslararası mevzuatta çeşitli maddelerle ele alınmıştır. Koruma altına alınan bu ilke ve esaslara uyulmaması, gerçekleştirilen işlemlerin hukuka aykırı kılınmasına sebebiyet verecektir.

OECD tarafından yayımlanan rehber ilkeler şunlardır[68]:

- Veri toplamanın sınırlılığı ilkesi
- Veri kalitesi ilkesi
- Belirli amaç ilkesi
- Kullanımın sınırlılığı ilkesi
- Veri güvenliği ilkesi
- Açıklık ilkesi
- Bireyin katılımı ilkesi
- Hesap verilebilirlik ilkesi

Buna ek olarak 1981 yılında Avrupa Konseyi 108 sayılı 'Kişisel Verilerin Otomatik Olarak İşlenmesi Sırasında Gerçek Kişilerin Korunmasına İlişkin Sözleşme'nin ve 95/46/EC sayılı Veri Koruma Direktifi ve 2016/679 sayılı Genel Veri Koruma Tüzüğünün ilgili maddelerinde;

[68] https://kvkkblog.com/kisisel-verilerin-korunmasi-tarihine-yolculuk/ Erişim Tarihi: 28.04.2023.

adil biçimde ve yasal yoldan elde edilme ve işlenme, belli ve meşru amaçlar için kaydedilme ve bu amaçlara aykırı şekilde kullanılmama, kaydedilme amaçlarına göre uygun ve yerinde olma, aşırı olmama, doğru bilgileri yansıtma ve gerektiğinde güncellenme, kaydedilme amaçlarına gerçekleştirmek için gerekli olan süreyi aşmayacak şekilde ilgili kişilerin kimliklerini belirlemeye imkan veren bir biçimde saklanma ilkeleri yer almaktadır[69].

KVKK'nın 4. Maddesinde kişisel verilerin işlenmesi sırasında uyulması gereken ilkeler tahdidi olarak sayılmıştır. Maddeye göre;

*"(1) Kişisel veriler, ancak bu Kanunda ve diğer kanunlarda öngörülen usul ve esaslara uygun olarak işlenebilir.*

*(2) Kişisel verilerin işlenmesinde aşağıdaki ilkelere uyulması zorunludur:*

*a) Hukuka ve dürüstlük kurallarına uygun olma.*

*b) Doğru ve gerektiğinde güncel olma.*

*c) Belirli, açık ve meşru amaçlar için işlenme.*

*ç) İşlendikleri amaçla bağlantılı, sınırlı ve ölçülü olma.*

*d) İlgili mevzuatta öngörülen veya işlendikleri amaç için gerekli olan süre kadar muhafaza edilme."*

KVKK 4. Maddesi birinci fıkrası kişisel verilerin işlenmesi konusunda temel bir ilke olan kanunilik ilkesini benimsemiştir. Bu ilke gereği kişisel veriler sadece KVKK'da belirtilen ve ilgili diğer kanunlarda öngörülen hallerde ve usuller ile işlenebilir. Yani kişisel verilerin işlenmesi keyfiyete dayanamaz, ancak kanuni bir dayanağı olduğu hallerde ve kanuni usullere uyularak işlenebilir.

### B. Hukuka ve Dürüstlük Kurallarına Uygun Olma ilkesi

Bu ilke hukukun genel hukuk kuralı ve evrensel hukukun ilkelerinden olduğu için diğer ilkeleri de kapsayıcı niteliktedir. Hukuka ve dürüstlük kurallarına uygunluk ilkesi, KVKK'nın yanı sıra diğer mevzuatlarda da yer almaktadır. Örneğin GVKT'de ilkeden bahseder, fakat ek olarak şeffaflık unsurunu da ele almıştır.

Hukuka uygun bir kişisel verilerin işlenme sürecinin gerçekleştirilebilmesi yalnızca genel hukuk normlarıyla değil, ilgili kanunlar ve diğer hukuki kurallar ile de tam uyumlu olması

[69] İmançlı, *op. cit.,* s.107.

gereklidir. Veri işleme faaliyetinin hukuka uygun olması hem anayasa ve ilgili kanunlara hem de KVKK'ya ve somut olaya göre tabi olunacak spesifik hukuk kurallarına bağlıdır[70].

*"Dürüstlük kurallarına uygunluk ise hukukumuzda, Medeni Kanun'un 2. maddesinde düzenlenen dürüstlük kuralının, kişisel veriler işlenirken ihlal edilmemesidir. Bu ilke kişisel veriler işlenirken, hakkın kötüye kullanılmasına ilişkin yasağa uyulmasını gerektirmektedir. Dürüstlük kuralı, kişilerin haklarını kullanırken güven kurallarına uygun ve makul bir kimseden beklenen şekilde davranılmasını ifade eder. Dürüstlük kuralının sınırları, her somut olayda objektif bir kimseden beklenecek davranışa göre belirlenir, kişilerin sübjektif durumu göz önüne alınmaz. Dürüstlük kuralına aykırılığın söz konusu olduğu durumlarda kişi, hakkını kullanmakta ve bu hakkın sınırları içinde davranmakta, ancak hakkın amacına aykırı şekilde hareket etmektedir[71]."*

Hukuka ve dürüstlük kurallarına uygun olma ilkesi, veri işleme faaliyetlerini yalnızca kanuni dayanağa sahipse işlenebilir olarak görmez. Aynı zamanda dürüstlük ve adalet ilkeleri gözetilerek bu sürecin yürütülmesi bu ilkenin bir gereğidir. Bu bağlamda dürüstlük kuralı ele alındığında; veri işleyen veri sorumlularının verileri toplama, kullanma ve işleme süreçlerinde şeffaf ve öngörülebilir olmaları gerekmektedir. Bir anonim şirketin işe alım sürecinde başvuran kişilerin verilerinin işlenmesi sırasında kişiyi yeterince bilgilendirmez, çıkarlarını zedeleyecek veya meşru beklentilerini göze almadan bir veri işleme faaliyetinde bulunacak olursa dürüstlük ilkesine aykırı biçimde bir veri işleme faaliyetinde bulunmuş olacaktır. Örneğin, işe alım sürecinde kişinin doğu kökenli olup olmaması gibi bir veri talep etmesi ve bundan dolayı kişisi hakkaniyetsiz olarak elemesi ölçüsüz bir veri toplama ve kullanma süreci gerçekleştirerek dürüstlük ihlaline sebebiyet verecektir.

*"Dürüstlük kurallarına uygun olma, veri işleme faaliyetinde bulunan kimselerin, verisi işlenen kişilerin çıkarlarını, makul beklentilerini göz önüne almaları ve onları göremeyeceği tarzda davranmamaları, işleme faaliyetinde asgari miktarda veri işlemeleri gereğini içerir. Dürüstlük kurallarına uygun olarak veri işleyen veri sorumlusu, kendisine hukuken tanınan veri işleme hakkını kötüye kullanmayacaktır[72]."*

KVKK'nın temel ilkelerinden biri olan "hukuka ve dürüstlük kurallarına uygun olma" ilkesi, anonim şirketler için de büyük önem taşır. Örneğin, bir anonim şirketin müşteri verilerinin

[70] Dülger, *op. cit.,* s.263-264.
[71] Kişisel Verilerin İşlenmesine İlişkin Temel İlkeler https://www.kvkk.gov.tr s.3. Erişim Tarihi 28.04.2023
[72] Orak**,** *op. cit.,* s. 56.

işlenmesi sürecinde elde ettiği kişisel verileri pazarlama amaçlı kullanmak istiyorsa müşterilerinden açık rıza alması gerekmektedir. Yine bir anonim şirket, çalışan verilerinin işlenmesi için çalışanlarının maaş ödemeleri, sosyal güvenlik işlemleri gibi işlemleri bakımından kişisel verilerini işler. Bu işlemler, iş sözleşmesi gibi hukuki bir dayanağı olduğu için hukuka uygun olacaktır. Ancak, çalışanların sağlık bilgileri gibi özel hayatlarına ilişkin bilgileri işlemek için çalışanların açık rızası alınması gerekmektedir. Bir şirket pazarlama faaliyetleri bakımından müşterilerine e-posta veya mesaj yolu ile kampanya mesajları göndermek istiyorsa, müşterilerden önceden açık rıza alması gerekmektedir. Aksi halde, bu durum spam olarak değerlendirilebilir ve hukuka aykırılık oluşturacaktır. Anonim şirketler için hukuka ve dürüstlük kurallarına uygunluğu ilkesine özen gösterilmesi; başta müşteriler, çalışanlar ve diğer paydaşlar bakımından güvenilirliğini artırması açısından önemi büyüktür. Ayrıca KVKK'ya uyum sağlayarak şirketleri olası hukuki yaptırımlardan korur ve veri güvenliği sağlayarak diğer şirketlere yönelik rekabet avantajı sağlar.

### C. Doğru ve Gerektiğinde Güncel Olma İlkesi

Kişisel verilerin doğruluğu ve güncelliği ilkesi, güvenilir bir veri işleme sürecinin mihenk taşlarından biridir. Bu ilke hem bireylerin haklarının korunması hem de veri sorumlularının doğru kararlar alması için hayati önem taşır. Doğru olmayan veya güncel olmayan veriler, bireylerin haklarının ihlal edilmesine neden olarak, haksız durumlara maruz kalmalarına ve yanlış kararların alınmasına sebebiyet verir. Bu nedenle, kişisel verileri işleyen veri sorumlusu kurum ve şirketler, verilerin doğruluğunu sağlamak için gerekli tüm önlemleri almakla işledikleri kişisel verilerin doğru olmasını temin etmekle ve bu verilerin doğruluğunu sürekli kontrol etmekle ve güncellemekle mükelleftir[73].

KVKK'ya göre herkes verilerinin düzeltilmesi hakkına sahip olmakla birlikte, bu ilke kanunun 4/2-b maddesinde ve GDPR'in ise 5/1-d maddesinde de düzenlenmiştir. KVKK m. 11/1/d uyarınca *"İlgili kişi, verilerin eksik veya yanlış işlenmiş olması halinde bunların düzeltilmesi hakkına sahiptir."* Görüldüğü üzere eğer veriler doğru ve güncel olarak tutulmazsa ilgili kişinin düzeltme talep hakkı doğacaktır.

Doğru ve gerektiğinde güncel olma ilkesi bakımından ele alınması gereken temel nokta, doğru tutulma ve güncel tutulma süreçlerinin farklılığıdır. Mutlak bir gereklilik olarak karşımıza çıkan

[73] ''KVKK Kişisel Verilerin İşlenmesine ilişkin Temel İlkeler'' https://www.kvkk.gov.tr/Icerik/4189/Kisisel-Verilerin-Islenmesine-Iliskin-Temel-Ilkeler Erişim Tarihi:25.11.2024

doğruluk ilkesi için özel bir hale gerek yoktur, her hal ve durumda doğruluk sağlanmalıdır. Fakat verinin güncel tutulma gerekliliği işleme amacına göre güncelliğin mühim olduğu hallerde, yalnızca gerektiği durumlarda zorunlu hale gelir. Bu farklılık veri sorumlusunun veri işleme faaliyetini gerçekleştirirken ki yükümlüklerini belirler[74]. Örneğin, THY Teknik Anonim Şirketinde çalışan bir uçuş personelinin kimlik numarası gibi bir verisi değişip güncelleme gerektirmezken, kilo verisi değişebilen bir veri olduğu için güncelleme yapılması gereklidir.

Bir anonim şirketin çalışanlarının banka hesap bilgileri, maaş ödemelerinin doğru yapılabilmesi için doğru ve güncel olması gerekmektedir. Aksi halde yanlış bir banka hesap bilgisi çalışanın mağduriyetine neden olabilir. Veya acil durum iletişim bilgileri, hastalık bilgileri gibi verilerin güncel ve doğru olması gereklidir ki olası bir acil durumda doğru müdahale uygulansın ve yakınlarına hızlıca haber verilebilsin. Örneğin bir çalışanın alenileşmiş şeker hastalığı olmasına rağmen, acil durum iletişim bilgileri ve sağlık verilerinin eksik veya yanlış olması nedeniyle yaşanan olumsuz sonuçlar veri sorumlusunun yani şirketin hukuki yaptırımlarla karşılaşmasına neden olabilir.

Sonuç olarak, doğru verileri kullanmak her şartta zorunluluk gerektirirken, güncel verileri kullanmak verinin niteliğine ve işin spesifikliğine göre değişebilir ve ihtiyaç duyulduğu zaman zorunluluk haline gelir. Doğru ve gerektiğinde güncel olma ilkesine uyum verisi işlenenlerin haklarının korunması ve veri sorumlularının kişisel verilerin korunmasıyla ilgili tüm yasal yükümlülüklerini yerine getirmesini, veri güvenliğini sağlar.

### D. Belirli, Açık ve Meşru Amaçlar İçin İşlenme İlkesi

GDPR m.5(1) b bendinde ve KVKK m.4 fıkra 2'nin (c) bendinde düzenlenmiş olan ilke kişisel verinin işlenirken amacına hizmet edecek, amacın niteliğine uygun ve bu amacın meşru olması yönelik, yapılacak işleme orantılı şekilde veri işleminin sağlanması gerekliliğini ifade eder. KVKK tasarı gerekçesinde bu "amacın belirliliği ilkesi" olarak da tanımlanır. Bu ilke, veri işleme faaliyetinin temel gerekçesini oluşturan meşru amacın net bir şekilde belirlenmesini mecburi hale getirir. Kişisel veri işleme faaliyetinin meşruluğunu kanıtlayan en önemli unsur bir veri sorumlusu için belirlenen amaçtır. Veri sorumlusunu sınırlayan bir çerçeveyi amaç unsuru oluşturur. Amaç unsuru veri sorumlusuna uyarı işlevi görerek veri sorumlusunun veri işleme faaliyetini amaç dışı bir alana taşımasının ve böylece kişisel verilerin kötüye

[74] Dülger**,** *op. cit.,* s.293.

kullanılmasının önüne geçilir. Belirli ve açık bir amaç, veri sahibine hangi amaçla kişisel verisinin işlendiğini anlamasını sağlayarak şeffaflığı güçlendirir ve veri sahibinin haklarını korur. Ayrıca veri sahibinin hangi hakları olduğunu ve bunları nasıl kullanabileceğini belirler[75]. Belirli amaç belirlenirken işleme faaliyetinin koşulları, işlenen verilerin kapsamı ve niteliği ile işleme sonucunda ortaya çıkabilecek riskler göz önünde bulundurulmalıdır. Amaç ne çok genel ne de aşırı detaylı olmalı ve amaçların birbiriyle ilişkisi olmalıdır. İleride gerekli olma ihtimali ile veri toplamak, amaç belirleme ilkesine aykırıdır. Veri, yalnızca mevcut ve belirli bir amaca yönelik olarak toplanabilir. Verisi kullanılacak kişi, verini ne amaçla kullanılacağı hakkında bilgi sahibi olmalı, uygun bir şekilde aydınlatılmalıdır. Veri sorumlusunun aydınlatma yükümlülüğü ile verisi kullanılan kişinin bilgilendirilme hakkının yakından ilişkili olduğu görülmektedir[76]. Örneğin, "şirketin pazarlama faaliyetleri için gerekli" gibi genel bir ifade yeterli olmayacaktır.

KVKK m. 4/2/c'de "işleme" kavramının kullanılması, amacın işleme anında belirlenmesi gerektiği şeklinde yorumlanmaktadır. İşleme kavramı toplamayı da kapsadığından, bu durum toplama anında en geç amacın belirlenmiş olması gerektiği sonucunu destekler. GDPR m.5(1) b bendine göre de *ilk işleme her zaman toplamadır. Toplamadan sonra gerçekleşen her türlü işleme faaliyeti ise sonraki işlemedir. Bu kapsamda toplamadan hemen sonra gerçekleşen depolama işlemi de sonraki işlemedir.*

Avrupa Birliği Genel Veri Koruma Tüzüğü'nün 5/1-b maddesine göre, kişisel verilerin işlenmesinin, başlangıçtaki amaca uygun olması gerekir. Ancak, işleme sürecinde amaçlar değişebilir veya genişleyebilir. Bu durumda, yeni amaç ile ilk amaç arasında bir uyum olup olmadığının değerlendirilmesi gerekmektedir. Çalışma Grubu, uygunluk değerlendirmesinde iki farklı yaklaşım sunar ve bunlardan esasa dayalı olanı, şekli yaklaşıma (Formal Assessment) göre daha uygun bulmuştur. Şekli yaklaşımda, yeni amaç ile ilk amaç arasındaki uyum, metinsel olarak değerlendirilir. Yani yeni amaç, ilk amaçta belirtilen kapsam içinde mi, yoksa tamamen farklı bir amaç mı olduğu incelenir. Veri sorumlusunun, verilerin sonraki işleme amacının, başlangıçta belirtilen amaçla açık veya örtük bir şekilde uyumlu olup olmadığını değerlendirmesi gerektiği vurgulanmıştır. Buna karşın, esasa ilişkin yaklaşımda, sadece metne

[75] Nafiye Yücedağ, ''Kişisel Verilerin Korunması Kanunu Kapsamında Genel İlkeler'', *Kişisel Verileri Koruma Dergisi*, Cilt 1, Sayı 1, 2019, s.52.
[76] Elif Küzeci**,** *Kişisel Verilerin Korunması,* Ankara, Turhan Kitabevi, 3. Baskı, 2019, s.336.

dayalı bir yorumlama yerine, amaçların anlamının somut olayın koşullarına göre belirlenmesi gerektiği ifade ederek daha esnek bir değerlendirme yapılmasını öngörmüştür[77].

Esasa dayalı yaklaşımda, uygunluk değerlendirmesinde dikkate alınması gereken çeşitli ölçütler, Tüzük 'ün 6. Madde 4. Bendinde belirlenmiştir. Buna göre ilk olarak, verilerin toplama amacı ile sonraki işleme amacı arasındaki ilişkinin varlığı önemlidir. Ayrıca, kişisel verilerin toplandığı bağlam da göz önünde tutulmalıdır. Veri sorumlusu ile veri sahibi arasındaki ilişki, bu değerlendirmenin temel unsurlarındandır. Ayrıca verilerin niteliği de önemli bir faktör olarak karşımıza çıkmaktadır. Örneğin, özel kategorideki veriler veya suçlarla ilgili verilerin işlenip işlenmediği değerlendirilmelidir. Ek olarak, planlanan sonraki işleme işleminin, ilgili kişiler üzerinde yaratacağı potansiyel etkiler de dikkate alınmalıdır. Son olarak, verilerin işlenmesi sırasında ek güvenlik önlemlerinin alınmış olması, örneğin şifreleme ya da anonimleştirme gibi yöntemlerin uygulanıp uygulanmadığı da uygunluk değerlendirmesinde göz önünde bulundurulması gereken diğer bir faktör olarak yer alır. Ancak en önemli kriter, sonraki işlemenin ilk amaca uygun olup olmadığıdır. İlgili kişinin makul beklentileri doğrultusunda, sonraki işleme amacı ne kadar farklılık gösterirse, uygunluk testini geçmesi o kadar güçleşecektir. Buna ek olarak, veri sorumlusu ile ilgili kişi arasındaki ilişkinin doğası, aralarındaki güç dengesi ve diğer somut koşullar da bu değerlendirmeyi etkileyebilecektir. Eğer sonraki işleme amacı, ilgili kişi açısından beklenmedik ya da sürpriz bir sonuç doğuruyorsa, uygunluk testi başarılı olamayacaktır[78].

Bu ilkenin uygulamadaki yansımalarını ve veri işleme süreçlerinde dikkate alınması gereken hususları daha somut bir şekilde ele alabilmek adına, anonim şirketlere ilişkin örnekler üzerinden konuyu detaylandırmak yerinde olacaktır;

Anonim şirketlerin veri işleme faaliyetleri, başlangıçtaki veri işleme amacıyla uyumlu olduğu sürece hukuka uygun şekilde genişletilebilir. Örneğin, bir e-ticaret şirketi olan X Teknoloji A.Ş., müşterilerine daha iyi hizmet sunabilmek amacıyla sipariş geçmişlerini analiz ederek kişiselleştirilmiş ürün önerileri sunmaktadır. Şirket, veri işleme faaliyetlerini genişleterek müşterilerin alışveriş alışkanlıklarını analiz etmeyi, hangi ürünlerin daha çok tercih edildiğini ve hangi ürünlerin daha az ilgi gördüğünü belirlemeyi planlamaktadır. Bu analizlerden elde edilen verilerle ürün yelpazesini güncellemek, yeni ürünler geliştirmek ve rekabet gücünü artırmak hedeflenmektedir. Bu durumda, yeni amaç olan ürün yelpazesini güncelleme ile

[77] Yücedağ, *op. cit.,* s.54.
[78] *Ibid.,* s.54

başlangıçtaki kişiselleştirilmiş ürün önerileri sunma amacı arasında doğrudan bir bağlantı bulunduğu için, yeni amacın başlangıç amacıyla uyumlu olduğu kabul edilebilir. Bu örnek, veri sorumlularının amaç uyumluluğu ilkesine uygun hareket etmeleri durumunda, veri işleme faaliyetlerini nasıl genişletebileceğini göstermektedir. Bu örnekte, yeni amaç olan ürün yelpazesini yenileme ile başlangıç amacı olan kişiselleştirilmiş ürün önerileri arasında doğrudan bir bağlantı vardır. Bu nedenle, yeni amaç, başlangıç amacıyla uyumlu kabul edilebilir. Anonim şirketlerin veri işleme faaliyetlerinde amaç uyumluluğunun değerlendirilmesi, müşteri rızası ve beklentileri bakımından önemli bir kriterdir. Örneğin, bir X Banka A.Ş., başlangıçta müşterilerine kredi kartı kullanımıyla ilgili bilgilendirme yapmak amacıyla mesaj göndermektedir. Ancak banka, veri işleme amacını genişleterek müşterilerin kredi kartı kullanım alışkanlıklarını analiz etmeyi ve onlara özel kredi teklifleri ile kampanyalar sunmayı planlamaktadır. Bu durumda, yeni amaç ile başlangıç amacı arasında dolaylı bir bağlantı bulunsa da müşterilerin sadece bilgilendirme amacıyla veri paylaştığı varsayıldığında, yeni kullanım amaç uyumsuzluğu olarak değerlendirilebilir. Çünkü müşteriler, kredi teklifleri veya kampanyalar hakkında bilgilendirme almayı önceden öngörmemiş ya da açık rıza vermemiş olabilir. Bu örnek, veri işleme faaliyetlerinde amaç uyumluluğu ilkesinin yanı sıra müşteri rızasının önemini ve rıza alınmadan yapılan amaç değişikliklerinin hukuka aykırılık oluşturabileceğini de göstermektedir.

### E. Amaçla Bağlantılı, Sınırlı ve Ölçülü Olma İlkesi

Kanunun 4. Maddesi (ç) bendinde ele alınan bu ilke, birçok düzenleme tarafından da ele alınmış ve bu sebeple genel bir ilke haline gelmiştir. Kanunun dışında direktif ve tüzükte de maddenin tanımına yer verilmiştir. Kişisel verilerin işlenmesinde bu ilkenin amacı, işlenen verilerin daha sonra yeniden işlenecek verilerin, işleme amacıyla orantılı ve uyumlu ve elverişli olmasıdır. Bu ilke aynı zamanda anayasal olarak da dayanak bulmuş bir ilkedir. *Asgarilik ilkesi olarak da adlandırılan bu ilke, toplanan kişisel veri miktarının, verilerin toplanması ve daha sonra işlenmesi amaçlarını başarmak için zorunlu olan miktarla sınırlı kalınmasını ifade etmektedir*[79]. İşlendikleri amaçla bağlantılı, sınırlı ve ölçülü olma ilkesine göre, kişisel veri işleme faaliyetlerinin düzenlenmesinde temel bir yapı taşıdır. GVKT'de "veri minimizasyonu" olarak adlandırılmaktadır. Veri minimizasyonu, veri sorumlusunun yalnızca amacına ulaşabilmek için gerekli olan verileri toplamasını ve gereksiz verilerden kaçınmasını öngören bir ilkedir. Eğer veri işleme sürecinde veri sorumlusu amaçlarına ulaşmak için belirli kişisel

[79] Murat Akçakoca, *Tıp Ceza Hukukunda Kişisel Sağlık Verilerinin Korunması,* Adalet yayınevi, 1. Baskı, Ankara, 2022, s.193.

veriler ile yetinebiliyorsa, fazladan veri işlememesi gerekmektedir. Bu ilkeye göre, işlenen veriler yalnızca belirlenen amaçların gerçekleştirilmesine elverişli olmalıdır. Ayrıca, gelecekte ortaya çıkabilecek muhtemel veri ihtiyaçlarını karşılamak amacıyla veri işlenmesi yoluna gidilmemelidir. Bu işlem yeni bir veri işleme faaliyeti anlamına gelecektir. Yani yalnızca amacın yerine getirilmesi için gerekli veriler işlenmeli, amaçla ilgisi olmayan verilerin işlenmesinden kaçınılmalıdır. Veri işleme ile amaç arasında mantıklı bir denge olmalı; kişisel verilerin işlenmesi, yalnızca amaca ulaşmak için gerekli olacak ölçüde olmalıdır[80]. İşlenecek veriler, işlenme amacıyla doğrudan ilgili olmalı, amacın gerçekleştirilmesi için gerekli olan verilerle sınırlı tutulmalı ve fazladan bilgi toplanmamalıdır. Bu bağlamda, ilkenin anonim şirketler bakımından uygulanabilirliğini somutlaştırmak adına, konuya ilişkin örnekler sunulması uygun olacaktır:

Amaçla bağlantılı, sınırlı ve ölçülü olma ilkesi, kişisel verilerin yalnızca işleme amacına uygun, gerekli ve ölçülü şekilde işlenmesini gerektirir. Bu ilke kapsamında amaçla bağlantılılık yönünden, X Anonim Şirketi'nin çalışanlarının işe alım süreçlerinde iletişim kurabilmek amacıyla ad, soyad ve telefon numarası gibi kişisel verileri toplaması uygun kabul edilirken, bu süreçle doğrudan ilgili olmayan sağlık bilgilerini talep etmesi bağlantılılık ilkesine aykırılık teşkil eder. Sınırlılık ilkesine ilişkin bir örnek olarak, X Anonim Şirketi'nin çalışanlarının işe giriş ve çıkışlarını takip etmek amacıyla yalnızca mesai saatlerini kaydetmesi yeterli iken, çalışanlarının tüm mesai günü boyunca lokasyon takibi yapması bu ilkeye aykırılık oluşturacaktır. Ölçülülük ilkesine yönelik olarak ise, X anonim şirketinin müşteri sadakat programı avantajlarından yararlanmak isteyen müşterilerinden isim, soy isim, iletişim bilgileri ve ödeme için kart bilgileri gibi gerekli bilgileri talep etmesi ölçülü bir veri işleme faaliyeti olarak değerlendirilebilir. Ancak, müşterinin medeni durumu veya aile bireylerine ilişkin bilgi talep edilmesi, veri işleme faaliyetinin amacını aşan ve ölçüsüz bir uygulama olacaktır[81]. Bu örnekler, kişisel verilerin işlenmesinde amaçla bağlantılılık, sınırlılık ve ölçülülük ilkelerinin ne şekilde dikkate alınması gerektiğini somut bir şekilde ortaya koymaktadır. Özetle bu ilke, anonim şirketlerin veri işleme süreçlerinde gereksiz yükümlülüklerden kaçınmasını sağlarken, veri sahiplerinin de mahremiyetini koruma amacını taşır.

[80] Umniyahasghar Yosif, Kişisel Verilerin İşlenmesi Şartları ve 6698 Sayılı Kişisel Verilerin Korunması Kanununun Ruhu Olarak Genel İlkeler, *Selçuk Üniversitesi Adalet Meslek Yüksekokulu Dergisi,* Cilt 4, Sayı 1, 2021, s.1-22.

[81] Veri sorumlusunun, yalnızca amacını gerçekleştirmeye yetecek kadar kişisel veri toplaması gerekmektedir. Küzeci, *op. cit.* s. 208.

Kişisel Verileri Koruma Kurulunun 12/03/2020 tarihli ve 2020/212 sayılı kararı[82], ses kayıt özelliği bulunan güvenlik kameralarının kullanımına ilişkin önemli prensipler ortaya koymaktadır. Bu kararda, kişisel verilerin işlenmesinde veri minimizasyonu ilkesi kapsamında, yalnızca işin gerektirdiği ölçüde ve amaçla bağlantılı veri toplanması gerektiği vurgulanmıştır (KVKK m.4/2-a). Ayrıca, amaçla bağlılık ilkesi (KVKK m.4/2-c) gereği, elde edilen ses kayıtlarının sadece belirlenen güvenlik ve denetim amaçları doğrultusunda işlenmesi ve başka amaçlarla kullanılmaması zorunludur. Bununla birlikte, ses kayıtlarının kişinin özel hayatına dair hassas bilgiler barındırabilmesi nedeniyle, özel nitelikli kişisel verilerin korunması ilkesi (KVKK m.6) de dikkatle gözetilmelidir. Son olarak, ilgili kişilerin, ses kayıt özelliği bulunan kamera sistemlerinin varlığı ve kapsamı hakkında önceden bilgilendirilmesi gerektiği, açıklık ve bilgilendirme ilkesi (KVKK m.10) kapsamında da kararda belirtilmiştir. Böylelikle, Kurulun 2020/212 sayılı kararı, ses kayıt özellikli güvenlik kameralarının kullanımı hususunda hem hukuki sınırları hem de koruma gerekliliklerini net şekilde ortaya koymaktadır.

### F. Verilerin Belirli ve Sınırlı Süre Muhafaza Edilme İlkesi

Kişinin veriler işlemenin amacına uygun şekil ve makul sürede muhafaza edilmelidir. Burada toplanan ve işlenen verilerin ne kadar süre tutulacağı hakkında çeşitli problemler ortaya çıkmaması için verinin işleme amacına, niteliğine, verinin işleme elverişliliği açısından süre miktarına bakılarak uygun ve makul bir sürenin belirlenmesi gerekmektedir. Veri sorumlusu işleyeceği verinin niteliğine uygun şekilde bu ilkeyi gözeterek veriyi muhafaza etmeli, bu muhafaza için belirlenen süreler için mevzuata bakmalı ve sonrasında ihtiyaç kalmayan veri varsa veriyi silmeli/yok etmeli/anonim hale getirme zorunluluğu vardır[83]. Eğer kanuni düzenlemelerde bir süre belirtilmemiş ise, saklama süresi amaca uygun olarak makul ölçüde bir süre olmalıdır. Verilerin silinmesi/yok edilmesi/anonimleştirilmesi süreçlerinde uygun yöntem ve tekniğin belirlenmesi işleme amacına ve kanuni düzenlemelere göre belirlenmelidir. *Kişisel Verilerin İşlenme Şartlarına İlişkin Genel İlkeleri* ele alan KVKK madde 4'ün gerekçesinde; *"Kişisel verilerin, ancak ilgili mevzuatta öngörülen veya işlendikleri amaç için gerekli olan süre kadar muhafaza edilmesi zorunludur. Buna göre, veri sorumluları, ilgili mevzuatta*

[82] KVKK, 12.03.2020 tarih ve 2020/212 sayılı Kararı, https://www.kvkk.gov.tr/Icerik/6892/2020-212, (E.T.: 28.06.2025).

[83] Kişisel verilerin işlenme süresi, yalnızca verinin toplandığı amaçla sınırlı olmalı ve bu amacın ortadan kalkmasıyla birlikte veri silinmeli, yok edilmeli ya da anonim hale getirilmelidir. Kişisel Verileri Koruma Kurulu da 05/12/2018 tarihli ve 2018/142 sayılı kararında, kişisel verilerin ilgili mevzuatta öngörülen veya işlendikleri amaç için gerekli olan süre kadar muhafaza edilmesi gerektiğini, bu sürenin dolmasına rağmen silinmeyen verilerin hukuka aykırı biçimde tutulduğunu belirtmiştir. Bu ilkeye aykırılık, veri sorumlusunun sorumluluğunu doğurabilir.

*verilerin saklanması için öngörülen bir süre varsa bu süreye uyacak; yoksa verileri, ancak işlendikleri amaç için gerekli olan süre kadar muhafaza edebilecektir. Bir verinin daha fazla saklanması için geçerli bir sebep olmaması durumunda, o veri silinecek veya anonim hale getirilecektir. Gelecekte kullanma ihtimalinin varlığına dayanarak veri saklanamayacaktır. Veri sorumlusu, Kanunun 16'ncı maddesi uyarınca Sicile kayıt için başvuru yaparken kişisel verilerin işlendikleri amaç için gerekli olan azami süreyi bildirmek zorundadır[84]."* Şeklinde ifade edilen bu ilke amaçla sınırlılık ve veri minimizasyonu ilkelerinin bir uzantısıdır ve meşru bir sebep kalmadığında artık bu kişisel verilerin muhafazasına devam edilmesi, kişisel veri sahibinin özel hayatına müdahale oluşturabilir.

GDPR'da "saklama süresinin sınırlandırma ilkesi" olarak yer alan bu ilke, KVKK'da düzenlenen son ilke olarak karşımıza çıkar. Her iki ilke de yalnızca işleme amacının gerektirdiği ölçüdeki süre boyunca kişisel verilerin saklanması gerektiğini ve bu sürecin bitmesi ile kişisel verinin muhafaza edilmesinin sona ermesi gerektiğini ifade eder. KVKK'da ele alınan madde hükmünde kişisel verilerin saklanma sürelerine ilişkin düzenlemelerde öncelikle ilgili mevzuatın dikkate alınması gerektiği vurgulanırken, GDPR mevzuata açık bir şekilde atıf yapmamış bunun yerine saklama süresinin sınırlandırılma ilkesinin etrafında genel ifadelere yer vermiştir. Bunun yanısıra GDPR 89. Maddede yer alan bazı özel istisnai hükümlerinde KVKK'da doğrudan bir karşılığı bulunmamaktadır[85]. Veri saklama süresine dair bir sınırlandırılma hem kişinin temel hak ve özgürlüklerini koruyacak hem de gereksiz veri işlemeyi önleme amacını taşıyacaktır. Kısacası, "Verilerin Belirli ve Sınırlı Süre Muhafaza Edilme İlkesi", kişisel verilerin, işlendikleri amaç için gerekli olan süre kadar saklanmasını ve bu sürenin sona ermesiyle birlikte silinmesini, anonim hale getirilmesini veya imha edilmesini öngörür. Bu ilke, hem veri sorumlusunun yasal yükümlülüklerini yerine getirmesini hem de kişisel veri güvenliğinin sağlanmasını amaçlamaktadır. Bu ilkenin uygulanabilirliğini somutlaştırmak amacıyla, anonim şirketler özelinde bazı örnekler vermek yerinde olacaktır: İnternetten alışveriş imkanı sunan bir anonim e-ticaret şirketi, aldığı siparişlerde müşterilerden isim, soy isim, adres ve telefon gibi bilgileri talep eder. Ancak siparişin teslimi tamamlandıktan ve ilgili işlemler sona erdikten sonra bu verilerin saklanmaya devam edilmesi, ilgili ilkeye aykırılık teşkil edecektir. Benzer şekilde, sağlık hizmeti sunan bir anonim şirket, hastalara ait kişisel verileri yalnızca ilgili sağlık mevzuatında öngörülen süre boyunca muhafaza etmeli; bu

[84] ''KVKK İlk Hali Tam Gerekçesi'' https://kvkk.pro/kvkk-gerekcesi.html Erişim Tarihi: 14.12.2024
[85] Zeynep Ebrar KAYA, KVKK ve GDPR Arasında Kişisel Verilerin İşlenmesine İlişkin Genel İlkelerin Kıyası, *Hukuk ve Bilişim Dergisi,* sayı:10, https://www.hukukvebilisimdergisi.com/kvkk-ve-gdpr-arasinda-genel-ilkelerin-kiyasi/ (Erişim Tarihi: 14.12.2024).

sürenin sona ermesiyle birlikte söz konusu verileri silmeli, anonimleştirmeli veya imha etmelidir. X Bankası A.Ş ise müşterisinin kredi başvurusu kapsamında isim, soy isim, adres, telefon bilgisi, maaş bordrosu, adına kayıtlı menkul veya gayrimenkul bilgilerini talep edebilir. Bu veriler, yasal saklama süresi sona erdiğinde yine silinmeli, anonimleştirilmeli ya da imha edilmelidir[86]. Anonim şirketlerin "Belirli ve Sınırlı Süre Muhafaza Edilme İlkesi" ne uygun hareket etmeleri, yalnızca veri güvenliğini sağlamakla kalmaz; aynı zamanda yasal yükümlülüklerin yerine getirilmesini kolaylaştırır ve veri ihlali riskini azaltır. Bu bağlamda, şirketlerin düzenli veri envanteri kontrolleri yapmaları ve yalnızca işleme amacına uygun süre boyunca veri saklamaları büyük önem taşır. İlkeye uygun davranan şirketlerin, kamuoyu nezdinde güvenilirlik düzeyleri de artış gösterecektir.

### G. Hesap Verilebilirlik İlkesi (GDPR)

GDPR'ın son ilkesi olan hesap verilebilirlik ilkesi, kişisel verilere ilişkin veri sorumlularının tüm işlemleriyle ilgili olarak veri işleme faaliyetinde şeffaf, tutarlı ve sorumlu olmalarını gerektiren bir ilkedir[87]. Bu ilke, veri sorumlularının kanuni sorumlulukları neticesinde aldıkları tedbirleri belgeleme, denetleme ve gerektiğinde yetkili makamlara kanıtlama yükümlülüğünü ifade ederek diğer altı ilkeye uygunluk denetlemesini sağlar. Değişen ve gelişen çağ ile birlikte bilişim teknolojisinde ani ve hızlı değişimler, veri işleme yöntemlerini çeşitlendirmiş olması sebebiyle kişilerin verilerinin korunması konusunda yeni riskler ortaya çıkmıştır. Bu risklere karşı etkin bir çözüm olarak karşımıza hesap verilebilirlik ilkesi çıkmaktadır. Bu değişimler ile birlikte dünyada yapılan düzenlemeler, veri sorumlularının sorumluluklarını artırmıştır. Hesap verilebilirlik ilkesi, bu düzenlemelere uyum sağlamak için önemli bir araç olmakla birlikte bireylerin kişisel verileri üzerindeki haklarının korunmasını sağlar. Veri sorumluları, işledikleri verilere ilişkin olarak şeffaf, açık, anlaşılabilir ve güncel oldukları sürece bireyler, haklarını daha etkin bir şekilde kullanmış olurlar. Bu çerçevede, kişisel verilerin işlenmesinde bir diğer önemli ilke olan hesap verilebilirlik ilkesi hem uluslararası düzenlemelerde hem de dolaylı olarak Türk mevzuatında kendine yer bulmaktadır. OECD'nin Özel Yaşamın Gizliliğinin ve

[86] 5411 sayılı Bankacılık Kanunu m. 42'de; "Alınan yazılar ve faaliyetler ile ilgili belgelerin asılları veya bunun mümkün olmadığı hâllerde sıhhatlerinden şüpheye mahal vermeyecek kopyaları ve yazılan yazıların makine ile alınmış, tarih ve numara sırası verilerek düzenlenecek suretleri, usulleri çerçevesinde ilgili banka nezdinde on yıl süreyle saklanır. Bu belgelerin mikrofilm, mikrofiş şeklinde veya elektronik, manyetik veya benzeri ortamlarda saklanmaları mümkün" olabileceği düzenlemesine yer verilmiştir.

[87] Bu ilke, Madde 29 Çalışma Grubu'nun (Article 29 Data Protection Working Party) çalışmaları sonucunda şekillenmiş ve GDPR kapsamında düzenlenmiştir. Madde 29 Çalışma Grubu, '*Opinion 3/2010 on the principle of accountability'* (13 Temmuz 2010) https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2010/wp173_en.pdf, (Erişim Tarihi: 01.11.2024)

Sınır Arası Kişisel Veri Dolaşımının Korunmasına İlişkin Rehber İlkeleri, Avrupa Birliği Genel Veri Koruma Tüzüğü ve ISO/IEC 29100[88] standardı bu ilkeye açıkça yer vermektedir[89]. 6698 sayılı Kişisel Verilerin Korunması Kanunu ise, hesap verilebilirlik ilkesini doğrudan ifade etmese de kanunun genel ilkeleri ve Kişisel Verileri Koruma Kurumu'nun yorumları, bu ilkenin önemini vurgulamaktadır. Her ne kadar KVKK'da direk ele alınmasa da m.12/2'de "*Veri sorumlusu, kişisel verilerin kendi adına başka bir gerçek veya tüzel kişi tarafından işlenmesi hâlinde, birinci fıkrada belirtilen tedbirlerin alınması hususunda bu kişilerle birlikte müştereken sorumludur."* ve m.12/3'de *"Veri sorumlusu, kendi kurum veya kuruluşunda, bu Kanun hükümlerinin uygulanmasını sağlamak amacıyla gerekli denetimleri yapmak veya yaptırmak zorundadır*." şeklinde yer alan bu düzenlemeler hesap verilebilirlik ilkesinin bir yansıması olarak karşımıza çıkmaktadır. Ayrıca bu yükümlülüklerin Kabahatler başlıklı 18. Maddesi ile idari para cezasına ve yaptırımlara bağlanması da yine hesap verilebilirlik ilkesinin bir tezahürüdür.

GDPR kapsamında hesap verebilirlik ilkesi, veri sorumlularının (kontrolörlerin), kişisel veri işleme faaliyetlerinin hukuka uygunluğunu hem denetim makamlarına hem de veri sahiplerine kanıtlayabilmesini gerektiren bir yükümlülük olmakla birlikte, kontrolörlerin yalnızca yasal gereklilikleri yerine getirdiğini beyan etmesiyle yetinmez. Bununla birlikte veri koruma için hangi önlemleri aldığını ve bu süreçleri belgelendirerek şeffaf bir şekilde sunabilmesini gerektirir. GDPR'da hesap verebilirlik ilkesinin somut yansımaları çeşitli maddelerde görülmektedir. Örneğin, GDPR Madde 25'te yer alan "Tasarım ve Varsayılan Olarak Veri Koruması" düzenlemesi gereği, kontrolörlerin verilerin toplanması ve işlenmesinden önce hangi kişisel verilerin işleneceğini, nasıl işleneceğini ve bu süreçte hangi teknik ve idari önlemlerin uygulanacağını planlaması gerekmektedir. Bu düzenleme, kişisel veri işleme faaliyetlerinde proaktif bir yaklaşımı benimsetmektedir. Yine aynı şekilde, Madde 30'da düzenlenen "işleme faaliyetlerinin kayıtları", kontrolörlerin sorumluluğu altındaki veri işleme faaliyetlerini kayda geçirmesini ve bu kayıtların istendiğinde denetim makamlarına sunulabilmesini öngörmektedir. Bu, kontrolörlerin şeffaflık ve izlenebilirlik sağlaması açısından önemli bir adımdır. Yapılan faaliyetlerin belgelenmesi, hem mevzuata uygun veri işleme süreçlerinin gerçekleştirildiğini göstermek hem de olası idari denetim ve incelemelerde

[88] ISO/IEC 29100 uluslararası standart, bilişim sistemlerinde kişisel verilerin korunması ile ilgili olarak hesap verilebilirlik ilkesinin nasıl uygulanacağını detaylı bir şekilde sunmaktadır.
[89] "Hesap Verebilirlik İlkesi" OECD Rehberi m.14'te şu şekilde tanımlanmıştır: "*Bir veri sorumlusu, belirtilen ilkelere uyulması için öngörülen önlemlere uymaması halinde sorumluluk taşımalıdır.*"

kanıt sunabilmek için büyük öneme sahiptir. Hesap verebilirlik ilkesi, niteliği gereği süreklilik arz eder ve kontrolörlerin veri işleme süreçlerinde aktif bir sorumluluk taşımasını sağlar. Bu ilke, GDPR'ın temel yapı taşlarından biridir[90].

Hesap verebilirlik mekanizmalarının kurulması veri sorumlusunun hukuki sorumluluğunu tamamen ortadan kaldırmaz; çünkü hata yapma ihtimali her zaman vardır. Çalışma Grubu, mahremiyet etki analizi, veri koruma sorumlusu ataması ve bağlayıcı topluluk kurallarını hesap verebilirlik kapsamında önemli araçlar olarak görür. Bu mekanizmalar, verinin niteliği ve riskine göre uygulanmalı, şeffaflık sürecin başarısını sağlar. Hesap verebilirlik, veri koruma otoritelerinin yetkilerini daraltmaz; aksine denetimi güçlendirir ve yaptırımların etkin kullanılmasını sağlar. Ayrıca sertifikasyon gibi araçlar, uyumun kanıtlanmasında önemli rol oynar[91].

Hesap verilebilirlik ilkesi gereğince veri sorumluları KVKK'nın tüm hükümlerine uygun hareket etmek KVKK'ya uyumu sağlamak, kişisel verilerin işlenmesiyle ilgili olarak bireylere yeterli bilgi vermek ve şeffaf olmak ve de kişisel verilerin güvenliğini sağlamak için gerekli olan tüm teknik, kanuni ve idari tedbirleri almak zorundadırlar. Kişisel verilerin korunması ile ilgili herhangi bir iddia durumunda, veri sorumlusunun KVKK'ya uyum sağladıklarını ispat yükümlülükleri vardır[92].

Özetle, hesap verebilirlik ilkesi, veri koruma otoritelerinin yetkilerini kısıtlamaz; aksine denetimleri daha etkili ve verimli kılar. Bilgi asimetrisini azaltarak, denetimlerin önceliklendirilmesini ve kaynakların tasarruflu kullanılmasını sağlar. Türkiye'de doğrudan kanunda yer almamakla birlikte, kanunun ruhunda bulunur. Bu ilkenin yasal olarak tanımlanması ve şeffaflıkla desteklenmesi önemlidir. Böylece, veri koruma hukukunda yeni bir sorumluluk anlayışı oluşur ve kişisel veriler daha etkin korunur[93].

---

[90] Zeynep Ebrar KAYA, KVKK ve GDPR Arasında Kişisel Verilerin İşlenmesine İlişkin Genel İlkelerin Kıyası, *Hukuk ve Bilişim Dergisi,* sayı:10, https://www.hukukvebilisimdergisi.com/kvkk-ve-gdpr-arasinda-genel-ilkelerin-kiyasi/ (Erişim Tarihi: 14.12.2024).

[91] Mehmet Bedii Kaya, "Kişisel Verilerin Korunmasında Yeni Paradigma: Hesap Verebilirlik İlkesi," *İstanbul Hukuk Mecmuası*, Cilt 78, Sayı 4, 2020, s. 1859-1897, http://dergipark.gov.tr/iuhfm, (Erişim Tarihi: 24.05.2025).

[92] Hesap verilebilirlik ilkesi Bknz.*https://kvkkblog.com/hesap-verilebilirlik/#:~:text=Hesap%20verilebilirlik%20ilkesi%20uyarınca%2C%20veri,getirildiğini%20ispat%20edebilecek%20durumda%20olmalıdır*. Erişim tarihi: 29/10/2024.

[93] Kaya, *Kişisel Verilerin Korunmasında Yeni Paradigma*, op. cit., s.1895.

## IV. KİŞİSEL VERİLERİN İŞLENME ŞARTLARI

### A. TANIMI

*"Kişisel verilerin işlenmesi, verilerin toplanması, elde edilmesi, kaydedilmesi, organize edilmesi, değiştirilmesi, saklanması, okunması, kullanılması, başkalarına aktarılması, yayılması, silinmesi, yok edilmesi, gibi verilerle ilgili yapılan her türlü işlem anlamına gelmektedir[94]."*

KVKK Madde 3,1. Fıkra, e bendi kişisel verileri,

*"Kişisel verilerin işlenmesi: Kişisel verilerin tamamen veya kısmen otomatik olan ya da herhangi bir veri kayıt sisteminin parçası olmak kaydıyla otomatik olmayan yollarla elde edilmesi, kaydedilmesi, depolanması, muhafaza edilmesi, değiştirilmesi, yeniden düzenlenmesi, açıklanması, aktarılması, devralınması, elde edilebilir hâle getirilmesi, sınıflandırılması ya da kullanılmasının engellenmesi gibi veriler üzerinde gerçekleştirilen her türlü işlemi"* şeklinde ifade eder.

Yine 95/46/EC sayılı Veri Koruma Direktifi 2/b maddesine göre ve 2016/679 sayılı Genel Veri Koruma Tüzüğü 4/2 maddesine göre, "*işleme, otomatik ya da otomatik olmayan araçlarla, kişisel verilerin toplanması, kaydedilmesi, saklanması, organize edilmesi, uyarlanması ya da değiştirilmesi, kullanılması, başkalarına transfer edilmesi, yayılması, kombinasyonu veya ilişkilendirilmesi, bloke edilmesi, silinmesi, yok edilmesi gibi kişisel veriler üzerinde yapılan her türlü faaliyeti*" ifade eder[95].

Anonim şirketler açısından konuyu ele aldığımızda; şirket, faaliyetleri gereğince hangi sektörde olursa olsun müşterileri, çalışanları, tedarikçileri ve diğer paydaşları ile etkileşim halinde olmak durumundadırlar. Bu etkileşim sürecinde birçok kişisel veriye ulaşırlar ve bu verileri çeşitli amaçlarla işlemeleri gerekir. Anonim şirketler, müşterilerine ürün veya hizmet sunmak, siparişleri takip etmek, ödemeleri almak gibi işlemler için müşterilerin kişisel verilerini (ad, soyad, kargo ve fatura adresi, iletişim bilgileri gibi) işler, çalışan yönetimleri, işe alımı, performans değerlendirmeleri, ücret ödemeleri, sosyal güvenlik işlemleri gibi süreçlerde çalışanların kişisel verileri kullanılır. Tedarik zinciri yönetimi için yapılan anlaşmalar, ödeme

[94] Christopher Kuner, *European Data Protection Law,* s.98, k.n.2.87; Nilgün Başalp**,** *Kişisel Verilerin Korunması*, s.33; Elif Küzeci**,** *op.cit.,* s.201.; Canan, İmançlı, *op.cit.* s.85.
[95] 95/46/EC sayılı Direktif madde 4/2., Ayşe Aslı Alçın, *'Türk Hukukunda Kişisel Sağlık Verileri ve İdarenin Kişisel Sağlık Verilerini Koruma Yükümlülüğü'* s. 375.

işlemleri, ürün teslimatları gibi süreçlerde tedarikçilerin temsilcilerinin kişisel verileri işlenir. Pazarlama bakımından müşterilere özel teklifler sunmak, pazar araştırmaları yapmak gibi faaliyetlerde müşterilerin kişisel verileri kullanılır. Pazarlama stratejileri geliştirmek için web siteleri ve mobil uygulamalar üzerinden elde edilen kullanıcı verileri (IP adresi, çerez bilgileri, cihaz bilgileri gibi) analiz edilerek kullanıcı deneyimi iyileştirilir.

GDPR'in ise 6 ile 10. Maddeleri arasında yine kişisel verilerin işleme şartları düzenlenmiştir. KVKK'nın 4. Maddesi, kişisel verilerin işlenmesi genel ilkeleri, 5. Maddesinde özel nitelikli olmayan kişisel verilerin işlenme şartları düzenlenirken, madde 6'da ise özel nitelikli kişisel verilerin işlenme şartları düzenlenmiştir.

*"Kişisel verilerin işlenmesinde kural, veriyi işlemeyi hukuka uygun hale getirecek bir işleme şartı bulunmadıkça verinin işlenmemesidir. Kişisel verinin işlenmemesi kural, işlenmesi ise istisnadır*[96]*."*

"108 No'lu Kişisel Verilerin Otomatik İşleme Tabi Tutulması Karşısında Bireylerin Korunması Sözleşmesi'nin özel veri kategorileri başlıklı 6'ncı maddesine göre "*iç hukukta uygun güvenceler sağlanmadıkça bu türden veriler otomatik işleme tabi tutulamaz."* Hassas verilerin işlenmesi istisnai olduğu için işlenebileceği haller ayrıca ve açıkça mevzuatlarda belirtilmiş olup, 95/46/EC sayılı Veri Koruma Direktifi madde 8/2 ve 2016/679 sayılı Genel Veri Koruma Tüzüğü madde 9/2'de bu istisnai haller düzenlenmiştir[97]."

2016'da KVKK yürürlüğe girmeden önce de 1982 Anayasasının kişisel verilerin korunması hakkının düzenlendiği, özel hayatın gizliliği başlığını taşıyan 20'nci maddesinin 3'üncü fıkrasında kişisel verilerin işleme şartları düzenlenmiş ve koruma altına alınmış, hassas nitelikli olduğu için de özel hayatın gizliliği başlığı altında ele alınmıştır. Bu düzenlemeye göre, "*kişisel veriler ancak kanunda öngörülen hallerde veya kişinin açık rızasıyla*[98] *"* işlenebilir.

Kişisel Verilerin Korunması Kanunu'nda yapılan son değişikliklerle, Avrupa Birliği Genel Veri Koruma Tüzüğü ile uyum sağlanarak, özellikle özel nitelikli kişisel verilerin işlenmesi ve yurt dışına aktarılması süreçlerinde önemli iyileştirmeler yapılmıştır. Kanun, özel nitelikli verilerin işlenebileceği durumlar genişletilmiş ve kişisel verilerin yurt dışına aktarılması süreçlerinde de

[96] Dülger**,** *op. cit.,* s.28.
[97] Alçın, *op. cit.,* s. 376.
[98] R.G Tarihi: 09.11.1982, Sayı: 17863.

daha detaylı düzenlemeler yapılmış, veri aktarımlarının güvenli ve şeffaf bir şekilde gerçekleştirilmesi sağlanmıştır. Bu sayede, kişisel verilerin korunması hukuki çerçevesi güçlendirilmiş ve veri sahiplerinin hakları daha etkin bir şekilde korunmuştur. Yasa, veri sahibinin açık rızası şartını bazı durumlarda esneterek, kişisel verilerin işlenmesine ilişkin daha geniş bir çerçeve çizmektedir.

### B. AÇIK RIZA

Açık rıza, "Belirli bir konuya ilişkin, bilgilendirilmeye dayanan ve özgür iradeyle açıklanan rızayı" ifade eder. (KVKK m.3/1-a)[99] KVKK'daki yeni düzenlemeler, kişisel verilerin işlenmesi süreçlerindeki şartlara dair önemli yenilikler getirse de tanım değişmemiştir.

"Kanun'un gerekçesinde ise, rıza tanımına başka unsurlarında eklenerek açıklamasının yapıldığı görülmektedir. Gerekçeye göre; "Açık rıza, 95/46/EC sayılı Direktif dikkate alınarak tanımlanmaktadır. Buna göre, açık rıza ilgili kişinin kendisiyle ilgili veri işlenmesine, özgürce, konuyla ilgili yeterli bilgi sahibi olarak, tereddüde yer bırakmayacak açıklıkta ve sadece o işlemle sınırlı olarak verdiği onay beyanı şeklinde anlaşılmalıdır." Gerekçeden de açıklandığı üzere rıza tanımı mehaz düzenleme olan Direktif esas alınarak yapılmak istenmiş ancak kanun metnine alınırken Direktif'te olduğu gibi rıza tanımı olarak değil, açık rıza olarak düzenlenmiştir[100]."

Kanun koyucu, açık rızanın kabul edilmesi için 3 unsurun gerekli olduğunu kabul etmiştir. Bu unsurlar;

*i) Belirli bir konuya ilişkin olma,*

*ii) Bilgilendirmeye dayanma,*

iii) *Özgür iradeyle açıklanmış olma* unsurlarıdır.

Hukuka uygun olmayan bir veri işlemesinde açık rızanın varlığı, bu verilerin işlenebileceği anlamına gelmemekle birlikte, tanımdan da anlaşılacağı üzere açık rıza alınacak kişi konuyla ilgili detaylıca bilgilendirilmiş olmalı, kişide bunu tereddüte yer bırakmayacak şekilde özgür iradesiyle açıklamış olmalıdır. Temel ilkelere uygun olmadan alınmış açık rızanın da bu verilerin hukuka uygun olarak işlenebileceği anlamına gelmeyeceği unutulmamalıdır. Hukuka

[99] Dülger**,** *op. cit.* s.390.
[100] Müzeyyen Bayraktar, *Kişisel Sağlık Verilerinin İşlenmesi ve Korunması,* Marmara Üniversitesi Sosyal Bilimler Enstitüsü Yayımlanmamış Yüksek Lisans Tezi, 2022, s.56-57

aykırı bir işlemin yapılması durumunda, veri sahibinin daha önce vermiş olduğu açık rıza, bu işlemi meşru kılmaz[101].

Açık rızanın alınma şekli için mevzuatlarda herhangi bir şekil şartı belirtilmemiştir. Bu nedenle de açık rızanın alınması bakımından herhangi bir şekil şartı bulunmamaktadır[102], ancak bu susma veya pasif edilgen bir davranışla açık rızanın oluşacağı, işleme işleminin onaylandığı anlamına gelmemektedir[103]. Açık rızanın yazılı olarak alınması zorunlu değilse de ispat kolaylığı ve şeffaflık bakımından yazılı olması daha güvenilir olmaktadır. Elektronik ortamda, sözlü olarak veya bir eylemle de açık rıza alınabilir[104]. Açık rızanın verilmesi herhangi bir şekil şartına tabi olmadığı gibi, rızanın geri alınması da hakkın gereği olarak her zaman mümkündür[105]. Kişisel verileri düzenleyen mevzuatlarda rızanın geri alınması ile ilgili bir hüküm mevcut bulunmadığından, bu konuda genel hükümler bize yol gösterecektir. Bu bağlam da TMK m.24/2' deki hususlar işlemenin niteliğine uygun düştüğü ölçüde kullanılır. Kişi verisinin işlemesine ilişkin verdiği açık rıza beyanını geri almak istediğinde bunu veri sorumlusuna bildirir. Bu beyan veri sorumlusuna ulaştığı andan itibaren, hukuka aykırı işlem gerçekleştirmemek için; veri sorumlusunun, kişinin verisini işleme faaliyetini derhal durdurması gerekmektedir[106].

Ayrıca kişisel veri kişiye sıkı sıkıya bağlı bir hal olduğu için tam ehliyetliler ile sınırlı ehliyetliler, kişisel verilerinin işlenmesi için kimsenin izin veya icazetine ihtiyaç duymadan rıza gösterebilir, bu rızaları hukuka uygun kabul edilir. Fakat doktrinde tam ehliyetsizler ve sınırlı ehliyetsizler bakımından kişiye sıkı sıkıya bağlı bir hak mı olduğu, yoksa nisbi anlamda sıkı sıkıya bağlı bir hak mı olduğu tartışmalı bir husus olduğu için bu haklarını kullanabilmek için yasal temsilcilerini icazeti gerekir diyen görüşlerde mevcut bulunmaktadır.[107]

---

[101] Dülger, *op. cit.*, s.391.
[102]KVKK, Açık Rıza, https://www.kvkk.gov.tr/SharedFolderServer/CMSFiles/e3c6aa10-9de4-46f8-9b51-71bcf07c09b5.pdf, s.3.
[103] Rızanın varlığından bahsedilmek için en azından bir işaretin gerekli olduğuna dair bknz. Cihan Avcı Braun, Kişisel Verilerin İşlenmesinde Rıza, *Yeditepe Üniversitesi Hukuk Fakültesi Dergisi*, 2018, C. 15, S.1, s.20. https://www.acarindex.com/pdfs/854766, (E.T.: 30.05.2025).
[104] KVKK, Açık Rıza, *op. cit., s.3.*
[105] Data Protection. WP, Consent. S.25; Elif Erdoğmuş, *6698 Sayılı Kişisel Verilerin Korunması Kanunu Kapsamında Açık Rıza,* Ankara, Seçkin Yayıncılık, 1. Baskı, 2022, s.77-79.
[106]Kişisel Verileri Koruma Kurulu'nun 12.01.2021 tarihli Kamuoyu Duyurusu, https://www.kvkk.gov.tr/Icerik/6856/WHATSAPP-UYGULAMASI-HAKKINDA-KAMUOYU-DUYURUSU, (E.T.: 30.05.2025).
[107] Sefer Oğuz, *Kişisel Verilerin Korunması Hukukunun Genel İlkeleri,* Bilgi Ekonomisi ve Yönetimi Dergisi, 2018, 13:2 (121-138), s.129. https://dergipark.org.tr/tr/pub/beyder/issue/41709/425303#article_cite.

Açık rızanın geçerli olabilmesi için kişisel verilerin işlenmesinde genel ve kapsamlı bir rıza değil, belirli bir konuya ilişkin, net ve herkesçe anlaşılır bir rıza alınması gerekmektedir. Bir kişi bir konuya ilişkin açık rıza verirken, bu açık rıza metninde onaylayacağı hususlar için hangi verilerin işleneceği veri sorumluları tarafından somut ve net bilgi olarak sunulmalıdır[108]. Genel nitelikte, belirli bir konu içermeyen rızalar "battaniye rıza" olarak adlandırılır ve kanunun ilgili maddesinde öngördüğü spesifik konuya dair rıza verme şartını karşılamazlar. Özetle bu rızalar hukuken geçerliliğe sahip değildir. Battaniye rıza, kişisel verilerin işlenmesinde kullanılan genel ve kapsamlı rızalardır[109]. Verilerinin her türlü işlenmesine önceden onay vermiş gibi görünen kişinin verdiği bu rıza geçersizdir. Çünkü şahsın hangi verisinin, hangi amaçla işleneceği konusunda yeterli bilgiye sahip olmadan, belirlilik ilkesine aykırı olarak verilmiş rızalardır. O yüzden kanun bu tür rızaları geçersiz saymaktadır. Sonuç olarak, açık rızanın somut ve belirli bir çerçevede verilmiş olmasına bağlı olarak bir açık rızanın hukuki geçerliliği belirlenir. Açık rıza, kişisel verilerin korunmasında temel bir kavram olmakla birlikte belirlilik ilkesi ise kanun maddesinde açık rızanın geçerli olabilmesi için mutlaka yerine getirilmesi gereken önemli bir şarttır. Anonim şirketlerin, kişisel verileri işlerken belirlilik ilkesine uygun olarak hareket etmeleri ve kişilerden açık, özgür ve bilgilendirilmiş rıza almaları gerekmektedir. Aksi takdirde, KVKK kapsamında yaptırımlarla karşı karşıya kalabilirler[110].

Konuya ilgili bilgi sahibi olmayan bir kişinin açık rızasından söz edilemeyeceği kanunda düzenlenmiştir. Kişinin neye rıza gösterdiğini, verilerin hangi konuya ve ne için işleneceğine dair bilgilendirilmesi, rızasının geri alınıp alınamayacağı hususlarını bilmesi gerekmektedir.

Kişisel verilerin işlenmesinde ilgili kişilerin açık rızasının geçerliliği, yalnızca şekli değil aynı zamanda maddi kriterlerin de sağlanmasına bağlıdır. Kişisel Verileri Koruma Kurulu'nun 10.06.2025 tarihli ve 2025/1072 sayılı İlke Kararı'nda da vurgulandığı üzere, ticari hizmetlerin sunumu sırasında SMS ile doğrulama kodu gönderilerek alınan onaylar, çoğu zaman hem aydınlatma yükümlülüğünün yerine getirilmediği hem de açık rızanın aldatıcı yöntemlerle temin edildiği bir süreç haline gelmektedir. Kurul, bu kararıyla anonim şirketler dahil olmak üzere veri sorumlularının, ürün ve hizmet sunumu sırasında gerçekleştirdikleri SMS doğrulama uygulamalarında açık rızaya dayalı veri işlemeyi gizleyemeceğini açıkça ortaya koymuştur. Tek bir işlem üzerinden hem hizmet onayı hem de ticari ileti izninin alınması gibi uygulamalar, ilgili

[108] A. Çiğdem Ayözger Öngün**,** *op. cit*, s.126-127.
[109] Serdar Çelikel, "Kişisel Verilerin İşlenmesinde, Açık Rıza Hukuka Uygunluk Nedeninin, 95/46 Sayılı Direktif ve GDPR' la Karşılaştırmalı Olarak İncelenmesi", *Uyuşmazlık Mahkemesi Dergisi*, Yıl 9, Sayı 17, Haziran 2021, s. 161-190.
[110] Bknz. KVKK, 31.05.2019 tarihli 2019/162 sayılı kurul kararı, https://www.kvkk.gov.tr/Icerik/5495/2019-162, (E.T.: 30.05.2025).

kişinin rızasını sakatlayan ve açık rızanın özgür iradeye dayanma unsurunu ortadan kaldıran bir yaklaşım olarak değerlendirilmiştir. Bu çerçevede Kurul, veri sorumlularının açık rızaya ilişkin taleplerini doğrulama kodundan bağımsız şekilde ve aydınlatma yükümlülüğüyle uyumlu biçimde yürütmeleri gerektiğini belirtmiştir. Karar, açık rızanın "bilgilendirmeye dayalı, özgür iradeye bağlı ve belirli bir işlem için verilmiş" olma şartlarını sağlamayan her uygulamanın veri işleme bakımından hukuka aykırılık teşkil edeceğini hatırlatmaktadır[111]. Bu doğrultuda, anonim şirketlerin özellikle dijital platformlar üzerinden hizmet sunarken, kişisel verilerin işlenmesine yönelik rıza süreçlerini ayrı, şeffaf ve açık şekilde yürütmeleri gerekmektedir.

## C. AÇIK RIZAYI ARANMAKSIZIN KİŞİSEL VERİLERİN İŞLENEBİLECEĞİ HALLER

KVKK madde 5'te kişisel verilerin açık rıza olmaksızın işlenemeyeceği belirtilirken, kanunun 5'inci maddesinin 2'nci fıkrasında da açık rıza aranmaksızın kişisel verileri işlemenin şartları hüküm altına alınmıştır. Sınırlı sayıda, tahdidi olarak düzenlenen bu hususları genişletmek mümkün değildir.

Maddeye göre;

*"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.*

[111]KVKK, 10/06/2025 Tarihli ve 2025/1072 sayılı İlke Kararı, https://www.kvkk.gov.tr/Icerik/8339/Urun-ve-Hizmet-Sunumu-Sirasinda-Ilgili-Kisilere-SMS-ile-Dogrulama-Kodu-Gonderilmesi-Suretiyle-Kisisel-Verilerin-Islenmesi-Hakkinda-Kisisel-Verileri-Koruma-Kurulunun-10-06-2025-Tarihli-ve-2025-1072-sayili-Ilke-Karari, (E.T.: 27.06.2025).

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

Şartlarından birinin varlığı hâlinde, ilgili kişinin açık rızası aranmaksızın kişisel verilerinin işlenmesi mümkün sayılmıştır.

a. **Kanunlarda Açıkça Öngörülmesi**

İşlenecek veriye dair açık rıza aranmayacağına dair kanunlarda özel bir düzenleme varsa, açık rıza gerekmeksizin kişinin verisi işlenebilir[112]. 6698 sayılı Kişisel Verileri Koruma Kanunu'nun gerekçesinde de bu tür durumlara örnekler verilmiştir[113]. Bu düzenlemelere örnek olarak; 2559 s. Polis Vazife ve Salahiyetleri Kanunu'nun 5. maddesindeki şüpheliden parmak izi alınması, Vergi Usul Kanununda yer alan Vergi borçlarının tahsil edilmesi, vergi incelemelerinin yapılması gibi işlemler için vergi mükelleflerinin kişisel verilerinin vergi idaresi tarafından işlenmesi, Ticaret Sicili yönetmeliğinde yer alan ticaret şirketlerine ilişkin bilgilerin ticaret sicilinde kayıtlı tutulup, bu verilerin de kamuya açık olması, 5411 sayılı Bankacılık Kanunu'nda ki bankaların müşterilere ait kişisel verileri, bankacılık işlemlerinin yürütülmesi ve risk değerlendirmesi yapılması gibi amaçlarla işleyebilmeleri, 3359 sayılı Sağlık Hizmetleri Temel Kanunu'nda sağlık hizmetlerinin sunulması sırasında hasta kayıtlarının tutulması, sağlık hizmetlerinin finansman edilmesi vb. gibi konularda kişisel verilerin işlenebileceği, 4857 sayılı İş Kanunu 75. Maddesine göre işverenlerin, iş sözleşmesinin kurulması ve ifası sırasında işçilerin kişisel verilerini işleyebilmeleri, 1136 sayılı Avukatlık Kanunu'nun 46. Maddesindeki avukatların icra takip dosyalarındaki kişisel verilere vekalet sunmaya gerek kalmadan erişim sağlayabilmeleri ilgili kanunlarda düzenlenmiştir. Belirsizlik durumları bu kapsama girmeyeceği için kanunun kesin ve açık bir şekilde bu yetkiyi verdiği hallerde açık rıza aranmadan veri işleme faaliyeti hukuken geçerlidir. "Kanunda açıkça öngörülmesi'' şartı, kişisel verilerin korunması ile diğer kamu yararlarının dengede tutulması amacıyla getirilmiş bir istisna olduğu bu örneklerden de açıkça görülmektedir. Yani, yasa koyucu, belirli alanlarda kişisel verilerin işlenmesinin kamu yararı veya başka önemli bir meşru gerekçe nedeniyle zorunlu olduğunu yorumlamış ve bu tür durumları da ilgili kanunlarda açıkça düzenlemiştir.

Kanunlarda açıkça öngörülmesi nedeniyle açık rıza aranmaksızın kişisel veri işlenebilecek durumlar anonim şirketler bakımından ele alındığında, genellikle şirketlerin hukuki

[112] KVKK, "Kanunlarda Öngörülme Kişisel Veri İşleme Şartına İlişkin Bilgi Notu", *KVKK Yayınları no:62*, Mart 2025, Ankara, s.10.
[113] Mehmet Bedi Kaya, Furkan Güven Taştan, *Kişisel Veri Koruma Hukuku*, Çevrimiçi Sürüm 3.0 Ocak 2025, s.25. https://mbkaya.com/hukuk/veri-koruma-hukuku.pdf, (Erişim Tarihi:13.01.2025).

yükümlülüklerini yerine getirmesi veya kamu yararına hizmet eden faaliyetlerle sınırlıdır. Bu durumlarda anonim şirketler, ilgili mevzuatın izin verdiği çerçevede kişisel veri işleyebilir. Bu ilkenin anonim şirketler bakımından uygulamasını somutlaştırmak adına, konuya ilişkin örnekler sunulması yerinde olacaktır;

Anonim şirketler, Türk Ticaret Kanunu gereği, pay sahipleriyle ilgili ad, soyad, iletişim bilgileri, hisseleri oranı gibi verileri kayıt altına almak ve bu bilgileri pay defterinde tutmak ile yükümlüdür[114]. Genel kurulda, pay sahiplerinin kimlik ve iletişim bilgilerinin paylaşılması ve bu bilgilerin toplantı tutanaklarında yer alması gibi veri işleme faaliyetleri, kanunda açıkça öngörüldüğü için açık rıza alınmasını gerektirmeyecektir.

Vergi Usul Kanunu ve diğer mali yükümlülükler gereğince anonim şirketlerin çalışanlarının, müşterilerinin veya tedarikçilerinin kişisel verilerini muhasebe kayıtlarında işleyip Vergi Dairesi'ne ya da diğer ilgili kurumlara bildirmesi gereklidir. Bu durum, açık rıza gerektirmeksizin yapılabilir. Şirket çalışanların maaş bilgilerini SGK'ya bildirmesi veya fatura düzenlenirken müşteri bilgilerini muhasebe sisteminde kayıt altına alması gibi veri işleme faaliyetleri, kanunda açıkça öngörüldüğü için açık rıza alınmasını gerektirmeyecektir.

6331 sayılı İş Sağlığı ve Güvenliği Kanunu kapsamında, anonim şirketlerin çalışanları için iş sağlığı ve güvenliğine yönelik gerekli önlemleri alması ve bu doğrultuda sağlık kontrolleri veya risk analizleri yapması zorunludur. Şirketin, çalışanlarının düzenli sağlık raporlarını iş güvenliği uzmanına sunması ve raporları saklaması gibi işlenen veriler, ilgili kanun gereği rıza aranmaksızın işlenebilir.

Anonim şirketler, çeşitli düzenleyici ve denetleyici kurumlara bilgi verme yükümlülüğüne sahiptir. Sermaye Piyasası Kurulu (SPK) veya Mali Suçları Araştırma Kurulu (MASAK) tarafından bir bilgi veya belge talep edildiği takdirde kişisel veriler açık rıza aranmaksızın işlenebilir. Örneğin, MASAK tarafından talep edilen bir işlemde, müşterilerin kimlik bilgilerinin paylaşılması gibi.

Anonim şirketler, HMK ve diğer ilgili mevzuattaki düzenleme gereğince, hukuki bir ihtilaf durumunda mahkemelerden ya da icra müdürlüklerinden gelen talep üzerine istenen kişisel verileri açık rıza aramaksızın paylaşabilecektir. Örneğin, alacak tahsili için, borçlunun kimlik bilgilerinin ve borcuna ilişkin bilgilerin mahkemeye sunulması gibi.

[114] Yavuz Akbulak, "TTK Işığında Anonim Şirketlerde Pay Senetleri", *Ankara Barosu Dergisi*, Sayı:1, Ocak 2016, s.521. https://dergipark.org.tr/tr/download/article-file/398510 (E.T: 13.01.2025)

**b. Fiili İmkansızlık**

KVKK'nın m.5/2-b bendinde düzenlenen bu hükümde yasa koyucu iki şart aramıştır:

*"1) Fiili imkânsızlık nedeniyle rızasını açıklayamayacak durumda bulunması veya rızasına hukuki geçerlilik tanınmaması,*

*2) Kişinin kendisinin ya da bir başkasının hayatı veya beden bütünlüğünün korunması için zorunlu olması."*

Kanun koyucu madde hükmüyle konuya netlik ve ayrıntı kazandırmış, tıbbi müdahaleler, acil durumlar veya doğal afet gibi hayati tehlike arz eden durumlar ile örneklendirerek konuya akıcılık kazandırmış ve bendin kapsamı somutlaştırmıştır. Kısacası, KVKK m.5/2-b bendi, kişisel verilerin korunması ile insan hayatı arasındaki dengeyi gözetmekte ve aralarında uzlaşma sağlamayı amaçlamaktadır.

İlgili maddenin gerekçesinde *"rızanın açıklanamadığı ya da geçerli olmadığı hallerde, kişilerin hayat veya beden bütünlüğünün korunması için kişisel verilerin işlenmesi öngörülmektedir. Örneğin kişinin şuurunun yerinde olmadığı veya akıl hastası olması sebebiyle rızasının geçerli olmadığı bir durumda, hayat veya beden bütünlüğünün korunması amacıyla, tıbbi müdahale yapılması sırasında, kişisel verileri işlenebilecektir. Bu bağlamda kan grubu, geçirilen hastalıklar ve ameliyatlar, kullanılan ilaçlar gibi veriler, ilgili sağlık sistemi üzerinden işlenebilecektir. Yine hürriyeti tahdit edilen bir kişinin kurtarılması amacıyla, kendisinin veya şüphelinin taşımakta olduğu telefon, bilgisayar, kredi kartı, banka kartı veya diğer teknik bir araç üzerinden yerinin belirlenmesi için bu veriler işlenebilecektir."* İfadeleri yer almaktadır.

Anonim şirketler açısından fiili imkânsızlık durumlarında açık rıza aranmaksızın kişisel verilerin işlenmesi çoğu zaman acil müdahale gerektiren beklenmedik olaylar ve kriz durumlarında ortaya çıkmaktadır. Bu duruma örnek olarak bir anonim şirketin, çalışanlarının sağlığı ve güvenliğini gözeterek acil bir durumda çalışanının alerji bilgisini, kullandığı ilaçları veya başkaca sağlık bilgileri gibi kişisel verilerini ilgili sağlık personeli ile paylaşması verilebilir. Bu tür durumlarda anonim şirketlerin, çalışanlarının, müşterilerinin veya üçüncü kişilerin hayatını, sağlıklarını veya beden bütünlüklerini koruma amacıyla veri işlemesi hukuka uygun hale gelmektedir.

Bu kapsamda bir uygulama örneği olarak, bir otel zinciri işleten anonim şirketin tesisinde konaklayan bir müşterinin, otel odasında bilincini kaybetmiş bir halde bulunması durumu ele alınabilir. Otel görevlilerinin durumu fark etmesinin ardından sağlık ekiplerine haber

verilmekte ve müşteriye ait kimlik bilgileri ile sistemde daha önceden kayıtlı olan sağlık bildirimleri (kalp rahatsızlığı gibi) ilgili sağlık personeliyle paylaşılmaktadır. Bu durumda, kişisel verilerin (kimlik ve sağlık bilgileri) açık rıza olmaksızın işlenmesi ve paylaşılması, KVKK m.5/2-b uyarınca hukuka uygun kabul edilir. Çünkü ilgili kişi fiili imkânsızlık nedeniyle rızasını açıklayamayacak durumdadır (bilinci kapalıdır) bu nedenle veri işleme faaliyeti, kişinin hayatının veya beden bütünlüğünün korunması amacıyla zorunludur. Dolayısıyla bu örnek olayda, veri sorumlusu sıfatıyla hareket eden anonim şirketin veri işleme faaliyeti, KVKK'nın 5. maddesinin ikinci fıkrasının (b) bendi kapsamında hukuka uygunluk sebebine dayanmakta olup, açık rıza aranmaksızın gerçekleştirilebilecek niteliktedir. Bu kapsamda dikkat edilmesi gereken husus, verilerin yalnızca hayati tehlikeyi bertaraf etmeye yönelik olarak ve ölçülülük ilkesine uygun bir şekilde işlenmesidir. Bu durum hem KVKK'nın genel ilkeleri hem de ilgili maddenin istisna niteliği gözetilerek değerlendirilmelidir.

Bir diğer örnek olarak anonim şirkete bağlı bir fabrikada yangın çıktığında veya deprem, sel gibi bir doğal afet durumunda, acil tahliye planının uygulanabilmesi ve kurtarma ihtiyaçlarını karşılamak sebebiyle fabrika çalışanlarının konum bilgileri veya listeleri kurtarma ekipleriyle paylaşılması durumu verilebilir.

Fiili imkânsızlık durumları, sadece acil ve hayati durumlar için geçerli olup, anonim şirketlerin veri işleme faaliyetlerinde istisna niteliğindedir. Şirketlerin veri işleme faaliyetleri, yalnızca amaca uygun ve ölçülü şekilde yapılmalı, veri işleme ilkelerine uygun olmalı, acil durum sona erdiğinde de işlenen veriler mevzuata uygun şekilde saklanmalı veya imha edilmelidir.

**c. Sözleşmenin Kurulması veya İfası İçin Gerekli Olması**

6698 sayılı Kanun'un m.5/2 c bendinde düzenlenen hükme göre, bir sözleşmenin kurulması veya ifası için gerekli olması hallerinde açık rıza gerekmeksizin kişisel veri işleme çalışmaları yapılması söz konusudur. Örneğin Trendyol, Hepsiburada gibi e-ticaret sitelerinde satış yapan bir anonim şirket, aldığı bir sipariş üzerine müşterisine bu siparişi ulaştırabilmek için isim, soy isim, adres ve iletişim bilgilerini istemek durumundadır. Sipariş oluşturulup ödemenin gerçekleşmesi ile birlikte artık sözleşme kurulmuş olur ve artık bu şirket ilgili madde gereğince açık rızaya gerek kalmaksızın kişinin bu verilerini işleyebilir ve adrese gönderilmesi üzerine kargo şirketine kişinin verilerini aktarabilir. Fakat bu şirketin ilgili kişiye başka ürünlerini pazarlama amacıyla reklam faaliyetleri sunması bu satış sözleşmesinin kurulması veya ifası için gerekli olma şartını taşımadığı nedeniyle kanuna aykırılık oluşturacaktır. Ayrıca hukuk

kurallarına uygun olmayan bir sözleşmenin veri işleme şartının hukuka uygun olması beklenemez, çünkü geçersiz bir sözleşme söz konusudur[115].

Kişisel Verileri Koruma Kurulu tarafından 06.07.2021 tarihli 2021/664 sayılı verilen karar sonucunda, müşterilerin ödeme işlemleri esnasında banka aracılığıyla veri sorumlusuna bazı bilgilerin aktarıldığı, aktarılan verilerin otomatik ödeme talimatıyla bankalardan veri sorumlusuna aktarılan bilgiler olduğu, veri sorumlusu bankanın bunları sitemine işlemek ve sözleşme kapsamındaki işleri gerçekleştirebilmek için zorunlu olduğu belirtilmiştir. Veri sorumlusu bankanın bu verileri eksik işlemesi durumunda şirketin meşru menfaatlerine zarar verebileceği ve kurul incelemesinde otomatik ödeme talimatıyla fatura ödeyen abonelerin faturasında banka adının yer almasının ilgili kişi açısından herhangi bir hak ihlali oluşturmadığını ve ilgili kişinin talebi doğrultusunda gerçekleştirildiği ortaya koymuştur. Bu doğrultuda Kurul, veri sorumlusunun bu verileri işlemesinde herhangi bir hukuka aykırılık unsurunun bulunmadığını tespit etmiş, özetle veri işleme sürecini meşru menfaatlere ve sözleşmenin ifası için zorunlu olmasına bağlayarak veri sorumlusunun uygun sınırlar içerisinde hareket ettiğini ve herhangi bir işlem yapılmasına gerek olmadığına karar verilmiştir[116].

Yine Genel Veri Koruma Tüzüğü'nün *İşlemenin Yasallığı* başlıklı 6. Maddesi, kişisel verilerin işlenme sürecindeki meşru dayanakları belirlemiştir. İlgili maddenin (b) bendine göre; *veri sahibinin taraf olduğu bir sözleşmenin ifası için veya sözleşme yapılmadan önce veri sahibinin talebi üzerine gerekli adımların atılması için işlemenin gerekli olması;* halinde işlemenin yasal olacağı belirtilerek kişisel verilerin işlenmesine izin verilir. Veri işleme süreci verisi işlenen kişiyle yapılan bir sözleşmesel yükümlülük gereği (örneğin, bir hizmet sağlayıcısıyla yapılan sözleşme veya bir X bankası AŞ'nin müşteriye hesap açabilmek için müşterisinin kimlik bilgilerini işlemesi gibi) doğrudan lüzumlu olmalıdır. Kişisel Verilerin Korunması Kanunun gerekçesi de bu hali destekler niteliktedir. "*Fıkranın (c) bendine göre, bir sözleşmenin kurulması veya ifasıyla ilgili olarak kişisel veri işlenebilecektir. Örneğin, yapılan bir sözleşme gereği paranın ödenmesi için alacaklı tarafın hesap numarası alınabilecektir. Yine bir bankayla kredi sözleşmesi yapılması sırasında bankanın, o kişiye ait maaş bordrosunu, tapu kayıtlarını, icra borcu olmadığına dair belgeyi edinmesi bu kapsamda değerlendirilecektir.*"

[115] Öztürk, Çalışkan, Seyhan, *op. cit.* s. 90.
[116] Kişisel Verileri Koruma Kurumu "*İlgili kişinin, doğal haz dağıtımı yapan bir şirket tarafından düzenlenen faturasında kişisel verisi niteliğindeki banka bilgisine yer* verilmesi" kararı https://www.kvkkarar.com/?_sf_s=Sözleşmenin%20Kurulması%20veya%20İfası%20İçin%20Gerekli%20Olması&_sft_kanun_maddesi=kvkk-madde-05%20c-bendi-fikra-2-kvkk-madde-5-2-kvkk-madde-5

### d. Kişisel Verilerin İşlenmesinin Veri Sorumlusunun Hukuki Yükümlülüğünü Yerine Getirebilmesi İçin Zorunlu Olması

Anayasa'nın 20. maddesi ile güvence altına alınan ve temel bir hak olarak belirlenen kişisel verilerin korunması, özel hayatın gizliliği ilkesi ile yakından ilişkilidir. Bu nedenle, bireylerin açık rızası olmaksızın kişisel verilerinin işlenebilmesi için, Anayasa'nın 13. maddesi gereği kanunla düzenlenmelidir. Madde 4/(ç) bendinde düzenlenen bu hale göre, veri sorumlusu hukuki yükümlüğünün yerine getirebilmek için lüzumlu hallerde kişisel verileri işleyebilecektir. Kişisel Verilerin Korunması Kanunun gerekçesine göre, "*veri sorumlusu, hukuki yükümlülüğünü yerine getirebilmesi için zorunlu olan verileri, ilgili kişinin rızası olmasa dahi işleyebilecektir. Örneğin bir şirketin çalışanına maaş ödeyebilmesi için, banka hesap numarası, evli olup olmadığa bakmakla yükümlü olduğu kişiler, eşinin çalışıp çalışmadığı, sosyal sigorta numarası gibi verileri işlemesi bu bendin verdiği yetkiye istinaden olacaktır."*

Genel Veri Koruma Tüzüğü'nün *İşlemenin Yasallığı* başlıklı 6. maddenin 1. Fıkrasının (c) bendine göre; "*işlemenin, denetleyicinin tabi olduğu yasal bir yükümlülüğe uyulması için gerekli olması durumunda ve ölçüde işleme yasal olacaktır."* GDPR c bendine özel başka düzenlemeleri de beraberinde getirmiştir. Yine aynı maddenin 2. Fıkrası "*Üye Devletler, paragraf 1'in (c) ve (e) noktalarına uyum sağlamak için, işleme ilişkin bu Yönetmelik kurallarının uygulanmasını uyarlamak amacıyla, işleme için daha kesin özel şartlar belirleyerek ve IX. Bölümde belirtilen diğer özel işleme durumları da dahil olmak üzere yasal ve adil işlemeyi sağlamak için diğer tedbirleri alarak daha özel hükümleri koruyabilir veya getirebilir*." Şeklindeki düzenlemesi ile, üye devletlerin GDPR çerçevesinde ek düzenlemeler (ulusal esneklik, spesifik amaçlar gibi konularda) yapabileceğini ifade eder. Ve 3. Fıkrası "*1 inci fıkranın (c) ve (e) bentlerinde sözü edilen işlemenin dayanağı aşağıdaki şekilde belirlenir:*

*Birlik hukuku; veya*

*Denetleyicinin tabi olduğu Üye Devlet hukuku."* düzenlemesi ile veri işleme dayanağının yasal bir yükümlülüğe veya resmi bir yetkiye dayanması hallerini açıklamaktadır.

Özetle; Madde 6(2) ve 6(3), GDPR'in temel prensiplerini korurken üye devletlere kendi yasal düzenlemelerini GDPR'in şeffaflık, veri minimizasyonu ve amaç sınırlaması gibi ilkeleriyle uyumlu olma şartıyla oluşturma imkanı tanır.

Kişisel verileri işlemesi gereken bir anonim şirket, kanunda belirtilen haller dışında bireylerin açık rızalarını almadan veriyi işleyemezler. Ancak, kanunlarda belirtilen zorunlu hallerde, anonim şirketin veri sorumluları açık rıza şartına bağlı kalmaksızın veri işleme faaliyetlerini gerçekleştirebilirler. Örneğin bir anonim şirketin alacakların tahsili için icra takipleri başlatıldığında, borçlunun kişisel verilerinin işlenmesi zorunlu hale gelecektir. Yine bir anonim şirket çalışanlarının özlük dosyalarını tutarken kişisel verilerini işlemek zorunda ve bir çalışanının sigorta primlerini yatırabilmek için Sosyal Güvenlik Kurumuna bildirmesi gereken, personelin T.C. kimlik numarasını ve maaş bordro bilgisini işlemek durumundadır.

**e. İlgili Kişi Tarafından Verinin Alenileştirilmiş Olması**

"İlgili kişi tarafından verinin alenileştirilmiş olması" KVKK'nın 5. Maddesi 2. Fıkra d bendinde düzenlenmiştir. Kişisel Verileri Koruma Kurumu'nun 16.12.2020 tarihli "Alenileştirme Hakkında Kamuoyu Duyurusu"nda, alenileştirilen verilerin işlenmesinde dikkat edilmesi gereken hususlara yer verilmiştir. Alenileştirilen kişisel verilerin işlenmesinin, alenileştirme amacıyla sınırlı olması gerektiği ve veri sorumlularının bu ilkeye uygun hareket etmesinin önemi vurgulanarak alenileştirmenin kişinin bilinçli iradesiyle desteklenmesi gerektiği belirtilmiştir. Kişinin hür iradesi ile alenileştirilen kişisel verisinin işlenme sürecinde, alenileştirme amacına uygunluk ve veri minimizasyonu ilkelerine dikkat edilmesi gerektiği vurgulanmaktadır[117].

Kanun maddesinin gerekçesinde durum şöyle tarif edilmiştir; *"Fıkranın (d) bendine göre, ilgili kişinin kendisi tarafından alenileştirilen bir başka ifadeyle herhangi bir şekilde kamuoyuna açıklanmış olan kişisel verileri işlenebilecektir. Çünkü ilgili kişi tarafından alenileştirilen ve böylelikle herkes tarafından bilinebilecek hale gelen bu tür verilerin işlenmesinde, korunması gereken hukuki yararın ortadan kalktığı kabul edilmektedir."*

Bu ilkenin anonim şirketler açısından nasıl uygulandığını daha iyi açıklayabilmek için, konuya ilişkin örnekler üzerinden somut değerlendirmeler yapılması faydalı olacaktır;

Bir anonim şirketin çalışanlarının kişisel verilerini web sitesinde, sosyal medya hesaplarında, haber siteleri veya diğer kamuya açık platformlarda kendi isteğiyle paylaşması durumunda, bu kişisel veriler artık özel niteliğini kaybetmiş ve kamuya mal olmuş kabul edilmektedir. 6698 sayılı Kanun'a göre, kişisel verilerin alenileştirilmesi, anonim şirketin veri sorumlusunun çalışanların kişisel verilerini açık rıza almadan işleyebileceği anlamına gelmez. Fakat verisi

[117] KVKK, "*Alenileştirme" Hakkında Kamuoyu Duyurusu,* https://www.kvkk.gov.tr/Icerik/6843/-ALENILESTIRME-HAKKINDA-KAMUOYU-DUYURUSU, (Erişim Tarihi:21.12.2024).

işlenen kamu görevlisi ise kimlik bilgileri, görevleri ve yaptıkları işler zaten kamuya açık olduğundan, bu bilgilerin işlenmesi genellikle açık rıza gerektirmeyecektir. Anonim şirketin yöneticilerinin isimleri, görevleri ve şirketle ilgili bilgileri genellikle kamuya açık kaynaklarda, ticaret sicil gazetesinde bulunabilmektedir. Bu nedenle, bu verilerin işlenmesi için açık rıza aranmayacaktır.

Diğer bir unsur ise kanuna dayalı bir zorunluluk hali bulunması olabilir. Bir suç işlenmesi durumunda, failin kimliği gibi alenileştirilmiş veriler, soruşturma ve kovuşturma süreçlerinde kullanılabilir. Bir kişinin sosyal medya hesabında paylaştığı doğum günü gibi bilgiler kamuya açık ve aleni olduğundan, bu bilgilerin bir doğum günü mesajı göndermek gibi amaçlarla kullanılması genellikle açık rıza gerektirmez. Ancak, bu bilgileri bir anonim şirket ticari amaçlarla, pazarlama ve reklam faaliyetleri için kullanılması veya kişiye özel bir profil oluşturulması için açık rıza alınması gerekebilir.

ABC A.Ş.'nin finans direktörü olan bir gerçek kişinin kendi sosyal medya hesabı veya kamuya açık platformlarda, şirketin finansal durumu, yatırım ortaklıkları, vergi performansı ya da mali başarıları hakkında kişisel bir yorum yapması veya doğrudan bilgi paylaşımında bulunması durumunda, bu veriler kişinin kendisi tarafından alenileştirilmiş sayılır. Örneğin, ilgili kişinin “2024 yılı cirosunun %25 artış göstererek 2500 milyon TL’ye ulaştığı” şeklindeki paylaşımı hem şirket verisi hem de bu veriye dayalı olarak kişinin mesleki pozisyonu ve mali sorumluluk alanı hakkında bilgi içerdiğinden, kişisel veri niteliği taşıyabilir. Bu tür bir verinin, daha sonra başka bir haber platformunda referans gösterilmesi, ekonomik analiz raporlarında kullanılması veya kamuya açık bir dosyada değerlendirilmesi, KVKK m.5/2-d kapsamında açık rıza aranmaksızın hukuka uygun şekilde gerçekleştirilebilir. Aynı şekilde, Ticaret Sicili Gazetesi’nde yayımlanmış bir yetkili ataması, vergi levhasında yer alan temsilci bilgisi veya MERSİS sistemine kayıtlı imza yetkisi gibi kayıtlar da kamuya açık resmî kaynaklarda yer aldığından, bu bilgilerin işlenmesi için ayrıca açık rıza alınması gerekmez. Bu durumda dikkat edilmesi gereken husus, verinin alenileştirilmesinin ilgili kişinin özgür iradesine dayanması ve verinin alenileştirilme amacıyla orantılı şekilde kullanılmasıdır. Kişisel verinin alenileştirilmiş olması, sınırsız ve ölçüsüz şekilde kullanılabileceği anlamına gelmemekte; KVKK’nın 4. maddesindeki genel ilkelere (özellikle ölçülülük ve amaçla sınırlı olma) uygun olarak işlenmesi gerekmektedir.

Kişisel verilerin korunmasına ilişkin temel ilkelerden biri olan "amaçla sınırlı işleme," bireylerin alenileştirdikleri verilerin dahi belirli sınırlar içinde ve alenileştirme amacı doğrultusunda işlenmesi gerektiğini öngörmektedir. Bu bağlamda, Kişisel Verileri Koruma

Kurulu'nun 07.11.2019 tarihli ve 2019/331 sayılı kararı[118], alenileştirilmiş verilerin kullanım sınırlarına dair önemli bir içtihat niteliği taşımaktadır. Karar, bir sigorta şirketi tarafından, açık rızası alınmaksızın sigortacılık faaliyetleri kapsamında bir bireyin aranması üzerine yapılan şikâyet başvurusuna dayanmaktadır. Şirket, ilgili kişinin ad, soyad ve telefon bilgilerine halka açık bir internet sitesinden ulaştığını ve bu nedenle verilerin kullanımının hukuka uygun olduğunu savunmuştur. Ancak Kurul, bu bilgilerin alenileştirme amacı dışında kullanıldığını ve bireyin mesleki yetkinliklerinden faydalanma amacı taşımadan yalnızca ticari faaliyetler kapsamında iletişim kurulduğunu tespit etmiştir. Bu durum, 6698 sayılı Kişisel Verilerin Korunması Kanunu'nun (KVKK) 5/2 (d) maddesi kapsamında değerlendirilememiştir. Kurul, ayrıca şirketin kişisel verilerin hukuka aykırı olarak işlenmesini önlemek için gerekli teknik ve idari tedbirleri almadığını belirlemiş ve KVKK'nın 12/1(a) maddesine aykırılık nedeniyle, şirket hakkında 18/1(b) maddesi uyarınca 100.000 TL idari para cezası uygulanmasına karar vermiştir. Bu karar, alenileştirilmiş kişisel verilerin yalnızca alenileştirme amacı doğrultusunda kullanılabileceğini vurgulamakta ve veri sorumlularının hukuka uygunluk ilkesi çerçevesinde gerekli tedbirleri alma yükümlülüğünü açıkça ortaya koymaktadır.

Bu karar, veri gizliliği konusunda önemli bir örnektir. Kişilerin kişisel verilerinin, izinleri olmadan farklı amaçlarla kullanılmasının önlenmesi gerektiğini gösterir. İnternet üzerindeki kişisel verilerin korunması konusunda önemli bir dönüm noktasıdır. Kişilerin, çevrimiçi ortamda dahi kişisel verilerinin gizliliğine önem vermeleri gerektiğini vurgular. KVKK'nın bu kararı, şirketlerin kişisel verileri sadece belirtilen amaçlar doğrultusunda kullanması gerektiği ilkesini pekiştirmiştir. Sonuç olarak, alenileştirilmiş verilerin işlenmesi, KVKK'nın genel ilkeleri çerçevesinde değerlendirilmeli, veri sorumluları da bu verileri işlerken KVKK m.4'te tahdidi sayılan ilkelere uygun hareket etmelidirler.

### f. Kişisel Verilerin İşlenmesinin Bir Hakkın Tesisi, Kullanımı veya Korunması İçin Zorunlu Olması

Kanun kişisel verilerin işlenmesi için belirli şartlarından biri de "Bir hakkın tesisi, kullanılması veya korunması için veri işlemenin zorunlu olması" halidir. Kanunun 5. Maddesinin 2. Fıkra, (e) bendinde bahsi geçen bu hüküm kapsamında Kişisel Verileri Koruma Kurulu tarafından hazırlanan "*Kişisel Verilerin İşlenme Şartları Rehberi*[119]*"* de bazı örnekler vererek konuyu

[118]KVKK, *"İlgili kişi tarafından alenileştirilen kişisel verinin, alenileştirme amacı dışında işlenmesi" hakkında Kişisel Verileri Koruma Kurulunun 07/11/2019 Tarihli ve 2019/331 Sayılı Karar Özeti* https://www.kvkk.gov.tr/Icerik/6623/2019-331, (Erişim Tarihi: 21.12.2024).
[119] KVKK, "*Kişisel Verilerin İşlenme Şartları Rehberi"*, www.kvkk.gov.tr, (Erişim Tarihi: 29.10.2024).

açıklamıştır. Bu kapsamda, söz konusu hüküm, bir hakkın tesisi, kullanılması veya korunması için gerekli olan kişisel verilerin, ilgili kişinin açık rızasına ihtiyaç duyulmaksızın işlenebileceğini ifade etmektedir. Örneğin, bir işverenin, çalışanı ile ilgili bir hukuki ihtilaf durumunda gerekli belgeleri kullanması ya da bir alacaklının borçlusu aleyhine yasal takip başlatmak için borçla ilgili bilgileri işlemesi bu kapsama girmektedir. Kişisel Verileri Koruma Kurulu, bu ilkenin kötüye kullanılmaması ve yalnızca gerçekten zorunlu olan durumlarda uygulanması gerektiğine dikkat çekmiştir. Rehberde de vurgulandığı üzere, veri işleme faaliyetinin hukuka uygunluğu, işlemenin belirli bir hakkın tesisi, korunması ya da kullanılması için gerekli olup olmadığı ile doğrudan ilişkilidir. Dolayısıyla, bu şartın uygulanabilmesi için veri işlemenin amacının açıkça belirlenmiş olması ve veri sorumlusunun, işlenen verilerin hakkın korunması için zorunlu olduğunu ispatlayabilmesi gerekmektedir.

Kanunun madde gerekçesinde; *"Fıkranın (e) bendine göre, bir hakkın tesisi, kullanılması veya korunması için veri işlemenin zorunlu olması durumunda kişisel veriler işlenebilecektir. Bu bağlamda, bir şirketin kendi çalışanı tarafından açılan bir davada ispat için bazı verileri kullanması veya kısıtlı bir kişinin haklarının korunması amacıyla vasinin veya kayyımın, kısıtlının mali bilgilerini tutması hukuka uygun sayılacaktır"* Şeklinde tarif edilmiştir. GDPR'da direk böyle bir düzenleme olmasa da hem KVKK hem de GDPR, bir hakkın tesisi, kullanılması veya korunması için (bir mahkeme sürecinde delil olarak kullanılacak verilerin işlenmesi gibi) veri işlemenin gerekli olabileceğini kabul eder.

Kişisel Verileri Koruma Kurulunun 08/10/2020 Tarihli ve 2020/765[120] Sayılı *Bir Banka Tarafından Kurul Kararı ile Verilen Talimatın Gereğinin Yerine Getirilmemesi Hakkındaki* kararında, veri sorumlusu bir bankanın müşterilerine sunduğu aydınlatma metninde, KVKK'nın 5/2. fıkrasının (e) bendine atıfta bulunmuş ve bankanın, müşterilerinin kişisel verilerini bir hakkın tesisi, kullanımı veya korunması için işleyebileceğini belirtmiştir.

Bir davada taraf olan bir anonim şirketin çalışanı, ispat hususunda kişisel verileri (ad, soyad, T.C. kimlik numarası, adres vb.) delil olarak sunulabilir veya karşı tarafın savunması için kullanılabilir. Mahkeme, tanıkların ifadelerini aldığında, ifadelerinde geçen kişilerin kişisel verileri işlenir. Veya suç işleyen kişinin veya mağdurun kişisel verileri, suçun aydınlatılması ve cezanın belirlenmesi için kişisel veri işlenebilir. Yine bir anonim şirkette borcun tahsili için başlatılan icra takibinde, borçlunun kişisel verileri (ad, soyad, adres, mal varlığı bilgileri vb.)

[120]Kişisel Verileri Koruma Kurulunun 08/10/2020 Tarihli ve 2020/765 Sayılı Kararı, https://kvkk.gov.tr/Icerik/6844/2020-765., (E.T.:29.10.2024).

icra dairesince işlenir. Şirketten bir ürün veya hizmet satın alan kişinin kişisel verileri (ad, soyad, adres, iletişim bilgileri vb.), satış sözleşmesinin ifası, fatura kesilmesi ve garanti süreci gibi işlemler için kullanılacağı için kişinin verileri işlenebilir hale gelmektedir. Bir anonim şirket faaliyeti gereğince bir kira ilişkisi kuracaksa kira sözleşmesi imzalanan kişilerin kişisel verileri (ad, soyad, T.C. kimlik numarası, adres vb.), kira bedelinin tahsilatı, konut teslimi gibi işlemler için veriler işlenebilir. Çalışanların kişisel verileri (ad, soyad, T.C. kimlik numarası, adres, banka hesap bilgileri vb.), ücret ödemeleri, sosyal güvenlik işlemleri, izin takibi gibi iş sözleşmesinden doğan yükümlülüklerin yerine getirilmesi için verileri işlenebilir. Anonim şirkette bir sigorta olayı meydana geldiğinde, sigortalının kişisel verileri hasar bilgileri vb. gibi hasarın tespiti ve tazminatın ödenmesi için veriler işlenebilir.

### g. Kişisel Verinin İşlenmesinin Veri Sorumlusunun Meşru Menfaatleri İçin Zorunlu Olması

Kişisel verilerin işlenmesi için açık rıza aranmayan hallerden biri de "veri sorumlusunun meşru menfaatleri için veri işlemenin zorunlu olması" halidir. Bu durum, şirketlerin veya kurumların kendi meşru menfaatleri doğrultusunda kişisel verileri işlemesine olanak tanırken bu işlem, ilgili kişinin temel hak ve özgürlüklerine zarar vermeyecek ölçüde kanuna uygun olmalıdır. Kısacası bu gerekçe, keyfi bir şekilde kullanılamayacağından ötürü veri sorumlusu, meşru menfaatini kullanırken KVKK'nın genel ilkelerine, veri işleme şartlarına uymak zorundadır.

Kişisel Verileri Koruma Kurulunun 02/12/2021 Tarihli ve 2021/1218 Sayılı kararında, "*ilgili kişinin fotoğraf ve sair verilerinin Nisan 2021 sonrası dönemde veri sorumlusunun internet sitesinde yayınlanmasından ibaret olan kişisel veri işleme faaliyetinin Kanun'un 5'inci maddesinin (2) numaralı fıkrasının (f) bendindeki "İlgili kişinin temel hak ve özgürlüklerine zarar vermemek kaydıyla, veri sorumlusunun meşru menfaatleri için veri işlenmesinin zorunlu olması" hukuki sebebine dayanabileceği, bu yüzden de anılan faaliyeti dolayısıyla veri sorumlusu hakkında Kanun kapsamında yapılacak herhangi bir işlemin bulunmadığına''* karar verilmiştir.

GDPR Madde 6/1-f bendi de KVKK'daki bu düzenlemeye benzer niteliktedir. ''*Veri sahibinin kişisel verilerinin korunmasını gerektiren çıkarları veya temel hak ve özgürlükleri bu çıkarlara üstün gelmediği sürece, özellikle veri sahibinin çocuk olması durumunda, veri sorumlusu veya üçüncü bir kişi tarafından takip edilen meşru menfaatler için işlemenin gerekli olması.*

*Birinci fıkranın (f) bendi, kamu otoritelerinin görevlerinin ifası sırasında gerçekleştirdikleri işlemlere uygulanmaz."*

Ancak bu menfaat, ilgili kişinin temel hak ve özgürlüklerine, özellikle de mahremiyet hakkına üstün gelmemelidir. Her iki kanunda da bu durum veri işleme gerekliliğini bir istisna olarak kabul eder ve meşru menfaati veri işleme sürecinin bir gerekçesi olarak görerek, veri işlemeyi kanuni dayanak ve meşru amaç çerçevesinde gerçekleştirmeyi amaçlar. Ancak bu meşru menfaat ilgili veri sahibinin temel hak ve özgürlüklerine zarar vermemelidir[121]. İlgili durum Kişisel Verileri Koruma kanunun madde gerekçesinde "*...ilgili kişinin temel hak ve özgürlüklerine zarar vermemek kaydıyla, veri sorumlusunun meşru menfaatleri için veri işlenmesinin zorunlu olması durumunda da açık rıza şartı aranmaksızın kişisel veriler işlenebilecektir. Buna göre, örneğin bir şirket sahibi, çalışanlarının temel hak ve özgürlüklerine zarar vermemek kaydıyla, onların terfileri, maaş zamları yahut sosyal haklarının düzenlenmesinde ya da işletmenin yeniden yapılandırılması sürecinde görev ve rol dağıtımında esas alınmak üzere çalışanların kişisel verilerini işleyebilecektir. Burada, işletmenin yeniden yapılandırılması ya da ehliyetli ve liyakatli çalışanların terfi almaları, veri sorumlusu statüsündeki şirket sahibinin meşru menfaati cümlesindendir. Kişisel verilerin korunmasına ilişkin temel ilkelere uyulması ve veri sorumlusu ile ilgili kişinin menfaat dengesinin gözetilmesi gerekmektedir."* şeklinde ele alınmıştır.

GDPR'ın şerhinde madde 6/1'in gerekçesi şöyle tarif edilmiştir; "*GDPR madde 5 kapsamındaki çeşitli veri koruma ilkelerinden biri olan yasal işleme ilkesi, kişisel verileri içeren her türlü işleme faaliyetinin yasal bir dayanağının olmasını gerektirir. Madde 6/1 bu tür yasal bir dayanağı nelerin oluşturabileceğini ayrıntılı olarak belirlemektedir. Aynı zamanda kişisel verilerin hukuka uygun olarak işlenmesinin madde 5/1'de belirtilen kişisel verilerin işlenmesine yönelik diğer tüm ilkelerin de yerine getirilmesini gerektireceği unutulmamalıdır. Altı gerekçenin seçimi, Avrupa Birliği Temel Haklar Şartı (CFR) madde 52/1 ve Avrupa İnsan Hakları Sözleşmesi (AİHS) madde 8/2'de belirtilen temel haklara yönelik yasal sınırlamalara ilişkin genel kurallara karşılık gelmektedir. AİHS ve CFR'nin ilgili formülasyonlarındaki farklılıklara bakılmaksızın, CFR kapsamındaki koruma AİHS kapsamındakinden daha kapsamlı olsa da bu iki yasal belgedeki ilgili kuralların etkisi özünde eşdeğer olarak kabul edilmelidir. CFR'ye göre veri koruma hakkı ancak bunun bir AB veya üye devlet yasasında açıkça öngörülmesi ve bu yasanın içeriğinin yalnızca aşağıdaki sınırlamaları öngörme koşuluna uyuması halinde sınırlandırılabilir. Kamu yararı ve başkalarının hak ve*

[121] Dursun Saat, "Kişisel Verilerin Korunması Kanunu'nda Öngörülen Meşru Menfaat Kavramının Ticaret Şirketleri Bakımından Değerlendirilmesi", Anadolu Üniversitesi Hukuk Fakültesi Dergisi, Cilt: 10, Sayı: 2, Temmuz 2024, s. 617-638. https://earsiv.anadolu.edu.tr/xmlui/bitstream/handle/11421/28842/10.54699-andhd.1491304-3962034.pdf, (E.T: 05.05.2025).

*özgürlüklerinin korunması olabilen tanımlanmış işleme amacına ulaşmak için gerekli ve uygun olmalıdır. Ayrıca öngörülen sınırlamanın orantılı olması ve temel veri koruma hakkının özüne saygı göstermesi gerekmektedir*[122]*."*

Veri sorumlusunun meşru menfaati, genellikle şirketin işleyişi, çalışan ilişkileri, personel yönetimi, müşteri ilişkileri, ürün veya hizmet geliştirme, pazarlama faaliyetleri, güvenlik, şirketin finansal işlemlerinde hile ve dolandırıcılığı önleme, alacak takipleri, tahkim ve arabuluculuk süreçleri gibi faaliyetlerle ilgili olabilir. Ayrıca şirket birleşmelerinde veri entegrasyonu sağlamak amacıyla birleşen şirketlerin müşteri ve şirketin çalışan verilerinin birleştirilmesi gerekmektedir, bu nedenle de bu kişisel verileri işlemek veri sorumlusunun meşru menfaatini doğuracaktır[123].

Bu kapsamda, veri sorumlusunun meşru menfaati gerekçesiyle gerçekleştirilen veri işleme faaliyetlerine ilişkin uygulamalardan biri de güvenlik kameraları aracılığıyla görüntü kaydı alınmasıdır. XYZ A.Ş. unvanlı bir depo işletmesi, iş yeri güvenliğini sağlamak, iş kazalarını önlemek ve yaşanan kazalarda sorumluluk sınırlarının belirlenmesi amacıyla depo alanlarında sürekli güvenlik kamerası sistemi kullanmaktadır. Sistem ayrıca, depolama sistemi üzerindeki hırsızlık vakalarını tespit etmek ve suçluların belirlenmesini kolaylaştırmak için de kullanılmaktadır. Bu uygulama kapsamında elde edilen görüntüler; depo güvenliğini sağlamak, iş kazası analizlerini hızlı ve objektif yapabilmek, hukuki sorumlulukların tespiti için somut delil elde etmek amacıyla sistematik şekilde toplanmakta ve gerekli hallerde raporlama için kayıt altına alınmaktadır. Burada, aktarılmak istenen veri görsel kayıtlar olduğu için açık rıza alınması mümkün değildir; çünkü bu veriler, ilgili çalışanların veya ziyaretçilerin işyeriyle kurulan sözleşmenin ifasıyla değil, XYZ A.Ş.'nin iş yeri güvenliği yükümlülüğünü yerine getirmesi amacıyla toplanmaktadır. Ancak bu uygulamanın meşru menfaat temelini oluşturabilmesi için Kurul'un belirlediği üç kriterin sağlanması gerekir (KVKK m.5/2-f):

Meşru bir menfaat varlığı:

XYZ A.Ş.'nin iş yeri güvenliği ve iş kazalarının delillerle desteklenmiş olarak incelenmesi menfaati, gerçek ve kazanç amaçlı olmayan, ancak iş süreçlerinin güvenli şekilde yürütülmesi için zorunludur.

Gereklilik (necessity):

---

[122] Christopher Kuner, Lee A. Bygrave, Christopher Docksey, *The EU General Data Protection Regulation (GDPR) A Commentary,* Oxford University Yayınları, 2020, s. 325.
[123] Dursun Saat, *op. cit.*

Kamera sistemi olmadan söz konusu amaçlara ulaşmak mümkün gözükmemektedir; iş kazaları sonrası somut delil elde edilmesi ve suçlu tespiti için sesli/görsel kayıtlar ön şarttır.

Denge testi:

Çalışanların ve ziyaretçilerin mahremiyet hakkı ile şirketin menfaati arasında ölçülü bir denge kurulmuştur. Kamera, yalnızca depo alanlarını kapsayacak şekilde konumlandırılmış; özel alanlar (soyunma odası, tuvalet) görüntülenmemekte; ayrıca açık uyarılarla aydınlatma yapılmaktadır.

## D. ÖZEL NİTELİKLİ (HASSAS) KİŞİSEL VERİLERİN İŞLENME ŞARTLARI

Kişisel verilerin Korunması Kanunu madde 6'da özel nitelikli veriler numerus clausus yoluyla sayarak kişilerin ırkı, etnik kökeni, siyasi düşüncesi, felsefi inancı, dini, mezhebi veya diğer inançları, kılık ve kıyafeti, dernek, vakıf ya da sendika üyeliği, sağlığı, cinsel hayatı, ceza mahkûmiyeti ve güvenlik tedbirleriyle ilgili verileri ile biyometrik ve genetik verileri gibi özel nitelikli kişisel verilerin işlenmesini daha sıkı bir şekilde düzenler. 12 Mart 2024 tarihli ve 32487 sayılı Resmi Gazete' de yayımlanan 7499 sayılı Kanun'un 33. Maddesiyle özel nitelikli kişisel verilerin işlenmesi koşulları daha kapsamlı bir şekilde hukuki çerçeve yeniden düzenlenmiştir[124]. Bu düzenlemeyle birlikte, veri işleme faaliyetlerinde daha yüksek güvenlik seviyeleri hedeflenmiş, özellikle sağlık, cinsel hayat gibi hassas kabul edilen kişisel verilerin işlenmesi konusunda önemli yenilikler getirilmiştir.

7499 sayılı Kanunun 33. maddesi ile yapılan bu değişiklikler, özellikle kişisel verilerin korunması alanında önemli bir dönüm noktası olmuştur. Bu değişiklikle kişisel verilerin korunması hukuku daha da güçlendirilmiştir. Türkiye Büyük Millet Meclisi Adalet Komisyonu, bu değişiklikleri yaparken bazı temel gerekçelere dayanmıştır. En temel gerekçe Avrupa Genel Veri Koruma Tüzüğü ile KVKK'nın uyumlaştırılmasıdır. Türkiye'nin Avrupa Birliği (AB) üyeliği sürecinde, KVKK'nın AB'nin kişisel veri koruma mevzuatına uyum sağlanması stratejik amacı odak noktasıdır. 7499 sayılı Kanunun 33. Maddesindeki bu değişiklikler ile KVKK'nın, Avrupa Genel Veri Koruma Tüzüğü ile daha uyumlu hale getirilmesi amaçlanmıştır. Uyumlanan KVKK ile AB ile ticaret ilişkileri güçlenecek hem Türk vatandaşlarının kişisel verilerinin daha etkin bir şekilde korunması sağlanacak hem de diğer ülkelerin Türkiye'deki verilerinin koruma altında olacağına inanç artacaktır.

[124] Öztürk, Bahri, Elif Altınok Çalışkan, Serkan Seyhan, *Kişisel Verilerin Korunması Hukuku Teorik ve Pratik Çalışma Kitabı*, Ankara, Seçkin Hukuk, 3. Baskı, 2024, s. 101.

Teknolojinin hızla gelişmesi kişisel verilerin işlenmesi yöntemleri ve hacmi de artırmış bu da kişisel verilere yönelik riskleri beraberinde getirmiştir. Bu yeni düzenlemelerle, bu risklere karşı daha güçlü bir koruma sağlanarak kişisel verilerin güvenliği artırılmak ve uyumlanmak istenmiştir. Bu değişikliklerle, bireylerin kişisel verileri üzerindeki hakları daha da genişletilmiş, bireylerin haklarının güçlendirilmesi amaçlanmıştır. Bireyler, kişisel verilerine erişme, düzeltme, silme ve benzeri gibi haklarını daha kolay kullanabileceklerdir. Ayrıca, veri sorumlularının yükümlülükleri artırılmış, bireylerin kişisel verilerinin nasıl işlendiği hakkında daha fazla bilgi vermeleri gerektiği sağlanmıştır. Bu sayede, veri sızıntıları ve diğer güvenlik olaylarının önlenmesi amaçları güdülmüştür. Özetle 33. Maddedeki bu değişikliklerle hem bireylerin hakları güçlendirilmiş hem de ülkemizin uluslararası standartlara uyum sağlaması hedeflenmiştir. Kişisel veri ihlallerine ilişkin yaptırımların daha ağırlaştırılması sebebiyle, veri sorumlularının kişisel verileri koruma konusunda daha duyarlı olmaları ve caydırıcılık hedeflenmiştir.

Kişisel Verileri Koruma Kurulunun 05/12/2018 Tarihli ve 2018/143 Sayılı kararında, sağlık verilerini KVKK'nın 6. maddesinde yer alan işleme şartlarından birine dayanmadan üçüncü kişilere aktaran veri sorumlusu hakkında değerlendirmelerde bulunmuştur. Bu karar ile özel nitelikli kişisel verilerin işlenme şartları, hukuka aykırı işlenmesinin sonuçları ele alınmış ve veri sorumlusu eczaneye idari para cezası verilmesine hükmedilmiştir.

Kişisel verinin kişiye sıkı sıkıya bağlı bir hal olduğu unutulmamalıdır. Örneğin bir Anonim Şirketin işe alım sürecinde başvuran adayların sağlık durumları, engellilikleri veya dini inançları gibi özel nitelikli verilerini istemesi ve bu verileri işlemesi ancak bu durumun işin gerektirdiği niteliklerle doğrudan ilgili olması ve adayın açık rızası alınması şartıyla mümkün olabilir[125].

[125] Uygulamada işe alım süreçlerinde işin niteliğine göre sağlık durumu veya engellilik bilgisinin alınmasının makul ve zorunlu olduğunu durumlar söz konusu olabilir. Örneğin, ağır fiziksel işlerde çalışacakların sağlık durumu sorgulanabilir. Ancak, işle doğrudan ilgili olmayan hassas verilerin toplanması ve işlenmesi eleştiri konusudur ve yasaklanmalıdır. İşverenlerin gereksiz veri toplaması veya açık rıza almadan veri işlemesi durumunda yaptırım ve tazminat sorumluluğu gündeme gelir.

# İKİNCİ BÖLÜM

## 6698 SAYILI KİŞİSEL VERİLERİN KORUNMASI KANUNU VE GVKT UYARINCA KİŞİSEL VERİLERİN YURT DIŞINA AKTARILMASI

Çalışmamızın bu bölümünde, kişisel verilerin yurt dışına aktarılması konusu, Türkiye'deki ve Avrupa'daki yasal düzenlemeler çerçevesinde ana hatlarıyla ele alınacak ve anonim şirketler bakımından örneklendirilecektir.

### I. YURT DIŞINA AKTARIMA İLİŞKİN TEMEL KAVRAMLAR

#### A. AKTARIM KAVRAMI

6698 sayılı Kişisel Verilerin Korunması Kanununda "aktarım" kavramı için doğrudan bir tanım yapılmamış; kanunun 8. Maddesi ile yurt içinde kişisel verilerin aktarımına ilişkin, 9. Maddesi ile de kişisel verilerin yurtdışına aktarılmasına ilişkin yöntemler ve bu sürecin nasıl gerçekleşeceğine dair yönergeler belirlenmiştir. Ayrıca Kurul tarafından yayınlanan rehber niteliğindeki kılavuzlarda da "aktarım" kavramına ilişkin herhangi bir tanıma yer verilmemiştir[126]. GDPR'da da aynı şekilde aktarım kavramına ilişkin bir tanım bulunmamaktadır.

Bu başlık altında aktarım kavramı esasen, kişisel verilerin bir yerden başka bir yere veya bir ülkeden başka bir ülkeye taşınmasını ifade eder. 9. Maddenin lafzına bakıldığında kişisel verilerin yurt dışına aktarılması kavramının sadece aktarımından ibaret olmadığı, aynı zamanda bu kişisel verilerin korunması ile ilgili, verilerin alıcı ülkenin yasaları ve güvenlik standartlarına uygun olarak işlenmesi gerektiği de görülmektedir. Yani bir veri aktarımının yapılabilmesi için

[126]KVKK, "6698 sayılı Kanunda Yer Alan Temel Kavramlar", *http://nitelikliveri.com/wp-content/uploads/2020/01/6698_sayili_kanunda_yer_alan_temel_kavramlar.pdf,* (Erişim Tarihi: 05.01.2025), *https://www.kvkk.gov.tr/Icerik/4187/6698-Sayili-Kanun'da-Yer-Alan-Temel-Kavramlar,(*Erişim Tarihi:05.01.2025).

verilerin aktarıldığı ülkenin de benzer bir koruma sağlayabilmesi gereklidir. Kanun maddesinde bu durum "yeterlilik" kararı ile ifade edilmiştir. Aktarım kavramını ele alan bir diğer kaynak, bizdeki Kişisel Verileri Koruma Kurumu'na benzer nitelikte olan, GDPR'in uygulanmasından sorumlu bağımsız bir Avrupa Birliği otoritesi Avrupa Veri Koruma Kurulu (EDPB)'dir. Kişisel verilerin yurt dışına aktarılması, EDPB'nin sıklıkla ele aldığı ve hakkında detaylı kılavuzlar yayınladığı bir konudur. EDPB, kişisel verilerin yurt dışına aktarılmasında temel olarak şu ilkelere dayanır[127]:

Avrupa Komisyonu Yeterli Koruma İlkesi: Verilerin aktarıldığı ülkede, AB'deki kadar kapsamlı bir veri koruma düzeyi bulunmalıdır. EDPB üçüncü ülkelerin veya uluslararası örgütlerin veri koruma düzeyini değerlendirerek yeterlilik kararları verir.

Standart Sözleşme Maddeleri (SCC): Veri ithalatçısı ve ihracatçısı arasında, veri koruma konusunda belirli standartları içeren sözleşmeler yapılması gereklidir. EDPB standart sözleşme maddelerinin içeriği ve uygulanması konusunda rehberlik sağlar.

Bağlayıcı Kurumsal Kurallar (BCR): Çok uluslu şirketlerin, tüm grup şirketleri için geçerli olacak şekilde, veri koruma konusunda yüksek standartları belirleyen iç politikalar oluşturması gereklidir. EDPB, BCR'ların değerlendirilmesi ve onaylanması sürecinde yer alır.

Veri Koruma Mekanizmaları: Üçüncü ülkelerle veya uluslararası örgütlerle veri koruma konusunda anlaşmalar yapılmasını gerektirir.

Ayrıca EDPB kişisel verilerin yurt dışına aktarılmasıyla ilgili şikayetleri değerlendirir, inceler ve gerekli kararları alır.

AB 2018/1725 sayılı Tüzük, uluslararası transferin tanımını yapmasa da Avrupa Veri Koruma Kurulu EDPB, AB ofisleri ve ajanslarının (EUI'lerin) kullanabileceği üç önemli temel kriter belirlemiştir[128]:

*"Aktarımda yer alan denetleyici veya işlemci, söz konusu işleme ilişkin olarak AB veri koruma hukukuna tabidir,*

*Denetleyici veya işlemci, kişisel verileri ifşa veya iletim yoluyla başka bir veri denetleyicisine veya işlemciye sunar,*

[127]EDPB, *https://edpb.europa.eu/* (Erişim Tarihi:05.01.2025).
[128]https://www-edps-europa-eu.translate.goog/data-protection/data-protection/reference-library/international-transfers_en?_x_tr_sl=en&_x_tr_tl=tr&_x_tr_hl=tr&_x_tr_pto=tc, Erişim Tarihi:06.01.2025).

*Bu diğer veri sorumlusu veya işlemcisi, AEA dışındaki bir ülkedir veya uluslararası bir kuruluştur."*

12.03.2024 tarihli ve 32487 sayılı Resmi Gazete 'de yayımlanan 7499 sayılı Ceza Muhakemesi Kanunu ile bazı kanunlarda değişiklik yapılmasına dair kanunun 34. Maddesi ile değiştirilen 6698 sayılı Kanunun 9. maddesinin uygulanmasına dair usul ve esasları belirleyen Yönetmeliğin 4. maddesinin (e) bendinde, kişisel verilerin yurtdışına aktarılması, *"kişisel verilerin 6698 sayılı Kanun kapsamındaki bir veri sorumlusu veya veri işleyen tarafından yurt dışındaki bir veri sorumlusu veya veri işleyene iletilmesi ya da başka bir suretle erişilebilir hâle getirilmesi"* şeklinde tanımlanmıştır[129].

Çalışmamızın konusu Anonim Şirketlerde Yurt Dışına Kişisel Veri Aktarımlarının Hukuki Dayanağı Olarak Standart Sözleşmeler ile sınırlı olduğu için KVKK kapsamında yurt içinde kişisel veri aktarımı incelenmeyecektir.

Bir Kişisel Veri İşleme Türü Olarak "Aktarım" kavramını ele aldığımızda; bu kavram bize, bir kişinin kimliğini doğrudan ya da dolaylı olarak belirleyen her türlü bilgi olarak tanımlayabileceğimiz "kişisel verilerin", bir yerden başka bir yere taşınmasını ifade eder. Bu aktarım, bir anonim şirketin farklı departmanları arasında olabileceği gibi, tamamen farklı bir kuruma veya kişiye de gerçekleşebilir. Örneğin, bir anonim şirketin internet sayfasından satın aldığınız ürünün kargo şirketine gönderilmesi sırasında isim-soy isim, telefon numarası, adres bilgilerinizin kargo şirketine aktarılması bir kişisel veri aktarımı örneğidir.

Veri sorumlularınca kişisel veri aktarımı yaparken kanunda belirlenen aşağıdaki noktalara dikkat etmek önemlidir:

Aktarımın hukuki bir sebebi olmalıdır. Kişisel verilerin aktarımı sırasında verilerin güvenliği sağlanarak aktarılacak verilerin kapsamı net bir şekilde belirlenmelidir. Ayrıca hangi kişisel verilerin aktarılacağına ilişkin kişinin veya kurumun kimliği ve verileri ne amaçla kullanacağı da açıkça belirtilmelidir.

Veri sorumlusu ve veri işleyen kavramları, yalnızca gerçek kişilerin için değil, tüzel kişiler içinde çalışanlarının kişisel verileri üzerindeki işleme faaliyetlerinde yükümlülüklerini belirlemek için kullanılır. Böylece kişisel verilerin işlenmesi sürecinde veri sorumlusu, veri işleyen ve verisi işlenen tüm tarafların sorumluluğu net bir şekilde belirlenmiş olmaktadır.

[129]KVKK, *"Kişisel Verilerin Yurt Dışına Aktarılması Rehberi*", KVKK Yayınları no:48, Ocak 2025, https://www.kvkk.gov.tr/Icerik/8142/Kisisel-Verilerin-Yurt-Disina-Aktarilmasi-Rehberi, (Erişim Tarihi: 05.01.2025)

Kişisel veriler bireylere ait olsa da bu verileri işleyen taraf olan kurumlar veya kişiler de yasal yükümlülük altındadır. Veri işleme sürecine dahil olan her taraf, veri sorumlusu veya veri işleyen olarak tanımlanır ve bu kapsamda kanunda belirlenmiş yasal yükümlülükleri vardır.[130]

Anonim şirketler, faaliyetleri gereği büyük miktarda kişisel veri işlemek mecburiyetinde kalırlar. Bu veriler farklı departmanlar arasında aktarılabileceği gibi üçüncü kişilere aktarımı da oldukça sık görülür.

Bir anonim şirket için iç aktarım örnekleri;

Personel dosyalarındaki bilgiler (Ad Soyad, doğum tarihi, T.C. kimlik numarası, iletişim bilgileri, adres bilgileri, öğrenim bilgileri vb.) muhasebe departmanına maaş ödemeleri için, hukuk departmanına ise iş sözleşmeleri için aktarılabilir. Müşteri bilgileri (Ad Soyad, iletişim bilgileri, sipariş geçmişi vb.) pazarlama departmanına pazarlama kampanyaları için, müşteri hizmetleri departmanına ise müşteri görüş ve şikayetlerini yönetmek için aktarılabilir. Üretim sürecinde çalışanların kişisel verileri (Ad Soyad, görev, çalışma saatleri, nöbet çizelgeleri vb.) üretim planlama ve performans değerlendirme süreçlerinde kullanılarak üretim departmanına iletilebilir.

Dış Aktarım Örnekleri ise;

Üretimde kullanılan ham maddelerin tedarikçilerine sipariş ve fatura bilgilerinin aktarılması yani tedarikçilere aktarım, Müşteri siparişlerinin kargo şirketlerine gönderilmesi sırasında isim soy isim, adres ve iletişim bilgilerinin aktarılması kargo şirketlerine veri aktarım örneğidir. Ödeme işlemlerinin gerçekleştirilmesi için çalışanların banka hesap bilgilerinin aktarılması Bankalara kişisel veri aktarım örneğidir. Kanuni yükümlülükler gereği vergi dairesi, sosyal güvenlik kurumları ve benzeri gibi resmi kurumlara yasal olarak gerekli olan bilgilerin aktarılması, verilerin yedeklenmesi, analiz edilmesi için bulut hizmet sağlayıcılarına aktarım sağlanması, ürün veya hizmet pazarlama kampanyaları için müşteri bilgilerinin pazarlama ajanslarına aktarılması gibi.

[130] Bknz. *https://www.kvkk.gov.tr/Icerik/2052/Yurtici-Aktarim*.

## B. SINIR ÖTESİ VERİ İŞLEMENİN ve ULUSLARARASI AKTARIMIN KAPSAMI

### 1. SINIR ÖTESİ VERİ İŞLEME KAPSAMI

Küreselleşen dijital dünya ile birlikte şirketlerin uluslararası faaliyetlerinin artması ve bulut teknolojilerinin yaygınlaşmasıyla daha sık görülmeye başlayan sınır ötesi işleme kavramı; bir veri sorumlusunun veya işleyicisinin, kişisel verileri başka bir ülke veya bölgedeki sistemler veya sunucular aracılığıyla işlemesi, analiz etmesi, düzenlemesi, paylaşılması anlamına gelmektedir. Sınır ötesi veri işleme kavramının tanımı GDPR madde 4 tanımlar kısmında şöyle yer almaktadır[131]:

*m.4 (23) "sınır ötesi işleme":*

*(a) veri sorumlusu veya veri işleyenin birden fazla Üye Devlet'te kurulu olması halinde, kişisel verilerin, söz konusu veri sorumlusu veya veri işleyenin birden fazla Üye Devlet'te bulunan kuruluşlarının faaliyetleri bağlamında işlenmesidir veya*

*(b) bir veri sorumlusu veya veri işleyenin Birlik içinde bulunan tek bir kuruluşunun faaliyetleri bağlamında gerçekleşen, ancak birden fazla Üye Devlet'teki veri öznelerini kayda değer ölçüde etkileyen veya kayda değer ölçüde etkileme ihtimali bulunan kişisel veri işlemesidir.*

GDPR'ye göre, verilerin AB dışına aktarılması için yeterli veri koruma standartlarına sahip ülkelere veri aktarımı yapılması, BCR, SCC ya da veri sahibinin açık rızası ile veri aktarımı yapılması koşullarının sağlanması gerekir.

Anonim şirketler, küresel faaliyetleri nedeniyle sıklıkla sınır ötesi veri işleme yapmak durumundadırlar. Bu durum, şirketlere hem yeni pazarlara ulaşma fırsatı sunar, hem de veri güvenliği ve yasal konularda riskleri de beraberinde getirir. GDPR sınır ötesi veri işleme işlemlerini düzenlerken, anonim şirketlerin veri işleme faaliyetlerine de belirli kurallar getirir. Sınır ötesi veri işleme, şirketlerin küresel pazarlara ulaşmasını ve daha geniş bir müşteri kitlesine hitap etmesini sağlar. Bulut teknolojileri gibi hizmetler sayesinde şirketler, veri depolama ve işleme maliyetlerini düşürebilir ve iş süreçlerini optimize ederek verimliliği artırabilir. Farklı ülkelerdeki teknolojik gelişmelerden yararlanma imkanı ile inovasyon sağlar. Bunun yanında farklı riskler de oluşabilir. Verilerin farklı ülkelerde depolanması ve işlenmesi, veri sızıntısı riskini artırabileceğinden veri gizliliğine halel getirebilir. Her ülkenin farklı veri koruma yasaları bulunması nedeniyle, şirketlerin bu yasaları ihlal etme, yasal uyumsuzluk

[131]GDPR, https://www.ab.gov.tr/siteimages/resimler/Nihai-ABB-HCDB-GDPR.pdf (Erişim Tarihi:05.01.2025)

oluşturma riski bulunur. Veri koruma yasalarına aykırı hareket eden anonim şirketler, yüksek miktarda idari para cezalarıyla karşı karşıya kalabilirler.

Anonim Şirketler bakımından sınır ötesi veri işleme kavramını daha iyi anlayabilmek için, örnekler üzerinden açıklama yapılacaktır:

Bir Türk anonim şirketi, tüm şirket verilerini Fransa merkezli bir bulut depolama hizmetine kaydediyorsa, bu sınır ötesi veri işlemeye örnektir. GDPR m.4'teki tanım ele alındığında görüldüğü üzere sınır ötesi veri işleme kavramı AB sınırları içinde gerçekleşir fakat Türkiye'yi de ilgilendiren bir veri işleme faaliyetidir.

Türkiye'de faaliyet gösteren bir e-ticaret şirketi, müşteri bilgilerini (ad, soyad, adres, ödeme bilgileri, vergi kimlik numarası gibi) Avrupa Birliği ülkelerinde bulunan bir sunucuda saklıyorsa, bu da sınır ötesi veri işlemesidir.

Bir Türk kozmetik şirketi, global pazarlama kampanyaları için müşteri verilerini farklı ülkelerdeki pazarlama platformlarına aktarıyorsa, bu durum sınır ötesi veri işlemesine girer.

Bir mobil uygulama geliştiren Türk şirketi, uygulamayı kullanan kullanıcıların verilerini İspanya veya Malta merkezli sunucularda saklıyorsa, bu da sınır ötesi veri işlemesidir.

Bir Türk üretim şirketi, yabancı bir ortakla iş birliği yaparak üretim süreçlerini yönetiyor ve bu süreçte ortak şirketin sistemlerine veri aktarımı yapıyorsa, bu da sınır ötesi veri işlemesine örnektir.

Funly Family Eğitim Teknoloji ve Oyun Ticaret A.Ş., oyuncuların oyun içi davranışlarını detaylı bir şekilde analiz etmek ve değerlendirmek amacıyla, topladığı kişisel verileri yabancı bir veri analiz platformuna aktarabilir[132]. Bu tür bir veri aktarımı, kişisel verilerin sınır ötesi paylaşımını teşkil eder ve bu nedenle KVKK ve ilgili uluslararası veri koruma düzenlemeleri kapsamında özel şartlara ve yükümlülüklere tabidir. Sınır ötesi veri aktarımı, oyuncuların kişisel verilerinin yurt dışındaki üçüncü taraflarca işlenmesini içerdiği için, veri sorumlusu olarak şirketin hem hukuki sorumluluğu artmakta hem de bu aktarımın güvenli, şeffaf ve yasalara uygun şekilde gerçekleştirilmesi gerekmektedir.

AB ülkelerinde faaliyet gösteren İsviçre merkezli bir teknoloji alanında hizmet veren bir anonim şirket, Türkiye'deki bir veri işleyicisine (bulut hizmet sağlayıcısı) müşteri verilerini aktarmak istiyor. Bu, sınır ötesi veri işleme olarak değerlendirilir çünkü kişisel veriler AB

[132] Bknz. https://www.funlyfamily.com/, https://funlygames.com/aydınlatma-metni.

dışındaki bir ülkeye aktarılacaktır. Bu halde, GDPR'ın sınır ötesi veri aktarımına dair belirlediği kurallar uygulanacaktır. Şirketin bu aktarımı gerçekleştirebilmesi için aşağıdaki adımlar ve güvenlik önlemleri gereklidir:

1. Yeterli Koruma Sağlayan Ülke Olarak Kabul Edilmesi: GDPR'ye göre, kişisel verilerin Avrupa Birliği (AB) dışına aktarılabilmesi için, verilerin aktarılacağı ülkenin yeterli koruma sağlaması gerekir[133]. Bu yeterli koruma, söz konusu ülkenin veri koruma yasalarının AB'nin GDPR'ine benzer bir düzeyde kişisel veri koruma sağladığını gösteren bir değerlendirmeye dayanır. Her ne kadar KVKK değişiklikleri ile GDPR uyumu yakalanmaya çalışılsa da henüz AB, ülkemizi güvenli ülke olarak görmemektedir[134]. Eğer Türkiye, GDPR'a göre yeterli veri koruma seviyesine sahip bir ülke olarak kabul edilmiş olsaydı veri aktarımı doğrudan yapılabilirdi. Türkiye, şu an itibarıyla Avrupa Komisyonu tarafından yeterli koruma sağlayan bir ülke olarak kabul edilmemektedir. Bu nedenle, Türkiye'ye yapılan veri aktarımları, diğer seçenekler (BCR/SCC/açık rıza) kullanılarak yapılmak zorundadır.

2. Bağlayıcı Şirket Kuralları (BCR)[135]: Eğer Türkiye'ye veri aktarılacak anonim şirket, Türkiye'deki veri işleyicisi ile bir grup şirketi içinde faaliyet gösteriyorsa, anonim şirket bu durumda BCR uygulayabilir. Bu kurallar, veri koruma standartlarını belirler ve şirketin tüm dünya genelindeki şubeleri için bağlayıcı hale gelir. BCR'ler, şirketin veri güvenliği sağlamak için aldığı önlemleri içeren bir dizi ilke ve düzenlemedir. Anonim şirketler, bu tür düzenlemelerle, verilerin korunmasını sağlayarak, GDPR'ye uygun hareket etmiş olurlar.

3. Standart Sözleşme Maddeleri (SCC): Adalet Divanı standart sözleşme maddelerini yeterli koruma sağlama yollarından biri olarak görür[136]. Türkiye'ye yapılan veri aktarımında, anonim şirket, Standart Sözleşme Maddeleri kullanarak, veri güvenliğini sağlamaya yönelik ek

[133] Bir yeterlilik kararına dayalı olarak yapılan aktarımlar başlıklı GDPR m.45: Bir yeterlilik kararına dayalı olarak yapılan aktarımlar Komisyonun bir üçüncü ülke veya söz konusu üçüncü ülke dahilindeki bir bölge veya bir ya da daha fazla sayıda sektörün ya da uluslararası bir kuruluşun yeterli düzeyde bir koruma sağladığına karar verdiği hallerde, bu ülke veya uluslararası kuruluşa yönelik bir kişisel veri aktarımı gerçekleşebilir. Böylesi bir aktarım için spesifik bir onay gerekmez.

[134] GDPR Uygun güvencelere tabi olarak yapılan aktarımlar başlıklı m.46:
1. 45(3) maddesi uyarınca bir kararın bulunmaması hâlinde, ancak veri sorumlusu veya veri işleyenin uygun güvenceler sağlamış olması hâlinde ve uygulanabilir veri öznesi haklarının ve veri öznelerine yönelik etkili hukuk yollarının mevcut olması koşuluyla, söz konusu veri sorumlusu veya veri işleyen bir üçüncü ülke veya bir uluslararası kuruluşa kişisel veri aktarabilir.

[135] GDPR m.46/2 1. paragrafta atıfta bulunulan uygun güvenceler, bir denetim makamından özel izin alınmasına gerek olmaksızın, aşağıdaki yollarla sağlanabilir:
(b) 47. Madde uyarınca bağlayıcı şirket kuralları.

[136] Avrupa Adalet Divanı, 16 Temmuz 2020 tarihli "Schrems II" kararında, Standart Sözleşme Maddeleri' nin (SCC) Avrupa Birliği dışındaki ülkelere yapılan veri aktarımlarında yeterli koruma sağlayabilecek mekanizmalardan biri olduğunu belirtmiştir. Ancak, bu mekanizmanın etkinliği, alıcı ülkedeki veri koruma düzeyinin AB standartlarına eşdeğer olması ve ek önlemlerin alınmasıyla mümkündür.

önlemler alabilir. SCC, Avrupa Komisyonu tarafından onaylanmış standart sözleşme maddeleridir ve verilerin AB dışına aktarılması sırasında veri sahibinin haklarını koruyacak şekilde düzenlenmiştir. Türkiye'de faaliyet gösteren anonim şirketler, AB'den Türkiye'ye yapılan veri aktarımlarında, Avrupa Komisyonu tarafından onaylanmış SCC'leri kullanarak, veri güvenliğini sağlamaya yönelik ek önlemler alabilirler. Bu sözleşmeler, veri sorumlusu ile veri işleyici arasında imzalanarak, kişisel verilerin korunmasına ilişkin taahhütleri ve yükümlülükleri belirler. Ancak, Türkiye'nin AB tarafından henüz "yeterli koruma" sağlayan ülkeler listesine dahil edilmemiş olması nedeniyle, SCC'lerin yanı sıra ek teknik ve organizasyonel tedbirlerin alınması gerekmektedir.

4. Veri Sahibinin Açık Rızası: Eğer yukarıdaki güvenlik önlemleri yetersizse, anonim şirket veri sahibinin açık rızasını alarak kişisel verileri yurtdışına aktarabilir. Ancak bu durumda, veri sahibine aktarılacak ülkede veri güvenliğiyle ilgili riskler hakkında bilgi verilmesi ve veri sahibinin bu riskleri kabul edip etmediğinin netleştirilmesi gereklidir. Değişiklik öncesinde kişisel verilerin aktarımı için ilgili kişinin net bir şekilde açık rızası gerekli idi. Ancak, değişen 9. Madde ile açık rıza artık diğer işleme şartlarıyla eşit konumda yer almakta, öncelikli/kural olarak dayanak kabul edilmemektedir.

5. Risk Değerlendirmesi ve Güvenlik Önlemleri: GDPR, sınır ötesi veri aktarımı yapmadan önce, veri sorumlusunun risk değerlendirmesi yapmasını ve gerektiğinde ek güvenlik önlemleri almasını gerektirir. Söz konusu anonim şirketin, Türkiye'ye veri aktarırken Türkiye'deki yasal düzenlemelerin veri güvenliği üzerinde nasıl bir etkisi olacağını analiz etmesi gerekmektedir.

## 2. ÜÇÜNCÜ ÜLKELERE VEYA ULUSLARARASI KURULUŞLARA AKTARIM KAVRAMI

GDPR çerçevesinde, kişisel verilerin üçüncü ülkelere veya uluslararası kuruluşlara aktarılması, kişisel verilerin Avrupa Birliği dışındaki bir ülkeye veya uluslararası bir organizasyona taşınmasını ifade eder. Bu tür bir veri aktarımı, AB dışındaki yerlerde kişisel verilerin nasıl korunacağına dair belirli düzenlemeler ve güvenlik önlemlerini içermelidir. Bu nedenle GDPR, kişisel verilerin üçüncü ülkelere veya uluslararası kuruluşlara aktarılması sürecini denetler ve çeşitli kurallara bağlar.

GDPR üçüncü ülke ile, Avrupa Birliği (AB) ve Avrupa Ekonomik Alanı (EEA) dışında kalan tüm ülkeleri kastetmektedir. Yani, AB ülkeleri dışında kalan herhangi bir ülke (ABD, Çin vs.

gibi) üçüncü ülke olarak kabul edilir. Uluslararası kuruluşlar[137] ise, Avrupa Birliği dışındaki organizasyonlar ve kurumlar olarak ifade edilir. Örneğin, Birleşmiş Milletler (BM), Dünya Sağlık Örgütü (WHO) gibi küresel organizasyonlar, GDPR kapsamında birer uluslararası kuruluş olabilir. GDPR'ın yaklaşımı, kişisel verilerin üçüncü ülkelere veya uluslararası kuruluşlara aktarımı konusunda yeterli koruma ilkesini temel almasıdır. Bu ilke, verilerin aktarıldığı ülkede veya kuruluşta, AB'deki kadar kapsamlı bir veri koruma düzeyinin bulunmasını gerektirir ve sıkı bir denetim uygular. Veri aktarımı, aşağıdaki şartlarla yapılabilir:

1. Yeterli Koruma Sağlayan Ülkeler: GDPR m.45[138]'e göre, Avrupa Komisyonu üçüncü ülke veya uluslararası bir kuruluş için yeterli seviyede bir koruma sağlanıp sağlanmadığını belirleyebilme yetkisine sahiptir. Komisyon eğer yeterli düzeyde koruma sağlandığını takdir ederse, kişisel verilerin aktarımı herhangi bir onay gerekmeksizin gerçekleşebilecektir. Üçüncü ülkelerin yasal prosedürlerini inceleyip değerlendiren komisyon o ülke yeterli koruma sağlıyorsa bir yeterli koruma kararı verir. Güvenli üçüncü ülkeler, Avrupa Komisyonu'nun yeterliliğe ilişkin bir karar temelinde uygun bir veri koruma düzeyini onayladığı ülkelerdir. Bu ülkelerde, ulusal yasalar, kişisel veriler için AB yasalarıyla karşılaştırılabilir bir koruma düzeyi sağlar.

Avrupa Komisyonunca belirlenen yeterli koruma düzeyi sağlayan üçüncü ülkeler şunlardır: Andorra, Arjantin, Kanada (ticari kuruluşlar), Faroe Adaları, Guernsey, İsrail, Man Adası, Japonya, Jersey, Yeni Zelanda, Kore Cumhuriyeti, İsviçre, GDPR kapsamında Birleşik Krallık ve LED kapsamında Amerika Birleşik Devletleri (AB-ABD Veri Gizliliği Çerçevesine katılan ticari kuruluşlar) ve Uruguay'ı yeterli koruma sağlayan ülkeler olarak tanımış ve bu ülkelere veri aktarımına açıkça izin vermiştir[139].

[137] GDPR m.4 (26): 'uluslararası kuruluş', uluslararası kamu hukukuna tabi bir kuruluş ve ona bağlı organlar veya iki veya daha fazla ülke arasındaki bir anlaşma ile veya bu anlaşmaya dayanarak kurulan herhangi bir diğer kuruluş anlamına gelir.

[138] GDPR m.45(1): Komisyonun bir üçüncü ülke veya söz konusu üçüncü ülke dâhilindeki bir bölge veya bir ya da daha fazla sayıda sektörün ya da uluslararası bir kuruluşun yeterli düzeyde bir koruma sağladığına karar verdiği hâllerde, bu ülke veya uluslararası kuruluşa yönelik bir kişisel veri aktarımı gerçekleşebilir. Böylesi bir aktarım için, herhangi bir özel onay gerekmez.

[139] https://commission-europa-eu.translate.goog/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en?_x_tr_sl=en&_x_tr_tl=tr&_x_tr_hl=tr&_x_tr_pto=tc, (E.T.: 06.01.2025).

Avrupa Adalet Divanı 16 Temmuz 2020 Schrems II kararına göre; *kişisel verilerin üçüncü ülkelere aktarılabilmesi için ilgili kişilere GDPR uyarınca AB'de teminat altına alınan korumaya eşdeğer bir koruma sağlanmış olmalıdır*[140].

2. Yeterli Koruma Sağlanmayan Ülkeler İçin Güvenlik Önlemleri: Avrupa Komisyonu tarafından yeterli koruma kararı verilmeyen bir ülke veya uluslararası kuruluş söz konusu olduğunda kişisel verilerin aktarılabilmesi için GDPR m.46[141]'da ki uygun güvencelere tabi olarak seçilen aktarım türlerinden biri ile sağlanmalıdır.

Örneğin, AB ülkelerinde faaliyet gösteren bir anonim şirketin ABD'deki bir iş ortağına kişisel veri aktarımı yapması gerekmektedir. GDPR'ye göre, ABD, Avrupa Komisyonu tarafından yeterli koruma sağlayan bir ülke olarak kabul edilmemektedir. Bu durumda, veri aktarımı için GDPR m.46'da ki uygun güvence yollarından birini seçmesi gerekmektedir.

Ülkemizde standart sözleşme kullanımına örnek vermek gerekirse;

Microsoft, küresel olarak veri hizmetleri sunan bir teknoloji alanında anonim şirkettir. Microsoft, GDPR ile uyumlu çalışmak için sıkça Standart Sözleşme Maddeleri kullanır. Türkiye, GDPR kapsamında yeterli koruma sağlayan bir ülke olarak kabul edilmediği için, Microsoft gibi veri işleyicilerinin Türkiye'deki müşterilerinin verilerini Avrupa'dan Türkiye'ye

[140]Hatice Hocaoğlu, Fatma Sümeyra Doğan, Zeynep Sena Saltık, Bulut Yasası ve Schrems II Kararı Işığında Türkiye'de Müşteri Hizmeti Uygulamaları Hakkında Uygulamacı Perspektifinden Değerlendirmeler, *Terazi Hukuk Dergisi*, Cilt: 16, Sayı: 174, Şubat 2021, Sayfa: 364-368.

[141] GDPR m.46:

1. 45(3) maddesi uyarınca bir kararın bulunmaması hâlinde, ancak veri sorumlusu veya veri işleyenin uygun güvenceler sağlamış olması hâlinde ve uygulanabilir veri öznesi haklarının ve veri öznelerine yönelik etkili hukuk yollarının mevcut olması koşuluyla, söz konusu veri sorumlusu veya veri işleyen bir üçüncü ülke veya bir uluslararası kuruluşa kişisel veri aktarabilir.

2. 1. paragrafta atıfta bulunulan uygun güvenceler, bir denetim makamından özel izin alınmasına gerek olmaksızın, aşağıdaki yollarla sağlanabilir:

(a)kamu makamları veya organları arasında hukuki bağlayıcılığı bulunan ve uygulanabilir bir belge;

(b) 47. madde uyarınca bağlayıcı şirket kuralları;

(c)93(2) maddesinde atıfta bulunulan inceleme usulü uyarınca Komisyon tarafından kabul edilen standart veri koruma hükümleri;

(d)93(2) maddesinde atıfta bulunulan inceleme usulü uyarınca bir denetim makamı tarafından kabul edilen ve Komisyon tarafından onaylanan standart veri koruma hükümleri;

(e)40. madde uyarınca onaylı davranış kuralları ile birlikte üçüncü ülkedeki veri sorumlusu veya veri işleyenin, veri öznesinin hakları ile ilgili olanlar da dâhil olmak üzere uygun güvenceler uygulamaya ilişkin bağlayıcı ve uygulanabilir taahhütleri veya

(f)42. madde uyarınca onaylı bir belgelendirme mekanizması ile birlikte üçüncü ülkedeki veri sorumlusu veya veri işleyenin, veri öznesinin hakları ile ilgili olanlar da dâhil olmak üzere uygun güvenceler uygulamaya ilişkin bağlayıcı ve uygulanabilir taahhütleri.

3. Yetkili denetim makamından alınan izne tabi olarak, 1. paragrafta atıfta bulunulan uygun güvenceler, özellikle aşağıdakilerle de sağlanabilir:

(a)Veri sorumlusu veya veri işleyen ile üçüncü ülke ya da uluslararası kuruluştaki veri sorumlusu, veri işleyen ya da kişisel verilerin alıcısı arasındaki sözleşme hükümleri veya

(b)kamu makamları ya da organları arasındaki idari düzenlemelere eklenecek olan uygulanabilir ve etkili veri öznesi hakları içeren hükümler.

aktarırken belirli güvenlik önlemleri alması gerekir. Bu güvenlik önlemlerinden biri de Standart Sözleşme Maddeleri' dir. SCC, GDPR kapsamında Avrupa Komisyonu tarafından onaylanan ve kişisel verilerin Avrupa dışına aktarılması için veri güvenliğini sağlamak amacıyla kullanılan sözleşme maddeleridir. Eğer bir veri aktarımı AB dışına, örneğin Türkiye'ye yapılacaksa, bu sözleşmelerle veri güvenliği garanti altına alınır. Microsoft Türkiye, Kişisel Verileri Koruma Kurumu tarafından 10 Temmuz 2024 tarihinde yayımlanan Standart Sözleşmeleri, Microsoft'un kurumsal anlaşma paketlerine dahil ettiğini açıklayarak KVKK ile uyumu sağlamıştır[142]. Microsoft'un Türkiye'ye veri aktarması için Standart Sözleşme maddelerini kullanması, GDPR'in hukuki çerçevesine uyumu için çok önemli bir adımdır. SCC, Türkiye gibi yeterli koruma sağlayan ülke olarak sayılmayan ülkeler için, GDPR ile uyumlu bir veri aktarımı ve veri güvenliği sağlamak için kritik bir mekanizmadır.

Microsoft, SCC'yi kullanarak AB dışındaki ülkelere veri aktarımı yaparken, GDPR'ye uygun hareket ettiğini ve kullanıcı verilerinin güvenliğini sağladığını kanıtlar. Bu, şirketin yasal sorumluluklarını yerine getirmesine yardımcı olur. Türkiye'deki şirketler de SCC aracılığıyla AB veri güvenliği standartlarına uygun olarak verilerini Microsoft'a aktarabilir. Böylece, veri güvenliği konusunda uluslararası kabul görmüş en yüksek düzeyde koruma hedeflenir.

Sınır ötesi veri işleme ile 3. ülkelere veya uluslararası kuruluşlara aktarım kavramı benzerlik gösterse de sınır ötesi veri işleme kavramında işleme faaliyeti AB sınırları içerisinde gerçekleşir fakat başka devletleri de ilgilendirir. 3. ülkelere veya uluslararası kuruluşlara aktarımda ise AB sınırlarını aşan bir veri işleme söz konusudur[143].

[142] https://www.linkedin.com/pulse/microsoft-türkiyeden-kvkk-ve-gdpr-uyumu-peakuptechnologies-ehi9f/ (E.T: 06.01.2025)
[143] Çelik, *op. cit.,* s.36-37.

## II. KVKK KAPSAMINDA KİŞİSEL VERİLERİN YURT DIŞINA AKTARIMI

Bu başlık altında, 6698 sayılı Kişisel Verilerin Korunması Kanunu'nun 9. maddesi çerçevesinde kişisel verilerin yurtdışına aktarılmasına ilişkin düzenlemeler ayrıntılı biçimde incelenecektir. Kanunun amacı doğrultusunda kişisel verilerin işlenmesi ve aktarımında bireylerin temel hak ve özgürlüklerinin korunması esas alınmıştır. Bu bağlamda, yurtdışına veri aktarımının hukuki çerçevesi, KVKK'nın uygulama alanı kapsamında değerlendirilerek ele alınacaktır. KVKK'nın uygulama alanı, kişisel verilerin Türkiye'de işlenmesi veya yurt dışına aktarılması durumlarında geçerlidir. Özellikle veri sorumlularının Türkiye'de bulunması veya Türkiye'de veri işlenmesi işleminin gerçekleşmesi halinde, Kanun hükümleri bağlayıcıdır. Bu nedenle, yurtdışına veri aktarımı konusu KVKK'nın temel uygulama alanlarından biri olup, sınır ötesi veri hareketlerinin güvenliğinin sağlanması açısından özel bir öneme sahiptir. Bu bağlamda, kişisel verilerin yurt dışına aktarımında; yeterlilik kararı, açık rıza, güvenli veri aktarımı yöntemleri, özel şartlar ve sözleşme yükümlülükleri unsurları detaylı bir şekilde ele alınarak, yurtdışına veri aktarımı ile ilgili hukuki çerçevenin kapsamlı bir analizi yapılacaktır.

### A. KVKK'NIN UYGULAMA ALANI

6698 sayılı Kişisel Verilerin Korunması Kanunu, kişisel verilerin işlenmesine ilişkin temel esasları belirleyerek bireylerin mahremiyetini korumayı temel alır. Kanunun uygulama alanı, çeşitli kriterlere göre belirlenmekte olup, bu kapsamda yer, kişi ve konu bakımından değerlendirilmesi gerekmektedir. Yer bakımından, Türkiye sınırları içinde gerçekleşen veri işleme faaliyetleri esas alınırken, bazı durumlarda yurtdışındaki veri işleyiciler de kanun kapsamına girebilmektedir. Kişi bakımından, KVKK hem gerçek hem de tüzel kişiler için bağlayıcı olup, veri sorumluları, veri işleyenler ve ilgili kişiler açısından farklı yükümlülükler getirmektedir. Konu bakımından ise kanun, kişisel verilerin işlenmesiyle ilgili tüm süreçleri kapsarken, bazı istisnalar öngörülmüştür. Aşağıda, KVKK'nın yer, kişi ve konu bakımından uygulama alanı detaylı olarak ele alınacaktır.

#### 1. Kişi Bakımından Uygulama Alanı

KVKK'nın 2. maddesi[144], kanunun yalnızca kişisel verileri işleyen gerçek ve tüzel kişilere uygulandığını açıkça ifade etmektedir. 6698 sayılı Kişisel Verilerin Korunması Kanunu

[144] KVKK, "m.2: (1) Bu Kanun hükümleri, kişisel verileri işlenen gerçek kişiler ile bu verileri tamamen veya kısmen otomatik olan ya da herhangi bir veri kayıt sisteminin parçası olmak kaydıyla otomatik olmayan yollarla işleyen gerçek ve tüzel kişiler hakkında uygulanır."

yalnızca kişisel verileri işlenen gerçek kişileri koruma altına almakta olup, tüzel kişilere ait verilerin işlenmesini kapsamamaktadır. Ancak, bazı durumlarda tüzel kişilere ilişkin bilgiler, belirli bir gerçek kişinin kimliğinin belirlenmesini sağlayabilir. Bu gibi durumlarda, tüzel kişiye ait verilerin işlenmesi de KVKK hükümlerine tabi olacaktır. Örneğin, bir anonim şirketin müşterilerine sunduğu sadakat programı kapsamında, katılımcıların ad, soyad ve iletişim bilgilerinin kaydedilmesi, doğrudan gerçek kişilere ait bilgiler içerdiğinden KVKK kapsamında değerlendirilmelidir. Benzer şekilde, bir şirketin bayi ağı oluşturmak amacıyla bayilerinin yetkili temsilcilerine ait kimlik ve iletişim bilgilerini toplaması da bu bilgilerin belirli bir gerçek kişiyle ilişkilendirilebilir olması nedeniyle kanunun koruma alanına girecektir. Veri işleyen kişi gerçek kişi veya tüzel kişi olsa da KVKK'nın uygulanması açısından bir farklılık bulunmamaktadır. Ancak, herhangi bir veri kayıt sisteminin parçası olmaksızın veri işleyen kişiler bu kapsam dışında kalmaktadır[145]. Buna ek olarak, veri işleyen tüzel kişilerin hem özel hukuk tüzel kişileri (örneğin, şirketler, dernekler, vakıflar) hem de kamu tüzel kişileri (örneğin, belediyeler, bakanlıklar, kamu kurumları) olabileceği unutulmamalıdır[146].

### 2. Konu Bakımından Uygulama Alanı

KVKK'nın konu bakımından uygulama alanı, kişisel verilerin işlenme yöntemleri ve amaçları doğrultusunda şekillenmektedir. Kişisel verilerin korunmasına ilişkin düzenlemeler içeren iş bu kanun, veri sorumlularının yükümlülüklerini açıkça tanımlamaktadır. KVKK'nın uygulama alanı, kişisel verilerin işlenmesi ile sınırlıdır. KVKK yalnızca gerçek kişilere ait kişisel verileri kapsamaktadır. Tüzel kişilere (şirketler, dernekler, vakıflar vb.) ait bilgiler bu kanunun kapsamına girmemektedir[147]. Örneğin, bir anonim şirketin vergi numarası KVKK kapsamında değerlendirilmese de şirketin çalışanlarının kimlik bilgileri ve iletişim verileri KVKK'nın uygulama alanına girer. KVKK'nın uygulanabilmesi için kişisel verilerin otomatik veya kısmen

---

https://www.mevzuat.gov.tr/mevzuat?MevzuatNo=6698&MevzuatTur=1&MevzuatTertip=5 , (Erişim Tarihi: 08.02.2025).

[145] Seda Kuyumcu, *"6698 Sayılı Kişisel Verilerin Korunması Kanunu Kapsamında Kişisel Verilerin Yurt Dışına Aktarılması ve Aktarım Koşullarının Değerlendirilmesi"*, (Yüksek Lisans Tezi, Danışman Dr. Öğr. Üyesi Mehtap İpek İşleten, İstanbul, Galatasaray Üniversitesi Sosyal Bilimler Enstitüsü Özel Hukuk Anabilim Dalı Yayımlanmamış Yüksek Lisans Tezi, Mayıs 2024, (https://tez.yok.gov.tr/UlusalTezMerkezi/tezSorguSonucYeni.jsp), s.77.

[146] Kuyumcu, *op. cit.,* s. 77.

[147] Kişisel Verileri Koruma Kurulu'nun 19.11.2018 tarihli ve 2018/131 sayılı kararında, tüzel kişilere ait verilerin KVKK kapsamında olmadığı belirtilmiştir. Ayrıca, 6698 sayılı Kişisel Verilerin Korunması Kanunu'nun 2. maddesinde, Kanun hükümlerinin kişisel verileri işlenen gerçek kişiler ile bu verileri işleyen gerçek ve tüzel kişiler hakkında uygulanacağı belirtilmiştir. Bu kapsamda, Kanun'un koruma altına aldığı kişisel veriler yalnızca gerçek kişilere ait olup, tüzel kişilere ait veriler Kanun kapsamında değerlendirilmemektedir. https://kvkk.gov.tr/yayinlar/KİŞİSEL%20VERİLERİN%20KORUNMASI%20KANUNU%20VE%20UYGULAMASI.pdf, (Erişim Tarihi: 11.02.2025)

otomatik yollarla işlenmesi ya da otomatik yöntemler olmadan bir veri kayıt sisteminin parçası olması gerekmektedir (KVKK m.2). Bir veri, manuel olarak işleniyor olsa ve herhangi bir dijital sistem kullanılmasa dahi, eğer bir veri kayıt sistemi kapsamında yer alıyorsa, bu veriyi işleyen gerçek veya tüzel kişi hakkında KVKK hükümleri uygulanır[148]. Avrupa Birliği Adalet Divanı'nın Tietosuojavaltuutettu v. Jehovan todistajat davasında verdiği 10 Temmuz 2018 tarihli karar da bu hususu teyit eder niteliktedir. Kararda, Yehova Şahitleri cemaati üyelerinin ev ziyaretleri sırasında bireylerden topladığı bilgilerin merkezi bir veri tabanında tutulmamasına rağmen, bu faaliyetlerin cemaatin genel organizasyonu ve amacı doğrultusunda sistematik olarak yürütülmesi nedeniyle veri işlemenin kişisel veya evsel faaliyet istisnası dışında kaldığı ve dini cemaatin veri sorumlusu olarak değerlendirileceği ifade edilmiştir[149]. Benzer şekilde, Türk hukukunda da bir anonim şirketin bireylerden sistematik biçimde sağlık, finansal ya da sosyal nitelikli veriler toplaması hâlinde, bu veriler elle tutulsa dahi bir veri kayıt sisteminin parçası sayılacağından KVKK kapsamına girer. Dolayısıyla, veri işleme faaliyetinin mahiyeti, aracından çok, verinin sistematikliğine ve organizasyon içindeki kullanım amacına göre değerlendirilmelidir.

Bu duruma anonim şirketler nezdinde verilebilecek tipik bir örnek, işe alım süreçlerinde adaylardan toplanan fiziksel başvuru formlarıdır. Çoğu anonim şirket, iş başvurularını yalnızca dijital ortamda değil, aynı zamanda matbu formlar aracılığıyla da kabul etmektedir. Bu formlar, adayın adı, soyadı, iletişim bilgileri, eğitim durumu ve iş tecrübesi gibi kişisel veriler içermekte ve çoğu zaman alfabetik sıralama, başvuru tarihi ya da pozisyon bazlı kategorilere ayrılarak dosya dolaplarında muhafaza edilmektedir. Söz konusu başvuru formları herhangi bir otomatik veri işleme sistemine aktarılmasa dahi, sistematik bir şekilde sınıflandırılıp saklandıkları için veri kayıt sistemi kapsamında değerlendirilir. Bu bağlamda, başvuru formlarını işleyen anonim şirket, veri sorumlusu sıfatıyla Kanun hükümlerine tabi hale gelir[150].

KVKK, kişisel verilerin toplanması, kaydedilmesi, depolanması, değiştirilmesi, aktarılması, yok edilmesi ve anonimleştirilmesi gibi süreçleri kapsar. Bir anonim şirketin müşteri bilgilerini CRM (müşteri ilişkileri yönetimi) sisteminde saklaması veya çalışan maaşlarını dijital bir veri

---

[148] Sinem Göçmen Uyarer, *Kişisel Verilerin Korunması Kanunu ve Türk Ceza Kanunu Kapsamında Kişisel Verilerin Korunması,* Ankara, Seçkin Yayıncılık, 2. Baskı, 2020, s.104.

[149] Avrupa Birliği Adalet Divanı (ABAD), C-25/17, *Tietosuojavaltuutettu v. Jehovan todistajat – uskonnollinen yhdyskunta*, karar tarihi, 10.07.2018, ECLI: EU: C: 2018: 551, https://curia.europa.eu/juris/document/document.jsf?docid=203822&doclang=EN (E.T. 28.06.2025).

[150] Şirket, bu verileri işlerken KVKK'nın 10. maddesinde düzenlenen aydınlatma yükümlülüğünü, 12. maddede belirtilen veri güvenliğini sağlama yükümlülüğünü ve ilgili kişilerin haklarına (madde 11) yanıt verme yükümlülüğünü yerine getirmekle yükümlüdür.

tabanında tutması bu kanunun kapsamına girerken, yalnızca kişisel kullanım amacıyla tutulan bilgiler KVKK'ya tabi değildir.

KVKK'nın konu bakımından uygulama alanı kanunun 2. maddesi[151] ile, kişisel verileri işlenen gerçek kişiler ile bu verileri tamamen veya kısmen otomatik yollarla ya da bir veri kayıt sisteminin parçası olmak şartıyla manuel olarak işleyen gerçek ve tüzel kişilere uygulanacağı şeklinde hükme bağlanmaktadır. 6698 sayılı Kanun'da "kısmen veya tamamen otomatik işleme" kavramı açıkça tanımlanmamıştır. Ancak, 108 sayılı Avrupa Konseyi Sözleşmesi'ne[152] göre, otomatik işleme; verilerin kaydedilmesi, işlenmesi, değiştirilmesi, silinmesi veya dağıtılması gibi işlemlerin tamamen veya kısmen otomatik yöntemlerle gerçekleştirilmesini belirtmektedir. Kanun kapsamında, bir veri kayıt sisteminin parçası olmak kaydıyla manuel olarak işlenen kişisel veriler de korunmaktadır. Kanun'un 3. maddesinde[153], veri kayıt sistemi, belirli kriterlere göre yapılandırılmış bir kayıt düzeni olarak tanımlanmıştır. Bu nedenle, manuel olarak tutulan veriler belirli bir sistem içerisinde organize ediliyorsa KVKK uygulanır. Bununla birlikte, bu durum söz konusu verilerin kişisel veri niteliğini ortadan kaldırmaz ve hukuka aykırı işlemler, 5237 sayılı Türk Ceza Kanunu çerçevesinde hukuki sorumluluk doğurmaya devam eder[154].

Her ne kadar KVKK geniş bir uygulama alanına sahip olsa da bazı istisnalar bulunmaktadır. Bu haller kanunun 28. Maddesi ile hükme bağlanmış olup maddenin ilk fıkrası tamamen kanunun kapsam dışındaki halleri ifade ederken, 2. Fıkrası ise kısmen kanunun kapsam dışında bıraktığı halleri düzenlemektedir[155]. Kanunun 28. maddesinin 1. fıkrasında, bu kanunun kapsamı dışında kalan durumlar ayrıntılı olarak belirtilmiştir. Bu kapsamda gerçek kişiler tarafından, "yalnızca

---

[151] KVKK, "m.2: (1) Bu Kanun hükümleri, kişisel verileri işlenen gerçek kişiler ile bu verileri tamamen veya kısmen otomatik olan ya da herhangi bir veri kayıt sisteminin parçası olmak kaydıyla otomatik olmayan yollarla işleyen gerçek ve tüzel kişiler hakkında uygulanır.", *https://www.mevzuat.gov.tr/mevzuat?MevzuatNo=6698&MevzuatTur=1&MevzuatTertip=5*, (Erişim Tarihi: 08.02.2025).

[152] 28.01.1981'de Strazburg'da imzalanan ETS 108 Kişisel verilerin Otomatik İşleme Tabi Tutulması Karşısında Bireylerin Korunması Sözleşmesi, m.2: "otomatik işlem" den tamamen veya kısmen otomatik yöntemlerle gerçekleştirilen; verilerin kaydı, bu verilere mantıksal ve/veya aritmetik işlemlerin uygulanması, verilerin değiştirilmesi, silinmesi, geri elde edilmesi veya dağıtılması anlaşılır.", *https://inhak.adalet.gov.tr/Resimler/Dokuman/2712020140848108_tur.pdf* (Erişim Tarihi: 11.02.2025).

[153] KVKK, "m.3: (1/e) Kişisel verilerin işlenmesi: Kişisel verilerin tamamen veya kısmen otomatik olan ya da herhangi bir veri kayıt sisteminin parçası olmak kaydıyla otomatik olmayan yollarla elde edilmesi, kaydedilmesi, depolanması, muhafaza edilmesi, değiştirilmesi, yeniden düzenlenmesi, açıklanması, aktarılması, devralınması, elde edilebilir hâle getirilmesi, sınıflandırılması ya da kullanılmasının engellenmesi gibi veriler üzerinde gerçekleştirilen her türlü işlemi" ifade eder.

[154] KVKK, Kişisel Verilerin Korunması Kanununa İlişkin Uygulama Rehberi, *Https://Www.Kvkk.Gov.Tr/Icerik/4197/Kisisel-Verilerin-Korunmasi-Kanununa-Iliskin-Uygulama-Rehberi*, Erişim Tarihi: 09.02.2025, s.38-39.

[155] Göçmen Uyarer, *op. cit.,* s.105.

kendileri veya aynı evde birlikte yaşadıkları aile bireyleriyle ilgili faaliyetler çerçevesinde, üçüncü şahıslara aktarılmamak ve veri güvenliği kurallarına riayet edilmek kaydıyla kişisel verilerin işlenmesi, kişisel verilerin anonim hale getirilerek veya resmi istatistik çalışmaları kapsamında araştırma, planlama ve istatistik amaçları doğrultusunda kullanılması, milli savunma, kamu güvenliği, kamu düzeni, ekonomik güvenlik gibi hassas alanlara zarar vermemek, özel hayatın gizliliğini veya kişilik haklarını ihlal etmemek ve suç unsuru içermemek şartıyla, sanat, tarih, edebiyat veya bilimsel çalışmalar kapsamında ya da ifade özgürlüğü çerçevesinde kişisel verilerin işlenmesi, kanunla yetkilendirilmiş kamu kurum ve kuruluşlarının, kamu güvenliği, kamu düzeni, milli savunma ve ekonomik güvenliği sağlamak amacıyla gerçekleştirdiği önleyici, koruyucu ve istihbari faaliyetler kapsamında kişisel verileri işlemesi, yargı organları veya infaz kurumlarının, yargılama süreçleri, soruşturma, kovuşturma veya infaz işlemleri çerçevesinde kişisel verileri kullanması halleri" tamamıyla kanun kapsamı dışında tutulmuştur. Bu doğrultuda bazı hallerde işlenen veriler doğrudan kişisel veri niteliğinde olsa dahi kanunun koruma alanı dışında değerlendirilmektedir. Örneğin, kişisel veya ailevi amaçlarla işlenen veriler KVKK kapsamına girmez. Bireylerin özel hayatlarında sakladıkları kişisel veriler bu kapsamda değerlendirilmez. Anonim hale getirilmiş veriler, artık kişisel veri niteliği taşımadıkları için KVKK'nın uygulama alanı dışında kalmaktadır. Sadece kağıt ortamında tutulan veriler, eğer herhangi bir otomatik işleme tabi tutulmuyorsa, KVKK kapsamında değildir.

Kısmen kapsam dışında tutulan haller KVKK'nın 28. maddesinin 2. Fıkrasında düzenlenmiştir. Bu düzenlemeye göre, "kişisel verilerin işlenmesi belirli amaçlarla gerçekleştirildiğinde, Kanunun aydınlatma yükümlülüğünü düzenleyen 10. maddesi, zararların giderilmesini talep etme hakkı saklı kalmak kaydıyla ilgili kişi haklarını düzenleyen 11. maddesi ve Veri Sorumluları Siciline kayıt zorunluluğunu içeren 16. maddesi uygulanmaz[156]. Bu istisnalar yalnızca aşağıdaki durumlarla sınırlıdır:

- Suçların önlenmesi ve soruşturulması amacıyla veri işlenmesi: Örneğin, bir terör saldırısını önlemek amacıyla istihbarat teşkilatının şüpheli kişilerin iletişim verilerini işlemesi bu kapsama girer. Bu durumda, soruşturmanın gizliliği ve devletin güvenliği gibi nedenlerle ilgili kişilere aydınlatma yapılması veya bazı haklarının kullanılması kısıtlanabilir.

[156]KVKK, Kişisel Verilerin Korunması Kanununa İlişkin Uygulama Rehberi, *Https://Www.Kvkk.Gov.Tr/Icerik/4197/Kisisel-Verilerin-Korunmasi-Kanununa-Iliskin-Uygulama-Rehberi*, (Erişim Tarihi: 11.02.2025), s.43.

- İlgili kişinin kendisi tarafından kamuya açık hale getirilen kişisel verilerin işlenmesi: Örneğin, bir ünlü oyuncunun sosyal medya hesabında özel hayatına dair paylaştığı bilgilerin magazin basını tarafından haber yapılması bu duruma örnek teşkil eder. Ancak, bu verilerin sadece alenileştirme amacına uygun şekilde kullanılması ve farklı amaçlarla işlenmemesi gerekir

- Yetkili kamu kurumları ve meslek kuruluşlarının yasal görevleri kapsamında veri işlemesi: Denetim ve düzenleme görevlerini yerine getiren kamu kurumları ya da meslek kuruluşları, disiplin soruşturması veya kovuşturma kapsamında gerekli olduğu takdirde kişisel verileri işleyebilir. Örneğin, bir belediyenin imar planlarını hazırlarken vatandaşların kişisel verilerini işlemesi veya bir baro tarafından avukatların sicillerini tutması bu kapsamda değerlendirilir. Bu kurumlar, yasal görevlerini yerine getirirken belirli ölçüde kişisel veri işleme yetkisine sahiptir.

- Devletin mali ve ekonomik çıkarlarının korunması amacıyla veri işlenmesi: Kamu maliyesi, vergi düzenlemeleri ve bütçe yönetimiyle ilgili olarak devletin ekonomik dengesini korumaya yönelik gerçekleştirilen veri işleme faaliyetleri de bu kapsama dahildir. Örneğin, Maliye Bakanlığı'nın vergi kaçakçılığını önlemek amacıyla kişisel verileri analiz etmesi veya Merkez Bankası'nın enflasyonu kontrol etmek için ekonomik verileri işlemesi bu duruma örnek verilebilir. Bu türden veri işleme faaliyetleri, devletin mali ve ekonomik istikrarını sağlama amacına hizmet eder."

Bu istisnaların uygulanması, her zaman dikkatli bir şekilde yapılmalı ve orantılılık ilkesine uygun olmalıdır. Yani, kişisel veri işleme faaliyetinin amacı ile kısıtlanan haklar arasında dengeli bir ilişki olmalıdır. Aksi takdirde, kişisel verilerin korunması hakkı ihlal edilebilir.

**3. Yer Bakımından Uygulama Alanı**

KVKK'da, kişisel verilerin yurt dışına aktarılması konusunda kişi ve konu bakımından düzenlemeler bulunsa da yer bakımından uygulama alanı açıkça belirlenmemiştir. Türkiye'deki bireylerin kişisel verilerinin yurt içi veya yurt dışında işlenmesi durumunda hangi hukuki çerçevenin geçerli olacağı önemli bir tartışma konusudur. Kanun'un 2. maddesi uyarınca, veri sorumlusunun veya veri işleyenin Türkiye'de bulunup bulunmamasından bağımsız olarak, Türkiye'de kişisel verileri işlenen bireylerin korunması gerekmektedir. Ancak, Türkiye'de fiziksel varlığı bulunmayan ancak Türkiye'deki kişilere hizmet sunan veya onların kişisel verilerini işleyen şirketlerin KVKK kapsamında sorumlu tutulup tutulmayacağı hususu belirsizdir. Bu nedenle, mülkilik ilkesi gereği Türk hukukunun geçerli olduğu yerlerde

KVKK'nın da uygulama alanı bulacağı kabul edilmektedir[157]. Ayrıca, kişisel verilerin izinsiz işlenmesi haksız fiil teşkil ediyorsa, uluslararası özel hukuk ilkelerine başvurulabilir[158].

Kişisel verilerin yurt dışına aktarımında iki farklı durum söz konusudur[159]: İlk olarak, yurt dışında bulunan bir veri sorumlusunun Türkiye'de veri işlemesi halinde KVKK hükümlerine uyması gerekir. Ancak asıl sorun, verilerin Türkiye'de hukuka uygun şekilde toplanıp yurt dışına aktarıldıktan sonra hukuka aykırı biçimde işlenmesidir. Bu durumda, aktarım süreci KVKK'ya uygun olduğu sürece yurtiçindeki veri sorumlusuna karşı hukuki bir talep mümkün olmayabilir. Yurt dışındaki veri işleyene karşı yaptırım uygulanması da zor olduğundan, Kanun'un coğrafi uygulama alanının belirsizliği, ihlallerin önlenmesini güçleştirmektedir. Bu noktada, Avrupa Adalet Divanı'nın Google Spain kararı önemli bir referans noktası olabilir[160]. Bu kararda, Google Inc.'in AB içinde fiziksel olarak yerleşik olmasa bile, AB içinde faaliyet gösteren Google Spain aracılığıyla reklam ve pazarlama faaliyetleri yürütmesi nedeniyle AB veri koruma düzenlemelerine tabi olduğu kabul edilmiştir. Divan, kişisel veri işleme faaliyetinin doğrudan AB içindeki kuruluş tarafından gerçekleştirilmesi şartının aranmadığını, ancak bu kuruluşun faaliyetleri çerçevesinde verilerin işlenmesinin yeterli olduğunu vurgulamıştır[161]. Google Spain kararındaki yaklaşım, KVKK'nın yer bakımından uygulanmasını değerlendirirken de dikkate alınmalıdır. Türkiye'de doğrudan bir tüzel kişiliği bulunmasa da Türkiye'deki bireylere yönelik hizmet sunan veya onların kişisel verilerini işleyen yabancı şirketlerin KVKK'ya tabi olması gerektiği sonucuna ulaşılabilir. Bu kapsamda, Türkiye'de faaliyet gösteren veya Türkiye'deki bireylerin verilerini işleyen yabancı şirketlerin KVKK hükümlerine uygun hareket etmesi gerektiği yönünde bir düzenleme ve uygulama geliştirilmesi, kişisel verilerin korunması açısından önem arz etmektedir. Örneğin, Türkiye'deki müşterilere yönelik online satış yapan ve verilerini yurt dışındaki sunucularda işleyen bir şirket düşünelim. Bu durumda, şirketin Türkiye'de bir temsilciliği veya ofisi bulunmasa bile, Türkiye'deki müşterilerin verilerini işlediği için KVKK hükümlerine uymak zorundadır.

---

[157] Seda Kuyumcu, *op. cit.,* s.79.
[158] Mesut Serdar Çekin, *Avrupa Birliği Hukukuyla Mukayeseli Olarak 6698 Sayılı Kanun Çerçevesinde Kişisel Verilerin Korunması Hukuku,* İstanbul, On İki Levha Yayıncılık, 3. Baskı, 2020, s.33.
[159] *Ibid.,* s.33.
[160] Bu karar, Avrupa Adalet Divanı tarafından verilmiş olup, arama motorlarının Avrupa Birliği veri koruma mevzuatına tabi olduğuna hükmetmiştir. Karar, bir İspanyol vatandaşının Google'da kendi adıyla yapılan aramalarda çıkan eski bir haberin kaldırılması talebi üzerine verilmiştir. Mahkeme, Google'ın İspanya'da bir şubesinin bulunması nedeniyle Avrupa Birliği veri koruma yasalarının Google'a uygulanabileceğine karar vermiştir. https://dergipark.org.tr/en/download/article-file/1671800 E.T:14.02.2025)
[161] Mesut Serdar Çekin, *op. cit.,* s.34.

Avrupa Adalet Divanı'nın (AAD) Google Spain kararına benzer şekilde, Fashion ID[162] davası da kişisel verilerin işlenmesi sürecine dahil olan birden fazla tarafın müşterek veri sorumlusu olup olmayacağı ve bir şirketin Avrupa Birliği (AB) sınırları içinde yerleşik olup olmamasına bakılmaksızın veri koruma düzenlemelerine tabi olup olmayacağı konularında önemli bir içtihat oluşturmuştur. Bu karar, KVKK'nın yer bakımından uygulanması açısından da dikkate alınması gereken bir örnek teşkil etmektedir. Fashion ID davasında, Almanya merkezli çevrimiçi perakende şirketi Fashion ID, web sitesine Facebook'un "Beğen" butonunu entegre etmiştir. Bu entegrasyon, ziyaretçilerin kişisel verilerinin, ziyaretçi Facebook üyesi olmasa veya butona tıklamasa bile, Facebook'a aktarılmasına neden olmuştur. AAD, Fashion ID'nin, Facebook ile birlikte müşterek veri sorumlusu olduğuna karar vermiştir. Bu karar, bir web sitesinin, üçüncü taraf eklentileri kullanarak ziyaretçilerinin kişisel verilerini toplaması durumunda, veri sorumluluğunun nasıl değerlendirileceğine dair önemli bir içtihat oluşturmaktadır[163].

Fashion ID kararında, bir şirketin yalnızca AB içinde fiziksel olarak yerleşik olması değil, aynı zamanda AB vatandaşlarının kişisel verilerini işleme faaliyeti gerçekleştirmesi halinde de GDPR kapsamında sorumluluk taşıyabileceği kabul edilmiştir. Benzer bir yorum KVKK açısından da benimsenirse, Türkiye'de fiziksel varlığı bulunmasa dahi Türkiye'deki bireylerin kişisel verilerini işleyen şirketlerin KVKK hükümlerine tabi olması gerektiği sonucuna ulaşılabilir. Bu çerçevede, özellikle yabancı şirketlerin Türkiye'deki veri işleme faaliyetlerini değerlendirirken, bu şirketlerin Türkiye'deki bireylere yönelik ürün ve hizmet sunup sunmadığı, Türkiye'de herhangi bir temsilciliği olup olmadığı veya Türkiye'de bulunan bireyleri hedefleyerek kişisel veri işleyip işlemediği gibi unsurlar dikkate alınmalıdır. KVKK'nın yer bakımından uygulanma alanının geniş yorumlanması, Türkiye'deki veri sahiplerinin korunması açısından daha etkili bir yaklaşım olacaktır. Fashion ID kararı, Türkiye'deki uygulamalar açısından da önemli bir referans noktasıdır. Özellikle, Türkiye'de faaliyet gösteren şirketlerin web sitelerinde üçüncü taraf eklentileri kullanırken, ziyaretçilerin kişisel verilerinin korunması konusunda dikkatli olmaları gerekmektedir. Bu tür durumlarda, ilgili şirketler KVKK

[162]Fashion ID Kararı ABAD - C-40/17 - Moda Kimliği, https://gdprhub-eu.translate.goog/index.php?title=CJEU_-_C-40/17_-_Fashion_ID&_x_tr_sl=en&_x_tr_tl=tr&_x_tr_hl=tr&_x_tr_pto=tc, https://curia.europa.eu/juris/document/document.jsf?text=&docid=216555&doclang=EN, (E.T:14.02.2025)

[163]Avrupa Birliği Adalet Divanı'ndan Müşterek Veri Sorumluluğuna İlişkin Karar, https://www.gsghukuk.com/tr/yayinlar/kose-yazilari/avrupa-birligi-adalet-divanindan-musterek-veri-sorumluluguna-iliskin-karar-yazilarimiz.pdf E.T:14.02.2025.

kapsamında veri sorumlusu olarak kabul edilebilir ve kanun çerçevesinde belirlenen yükümlülüklere tabi olabilirler.

### B. KİŞİSEL VERİLERİN YURT DIŞINA AKTARIMI SÜRECİNE İLİŞKİN İŞLEME ŞARTLARI

6698 sayılı Kişisel Verilerin Korunması Kanunu'nun, 12 Mart 2024 tarihli ve 32487 sayılı Resmî Gazete' de yayımlanan 7499 sayılı Kanun'un 34. maddesi ile değiştirilen 9. maddesi, kişisel verilerin yurt dışına aktarılmasına ilişkin usulü yeniden düzenlemiştir. Eski düzenleme kapsamında, kişisel verilerin yurt dışına aktarımı kural olarak ilgili kişinin açık rızasına dayanıyordu. Bununla birlikte, ilgili kişinin açık rızası olmaksızın veri aktarımı yapılabilmesi için KVKK'nın 5. ve 6. maddelerinde belirtilen veri işleme şartlarının mevcut olması ve Kişisel Verileri Koruma Kurulu tarafından, verilerin aktarılacağı ülkenin yeterli koruma düzeyine sahip olduğunu gösteren bir "yeterlilik kararı" alınması gerekiyordu. Aktarımın gerçekleştirileceği ülke için yeterlilik kararı bulunmaması hâlinde ise, veri sorumlularının yeterli koruma sağladıklarına dair taahhütte bulunmaları ve Kurulun onayını almaları şart koşulmaktaydı. Ancak, bu düzenleme uygulamada çeşitli zorluklara yol açmış ve kişisel verilerin yurt dışına aktarımı konusunda belirsizlikler doğurmuştur[164]. KVKK her ne kadar GDPR ile uyumlanmaya çalışılsa da Türkiye'deki kanunların GDPR kadar kapsamlı ve detaylı olmayışı, yeterlilik kararlarının uzun ve detaylı değerlendirme süreçleri, siyasi ve ekonomik faaliyetler Türkiye hakkında yeterlilik kararı verilmemesine sebep olmuştur. Üstelik kurulun yayınladığı kararlara göre 80'den fazla taahhütname başvurusu yapılmasına rağmen bu başvurulardan yalnızca 8 tanesinin kurul tarafından onaylanıp geçerli kılınması, yurt dışına veri aktarımının uygulamada neredeyse sadece açık rıza ile yapılabilmesine yol açmıştır. Bu durum ülkemizde kişisel verilerin yurt dışına aktarılması konusunda büyük zorluklar yaratmış ve şirketlerin, özellikle bulut tabanlı hizmetler kullanan firmaların, hukuka uygun veri aktarımı yapmasını olanaksızlaştırdığı gibi şirketlerin ticari faaliyetleri olumsuz etkilenmiş ve yatırımları engelleyen bir sorun haline gelmiştir. KVKK Reform Yasası ile, Avrupa Birliği'nin 2018'de kabul ettiği GDPR'ın hükümleri göz önünde bulundurularak, kişisel verilerin Avrupa Birliği dışına aktarılmasına yönelik yeni düzenlemeler yapılmıştır. Bu düzenlemeler, teknoloji ve dijitalleşmenin hızla gelişen yapısını ve ticari hayatın dinamiklerini dikkate alarak, aynı zamanda kişisel verilerin korunmasını sağlamayı hedeflemektedir[165].

---

[164] Mehmet Bedi Kaya, "KVKK Reformu 2024 Değişiklikleri", Dijital Baskı v1.0- Mart 2024, s.25. *https://mbkaya.com/hukuk/kvkk-reformu.pdf,* (Erişim Tarihi:13.01.2025).
[165] *Ibid.,* s.26.

Kurulun yayımladığı "Kişisel Verilerin Yurt Dışına Aktarılma Rehberinde" kişisel verilerin yurt dışına aktarılması faaliyeti üç farklı kriter üzerinden tanımlanmıştır[166]:

*"1) Veri sorumlusu ya da veri işleyen (veri aktaran) söz konusu kişisel veri işleme faaliyeti için Kanuna tabi olmalıdır.*

*2) Veri aktaran tarafından işlenen kişisel veriler, iletilmeli veya başka bir suretle erişilebilir hale getirilmelidir.*

*3) Veri aktarılan veri sorumlusu ya da veri işleyen, Kanuna tabi olup olmadığına bakılmaksızın üçüncü bir ülkede olmalıdır."*

Bu üç kriter, kişisel verilerin yurt dışına aktarılması işleminin hukuki zeminini oluşturmaktadır.

KVKK'nın yeniden düzenlenen 9. Madde[167]'sine göre kişisel verilerin yurt dışına aktarılabilmesi için öncelikle KVKK'nın 5. ve 6. maddelerinde belirtilen kişisel veri işleme şartlarından en az birinin mevcut olması gerekmektedir. Ayrıca, kişisel verilerin aktarılacağı ülke, sektör veya uluslararası kuruluş hakkında Kişisel Verileri Koruma Kurulu tarafından yeterli koruma sağladığına dair bir yeterlilik kararı alınmış olmalıdır. Yeterlilik kararı, Resmî Gazete' de yayımlanarak yürürlüğe girer ve en geç dört yılda bir değerlendirilerek gerekli görülmesi halinde değiştirilir, askıya alınır veya kaldırılabilir. Eğer aktarılacak ülke hakkında yeterlilik kararı bulunmuyorsa, veri aktarımının gerçekleşebilmesi için belirli güvencelerin

---

[166] KVKK, *"Kişisel Verilerin Yurt Dışına Aktarılması Rehberi*", KVKK Yayınları no:48, Ocak 2025, s.13-19, https://www.kvkk.gov.tr/Icerik/8142/Kisisel-Verilerin-Yurt-Disina-Aktarilmasi-Rehberi, (Erişim Tarihi: 13.01.2025)

[167] MADDE 9- (1) Kişisel veriler, 5 inci ve 6 ncı maddelerde belirtilen şartlardan birinin varlığı ve aktarımın yapılacağı ülke, ülke içerisindeki sektörler veya uluslararası kuruluşlar hakkında yeterlilik kararı bulunması halinde, veri sorumluları ve veri işleyenler tarafından yurt dışına aktarılabilir.
(2) Yeterlilik kararı, Kurul tarafından verilir ve Resmî Gazete'de yayımlanır. Kurul, ihtiyaç duyması halinde ilgili kurum ve kuruluşların görüşünü alır. Yeterlilik kararı, en geç dört yılda bir değerlendirilir. Kurul, değerlendirme sonucunda veya gerekli gördüğü diğer hallerde, yeterlilik kararını ileriye etkili olmak üzere değiştirebilir, askıya alabilir veya kaldırabilir.
(3) Yeterlilik kararı verilirken öncelikle aşağıdaki hususlar dikkate alınır:
a) Kişisel verilerin aktarılacağı ülke, ülke içerisindeki sektörler veya uluslararası kuruluşlar ile Türkiye arasında kişisel veri aktarımına ilişkin karşılıklılık durumu.
b) Kişisel verilerin aktarılacağı ülkenin ilgili mevzuatı ve uygulaması ile kişisel verilerin aktarılacağı uluslararası kuruluşun tâbi olduğu kurallar.
c) Kişisel verilerin aktarılacağı ülkede veya uluslararası kuruluşun tâbi olduğu bağımsız ve etkin bir veri koruma kurumunun varlığı ile idari ve adli başvuru yollarının bulunması.
ç) Kişisel verilerin aktarılacağı ülkenin veya uluslararası kuruluşun, kişisel verilerin korunmasıyla ilgili uluslararası sözleşmelere taraf veya uluslararası kuruluşlara üye olma durumu.
d) Kişisel verilerin aktarılacağı ülkenin veya uluslararası kuruluşun, Türkiye'nin üye olduğu küresel veya bölgesel kuruluşlara üye olma durumu.
e) Türkiye'nin taraf olduğu uluslararası sözleşmeler.

sağlanması gerekir. Bu kapsamda, Kurul tarafından belirlenen standart sözleşmelerin taraflar arasında imzalanarak Kurul'a bildirilmesi, çok uluslu şirket grupları için bağlayıcı şirket kurallarının benimsenmesi, kamu kurumları ile yabancı ülkeler arasındaki anlaşmalar veya Kurul tarafından belirlenen diğer uygun güvenceler sağlanmalıdır. Ancak, bu şartların hiçbirinin karşılanamadığı durumlarda kişisel verilerin yurt dışına aktarılması ancak belirli istisnai hallerde mümkün olabilir. Bu istisnalar arasında ilgili kişinin açık rızasının bulunması, kanunlarda açıkça öngörülmesi, fiili imkânsızlık nedeniyle rızası alınamayan kişilerin hayatı veya beden bütünlüğünün korunması için aktarımın zorunlu olması, bir sözleşmenin kurulması veya ifasıyla doğrudan ilgili olması, veri sorumlusunun hukuki yükümlülüğünü yerine getirebilmesi için aktarımın gerekli olması, bir hakkın tesisi, kullanılması veya korunması amacıyla veri işlenmesinin zorunlu olması ya da ilgili kişinin temel hak ve özgürlüklerine zarar vermemek kaydıyla veri sorumlusunun meşru menfaatleri için işlemenin gerekli olması yer almaktadır.

Kişisel verilerin yurt dışına aktarılmasını meşru kılan nedenlerden biri de ilgili kişinin açık rızasının alınmasıdır. Dolayısıyla, açık rızaya ilişkin yapılan açıklamalar bu bağlamda da geçerliliğini koruyacaktır. Ancak, burada bilgilendirmenin kapsamına özel bir vurgu yapmak gerekmektedir. Şöyle ki, yalnızca ilgili kişiye verilerinin yurt dışına aktarılabileceğini bildirmek yeterli olmayacaktır. Bunun yanı sıra, verilerin hangi amaçlarla, hangi ülkelere aktarılacağı, hangi yöntemlerle saklanacağı ve kimlerle paylaşılacağı hususlarının da açık, anlaşılır ve kategorik bir şekilde belirtilmesi gerekmektedir[168]. Böylece, ilgili kişinin bilgilendirilmiş ve açık bir şekilde rıza göstermesi sağlanacaktır. Tüm bu düzenlemeler, kişisel verilerin yurt dışına aktarılması sürecinde veri güvenliğini sağlamak ve ilgili kişilerin haklarını korumak amacıyla getirilmiştir. Özellikle Türkiye'de fiziksel varlığı bulunmayan ancak Türkiye'deki bireylerin kişisel verilerini işleyen şirketlerin de KVKK'ya tabi olup olmadığı konusu, bu yeni düzenlemeler ışığında daha net bir şekilde değerlendirilmesi gerekmektedir.

[168] Mesut Serdar Çekin, *op. cit.,* s.131.

## C. YURT DIŞINA KİŞİSEL VERİ AKTARIMINDA ARANAN EK ŞARTLAR

Kişisel verilerin yurt dışına aktarımı, 6698 sayılı Kişisel Verilerin Korunması Kanunu'nun 9. maddesi ile düzenlenmiş olup, aktarımın temel koşulları kanunda açıkça belirtilmiştir. Ancak, bu temel koşulların yanında, kişisel verilerin güvenliği ve ilgili kişilerin haklarının korunması amacıyla Kanunda "ek şartlar" olarak adlandırılan ilave düzenlemeler de getirilmiştir. "Ek şartlar" ifadesi, temel yasal zorunlulukların ötesinde, aktarımın güvenli, şeffaf ve mevzuata uygun şekilde gerçekleştirilmesini sağlamak amacıyla getirilen, özel ve tamamlayıcı önlemleri ifade etmektedir. Bu şartlar, veri sorumlularının yurt dışına veri aktarırken yerine getirmeleri gereken yükümlülükleri detaylandırır ve risklerin azaltılmasını amaçlar. Bu bağlamda, yurt dışına kişisel veri aktarımında "temel koşulların" yanında, veri güvenliğinin sağlanması, açık rıza alınması, yeterlilik kararı gibi önlemlerin ve ayrıca standart sözleşme hükümleri veya bağlayıcı şirket kuralları gibi hukuki mekanizmaların kullanılması gibi ek şartlar gündeme gelmektedir. Bu başlıkta konu temel hatlarıyla ele alınacak, aşağıda bu ek şartlar, kapsamlı biçimde ele alınarak açıklanacaktır.

Yurt dışına kişisel verilerin aktarılması sürecinde değişiklik öncesinde m.9/2 ile düzenlenen şartlar, değişen kanun ile yeniden ele alınmış ve aktarım için üç ayrı seçenek öngörülmüştür[169]:

1.Yeterlilik kararı ile veri aktarımı (m.9/1-2-3)

2. Uygun güvence sağlayarak veri aktarımı (m.9/4-5)

3. İlk iki durumun sağlanamadığı hallerde arızi durumlar kapsamında veri aktarımı (m.9/6)

Kişisel Verileri Koruma Kurulu, belirli ülkelerin yeterli koruma seviyesine sahip olduğunu belirleyebilir. Bu durumda, ilgili ülkelere veri aktarımı için ilgili kişinin açık rızası aranmaksızın, Kanun'un 5. maddesinin 2. fıkrası ile 6. maddesinin 3. fıkrasında belirtilen şartlardan birinin varlığı yeterlidir. Eğer veri aktarılacak ülkede yeterli koruma bulunmuyorsa, veri sorumluları veya veri işleyenler uygun güvenceler sağlamak zorundadır. Bu güvenceler, Kurul tarafından onaylanan bağlayıcı şirket kuralları veya veri aktarım taahhütnameleri gibi araçlarla tesis edilebilir. Bu durumda, ilgili kişinin açık rızası aranmaksızın, Kanun'un 5. maddesinin 2. fıkrası ile 6. maddesinin 3. fıkrasında belirtilen şartlardan birinin varlığı yeterlidir. Yukarıdaki şartların sağlanamadığı durumlarda, kişisel verilerin yurt dışına aktarımında daha esnek ve uyumlu bir yaklaşım benimseyerek, veri sorumlularının uluslararası

[169] Kaya, *op. cit.,* s.30, https://mbkaya.com/hukuk/kvkk-reformu.pdf, (Erişim Tarihi:13.01.2025).

veri transferlerini daha etkin bir şekilde gerçekleştirmelerine olanak tanımaktadır[170]. Bazı istisnai hallerde, yeterlilik kararı veya uygun güvence sağlanamasa bile kişisel veri aktarımı mümkün olabilir. Bu durumlar, ilgili kişinin açık rızasının alınması, sözleşme gerekliliklerinin yerine getirilmesi, kamu yararı veya hukuki hakların tesisi gibi özel şartlara bağlıdır. Ancak, bu tür aktarımlar istisnai niteliktedir. Bu üç yöntem, KVKK kapsamında yurt dışına veri aktarımının hukuki çerçevesini oluşturmakta ve veri sahiplerinin haklarını koruma altına almayı amaçlamaktadır. Kanun metninde, bu yöntemler arasında hiyerarşik bir sıralama olduğuna dair herhangi bir hüküm bulunmamaktadır[171]. Dolayısıyla, veri sorumluları ve işleyenler, her bir duruma uygun olan yöntemi seçmekte serbesttirler. Yeni düzenlemeyle birlikte, kişisel verilerin uluslararası dolaşımı daha sıkı kurallara bağlanarak denetim mekanizmaları güçlendirilmiştir.

### D. 108 SAYILI SÖZLEŞME'NİN YURT DIŞINA AKTARIMA ETKİSİ

Kişisel verilerin korunması alanındaki en kapsamlı ilk uluslararası sözleşme, Avrupa Konseyi'nin 1970'li yıllardan itibaren yürüttüğü çalışmaların sonucu olarak 28 Ocak 1981'de Strazburg'da imzalanan "Kişisel Verilerin Otomatik İşlenmesine Karşı Bireylerin Korunması Sözleşmesi"dir. Bu sözleşme 1 Ekim 1985'te yürürlüğe girmiştir. Türkiye, söz konusu sözleşmeyi imzalayan ilk ülkeler arasında yer almakta olup, 17 Mart 2016 tarihli ve 29656 sayılı Resmi Gazetede yayımlanarak iç hukuk sistemine dahil edilmiştir. Günümüzde 108 sayılı Sözleşme olarak bilinen bu düzenlemenin temel amacı, üye ülkelerde yaşayan veya vatandaşlık durumuna bakılmaksızın herkesin kişisel verilerinin otomatik işlenmesine karşı özel hayatının korunmasını hedeflemektedir. Ayrıca bu sözleşme, kişisel verilerin korunması hakkını Avrupa İnsan Hakları Sözleşmesi'nin 8. maddesinde yer alan özel hayatın gizliliği ilkesine dayandırmaktadır. Sözleşme, kişisel verilerin aktarıldığı ülkede de yeterli bir koruma düzeyinin sağlanmasını öngörmektedir. Kişisel verilerin yurt dışına aktarılacağı durumlarda, veri sorumlusunun veri sahiplerini bilgilendirme yükümlülüğü vardır. Veri sahiplerinin, kişisel verileri hakkında bilgi alma, düzeltme, silme gibi hakları korunur. Bu haklar, yurt dışına aktarılan veriler için de geçerlidir. Ayrıca sözleşme, veri aktarımının kişinin temel hak ve özgürlüklerini ihlal edeceği durumlarda aktarımın yasaklaması söz konusu olabilir. Üye devletlerin kişisel verilerin korunmasını denetlemek için bağımsız bir otorite kurmalarını ve bu otoritelerin, yurt dışına veri aktarımlarını da denetlemelerini öngörmektedir.

---

[170] https://www.kvkk.gov.tr/Icerik/4106/Kisisel-Verilerin-Yurtdisina-Aktarilmasi (Erişim Tarihi: 04.03.2025).

[171] Işıl Çelik, *6698 Sayılı Kişisel Verilerin Korunması Kanunu ve 2016/679 Sayılı Avrupa Birliği Genel Veri Koruma Tüzüğü Kapsamında Kişisel Verilerin Yurt Dışına Aktarılması*, On İki Levha Yayıncılık, 2022, s.60.

Kişisel Verileri Koruma Kurulu'nun 22/07/2020 tarih ve 2020/559 sayılı kararı, otomotiv sektöründe faaliyet gösteren bir şirketin kişisel verileri yurt dışına aktarmasıyla ilgili yapılan bir şikayet üzerine verilmiştir. Karar, özellikle 108 sayılı Sözleşme açısından önemli bir dönüm noktası olmuştur[172]. Kurul, 108 Sayılı Sözleşmeye taraf olmanın tek başına kişisel verilerin yurt dışına aktarımı için yeterli bir gerekçe olmadığını belirtmiştir. Sözleşme, genel bir çerçeve sunarken, KVKK'nın belirlediği diğer şartların da sağlanması gerektiği vurgulanmıştır. Verilerin aktarıldığı ülkede yeterli koruma düzeyinin olduğunun kanıtlanması gerekmektedir. 108 Sayılı Sözleşme 'ye taraf olmanın bu kanıtı tek başına oluşturmayacağı belirtilmiştir.

Sonuç olarak, kurul kararlarına göre 108 Sayılı Sözleşme, kişisel verilerin korunması konusunda önemli bir uluslararası sözleşme olup temel bir çerçeve sunsa da Türkiye'de kişisel verilerin yurt dışına aktarımı için önemlidir fakat tek başına yeterli bir dayanak değildir. Veri sorumluları, kişisel verileri yurt dışına aktarırken hem 108 Sayılı Sözleşmeyi hem de KVKK hükümlerini göz önünde bulundurarak hareket etmelidirler. Bu karar, kişisel veri koruma hukuku alanında çalışanlar, veri sorumluları ve bireyler için önemli bir emsal teşkil etmektedir.

[172] KVKK, Kişisel Verilerin 108 Sayılı Sözleşme Dayanak Gösterilerek Yurt Dışına Aktarılması Hakkında Kişisel Verileri Koruma Kurulu'nun 22/07/2020 tarih ve 2020/559 sayılı Karar Özeti, *https://www.kvkk.gov.tr/Icerik/6790/2020-559*, (Erişim Tarihi:14.01.2025).

## III. AKTARIM GERÇEKLEŞTİRELECEK ÜLKEDE YETERLİ KORUMANIN BULUNMASI

6698 sayılı Kişisel Verilerin Korunması Kanunu'nun 9. maddesi, kişisel verilerin yurt dışına aktarımına ilişkin temel şartları belirlerken, aktarımın yapılacağı ülke veya uluslararası kuruluşta yeterli korumanın bulunması hususunu önemli bir güvence unsuru olarak ön plana çıkarmıştır. Bu bağlamda, yurt dışı veri aktarımında hukuka uygunluğun sağlanması için, Kanun tarafından öngörülen hukuki dayanaklardan birinin mevcut olması gerekir. Bunlar arasında, özellikle yeterlilik kararı kavramı kritik bir rol oynamaktadır. Yeterlilik kararı, aktarım yapılacak ülkenin kişisel verilerin korunmasına ilişkin mevzuatının KVKK ile uyumlu ve veri sahiplerinin haklarının yeterince korunuyor olduğunun tespiti anlamına gelir. Bu karar, veri sorumlularına yurt dışına güvenli ve hukuki çerçevede veri aktarımı yapma imkânı sağlar.

Bu bölümde, öncelikle yurt dışına veri aktarımının hukuka uygunluk nedenleri kapsamında değerlendirilen temel şartlar ele alınacak; ardından, KVKK'nın 9. maddesinin birinci, ikinci ve üçüncü fıkralarında düzenlenen yeterlilik kararı kavramı ayrıntılı şekilde incelenecektir.

### 1. HUKUKA UYGUNLUK NEDENLERİNDEN BİRİNİN VARLIĞI

7499 sayılı Kanun ile değiştirilen KVKK'nın 9. maddesi, yurt dışına veri aktarımına ilişkin önemli bir değişiklik getirmiştir. Önceki düzenlemede, yalnızca KVKK'nın 5/2 ve 6/3 maddelerine yapılan atıf, yeni düzenleme ile genişletilmiş ve KVKK'nın 5. ve 6. maddelerinin tamamını kapsayacak şekilde yeniden ele alınmıştır. Bu değişiklik, özellikle özel nitelikli kişisel verilerin yurt dışına aktarımı açısından dikkate değerdir.[173]

KVKK m.9/1 kapsamında, kişisel verilerin yurt dışına aktarımı için iki temel şart olarak düzenlenen; aktarım gerçekleştirilecek ülkede yeterli korumanın bulunması ve KVKK m.5/2 ve m.6/3'te belirtilen hukuka uygunluk nedenlerinden birinin varlığı şartları, Avrupa Birliği Genel Veri Koruma Tüzüğü'nde ile benzerlik göstermektedir[174]. GDPR'da kişisel verilerin Avrupa Ekonomik Alanı dışına aktarımı 45. ve 46. maddelerde düzenlenmiştir. GDPR'da kişisel verilerin yurt dışına aktarımına ilişkin hukuka uygunluk nedenleri, genel veri işleme şartlarıyla bağlantılıdır. Özellikle KVKK m.9 ve GDPR m.45-49, yurt dışına aktarım mekanizmalarını düzenler ve KVKK m.5 ile m.6 ve GDPR m.6 ile m.9'da belirtilen hukuka

[173] Kuyumcu, op. cit., s. 103.
[174] Kişisel Verilerin Korunması Kanunu, m.9/1; Avrupa Birliği Genel Veri Koruma Tüzüğü (GDPR), Madde 44 ve devamı.

uygunluk nedenlerine dayanmaktadır. Eğer yurt dışına aktarım yapılacak ülkede yeterli koruma bulunmuyorsa, aktarımın gerçekleşebilmesi için KVKK m.5/2'deki (GDPR m.6'ya denk düşmektedir) ve KVKK m.6/3'teki (GDPR m.9/2'ye denk düşmektedir) hukuki dayanaklardan en az biri bulunmalıdır. GDPR m.49/1-a, açık rızanın yurt dışına veri aktarımı için istisnai bir yol olarak kullanılmasına izin vermektedir. KVKK m.9/3 de benzer şekilde açık rızayı bir istisna olarak düzenlemiştir. GDPR, özellikle tıbbi amaçlar, bilimsel araştırmalar ve kamu yararı için geniş kapsamlı istisnalar tanırken, KVKK bu alanlarda daha kısıtlayıcıdır. GDPR m.46, Standart Sözleşme Maddeleri (SCC) gibi belirli hukuki araçlar sunarken, KVKK m.9/2 daha genel bir "uygun güvenceler" yaklaşımını benimsemektedir.

Eğer kişisel verilerin aktarılacağı ülkede yeterli koruma bulunuyorsa ve KVKK'nın 5. ve 6. maddelerinde belirtilen veri işleme şartlarından biri mevcutsa, anonim şirketler ilgili kişinin açık rızasını almadan veri aktarımını gerçekleştirebilirler. Bu bağlamda, Kurul tarafından yeterli korumaya sahip olduğu belirlenen ülkeler listesi henüz resmi olarak yayımlanmamıştır. Dolayısıyla, şu an için yeterli koruma bulunan ülkelere yönelik spesifik Kurul kararları mevcut değildir.

Özellikle, özel nitelikli kişisel verilerin yurt dışına aktarımında, artık KVKK'nın 6/4 maddesinde belirtilen ve Kişisel Verileri Koruma Kurulu tarafından ilan edilen yeterli önlemlerin alınması zorunlu hale gelmiştir. Önceki uygulamada, bu durum yorum yoluyla değerlendiriliyordu. Ancak yeni düzenleme ile bu husus açıkça kanuni çerçeveye oturtulmuştur.[175] Buna göre, özel nitelikli kişisel verilerin yurt dışına aktarımında, yalnızca işleme şartlarının sağlanması yeterli olmayıp, aynı zamanda Kurul tarafından belirlenen güvenlik tedbirlerinin de eksiksiz şekilde uygulanması gerekmektedir. Bu değişiklik, veri güvenliğini artırmayı ve uluslararası veri transferlerinde daha sıkı bir hukuki çerçeve oluşturmayı amaçlamaktadır.

Sonuç olarak, yeterli koruma bulunan ülkelere kişisel veri aktarımı için Kurul izni gerekmemekte ve uygun güvenceler aranmasına gerek bulunmamaktadır. Ancak, yeterli koruma bulunan ülkeler listesi henüz yayımlanmadığı için, veri sorumluları mevcut durumda uygun güvenceler yoluyla veri aktarımını gerçekleştirmelidir.

[175] Kuyumcu, op. cit., s. 103.

KVKK m.5/f.2, m.6/f.3 ve m.6/f.4'te yer alan hukuka uygunluk nedenleri, çalışmamızın önceki bölümlerinde detaylı bir şekilde ele alındığından, bu kısımda yalnızca bu açıklamalara atıfta bulunulacaktır.[176]

### 2. YETERLİLİK KARARI (m.9/1-2-3)

Kişisel verilerin yurt dışına aktarılması, hukuka uygun bir çerçevede gerçekleştirilmelidir. kişisel verilerin yurt dışına aktarımı konusunda açık rızanın bulunmadığı durumlarda, yalnızca Kanun'un 5. ve 6. maddelerinde belirtilen hukuki şartların sağlanması yeterli olmayıp, verilerin aktarılacağı ülkenin veya ilgili sektörlerin yeterli koruma seviyesine sahip olması gerekmektedir. Bu yeterlilik değerlendirmesi, Kişisel Verileri Koruma Kurulu tarafından yapılmaktadır. Nitekim Kurul, "Yeterli Korumaya Sahip Ülkelerin Belirlenmesinde Esas Alınacak Kriterler[177]" hakkında bir karar yayımlamış olmakla birlikte[178], bu çalışma tarihi itibariyle güvenli ülke listesi henüz ilan edilmemiştir. Eğer verilerin aktarılacağı ülkede yeterli koruma bulunmuyorsa, ilgili ülkelerdeki veri sorumlularının yeterli korumayı yazılı olarak taahhüt etmeleri ve Kurul'dan izin almaları gerekmektedir.[179]

Kanun'un güncellenen 9. maddesi, yeterlilik kararlarının sadece ülkeler bazında değil, belirli sektörler ya da uluslararası kuruluşlar özelinde de verilebilmesine imkân tanımaktadır. Böylece, bir ülkenin genel veri koruma düzenlemeleri yetersiz bulunsa bile, o ülkedeki belirli sektörlerin veya kurumların gerekli güvenlik standartlarını sağlaması hâlinde veri aktarımı mümkün olabilecektir. Yeterlilik kararlarının alınma süreci, Kişisel Verileri Koruma Kurulu'nun detaylı değerlendirmelerine dayanmakla birlikte, bu değerlendirmelerde aktarım yapılacak ülkenin veri koruma mevzuatının Türkiye mevzuatı ile uyumlu olması yanında, karşılıklılık ilkesinin de gözetilmesi esastır. Yani, sadece aktarım yapılan ülkenin veri koruma düzeyi yeterli bulunmakla kalmayıp, Türkiye'den aynı düzeyde veri aktarımı yapılmasına izin veren bir karşılıklı uygulamanın bulunması da kararın verilmesinde önemli bir kriter olarak dikkate alınmaktadır[180]. Kurul, gerektiğinde ilgili kamu kurumları ve diğer yetkili kuruluşlardan görüş alarak kararlarını şekillendirmekte ve bu kararları en fazla dört yılda bir gözden geçirmektedir.

---

[176] Ayrıntılı bilgi için bknz. s.33 vd.

[177] KVKK, Yurt Dışına Aktarım, *https://www.kvkk.gov.tr/Icerik/2053/Yurtdisina-Aktarim*, (Erişim Tarihi: 05.03.2025).

[178] Yeterli koruma bulunan ülkeler konusunda kurul tarafından henüz bir belirleme yapılmadığı *https://www.kvkk.gov.tr/Icerik/2053/Yurtdisina-Aktarim*, sayfasında belirtilmektedir.

[179] Mesut Serdar Çekin, *op. cit.,* s.131-132.

[180] KVKK, *"Kişisel Verilerin Yurt Dışına Aktarılması Rehberi*", KVKK Yayınları no:48, Ocak 2025, s.32. https://www.kvkk.gov.tr/Icerik/8142/Kisisel-Verilerin-Yurt-Disina-Aktarilmasi-Rehberi, (Erişim Tarihi: 10.03.2025).

Ancak, belirlenen dört yıllık süre, zorunlu bir bekleme süresi niteliğinde değildir. Kurul, ihtiyaç duyduğunda bu sürenin dolmasını beklemeden de yeterlilik kararlarını tekrar gözden geçirebilir, değiştirebilir veya iptal edebilir. Kurul'un yeterlilik kararlarını belirlerken dikkate aldığı kriterler kesin sınırlarla belirlenmemiş olup, gerektiğinde farklı ölçütler de göz önünde bulundurulabilir.[181] Genel olarak, ilgili ülkenin veya kuruluşun veri koruma düzenlemeleri, denetim mekanizmaları, bireylere sağlanan hak arama yolları ve teknik güvenlik önlemleri gibi hususlar değerlendirme kapsamında yer almaktadır. Bu çerçevede, kişisel verilerin uluslararası düzeyde güvenli bir şekilde aktarılabilmesi için hem hukuki hem de teknik standartların sağlanması esas alınmaktadır.

Genel Veri Koruma Tüzüğü, kişisel verilerin Avrupa Ekonomik Alanı dışına aktarılmasını sıkı kurallara bağlamış ve bu çerçevede yeterlilik kararını (adequacy decision) önemli bir mekanizma olarak düzenlemiştir. GDPR'ın 45. maddesi[182]'ne göre, Avrupa Birliği Komisyonu, AEA ile eşdeğer seviyede bir veri koruma düzenlemesine sahip olan AB üyesi olmayan ülkeleri, belirli bölgeleri, sektörleri veya uluslararası kuruluşları tespit ettiğinde, bu durumu "Yeterlilik Kararı" ile resmiyete kavuşturmaktadır. Yeterlilik kararı, AEA içindeki tüm ülkeler için bağlayıcıdır ve kararın verildiği ülkelere ek bir güvenlik tedbiri gerekmeksizin veri aktarımına izin verir. AB üyesi devletler, bağımsız olarak yeterlilik kararı alma yetkisine sahip değildir; bu yetki yalnızca Avrupa Komisyonu'na aittir. Türkiye'de ise m.9/3 bağlamında Kişisel Verileri Koruma Kurulu tarafından alınan "yeterli korumaya sahip ülkeler" kararı, GDPR'daki yeterlilik kararına benzer bir işleve sahiptir. Yeterlilik kararı verilen ülkelerle veri aktarımı, AEA içindeki veri akışıyla aynı kurallara tabi olur ve ek bir izin veya güvence gerektirmez.[183]

Avrupa Komisyonu tarafından yeterli veri korumasına sahip olduğu kabul edilen ülkeler arasında şu ülkeler bulunmaktadır[184]: Andorra, Arjantin, Birleşik Krallık (Brexit sonrası yeterlilik kararı verildi), Güney Kore, İsrail, Japonya, İsviçre, Uruguay.

---

[181] KVKK, Yeterli Korumaya Sahip Ülkelerin Belirlenmesinde Esas Alınacak Kriterler Hakkında Kişisel Verileri Koruma Kurulu'nun, 02/05/2019 tarih ve 2019/125 sayılı Karar Özeti, *https://www.kvkk.gov.tr/Icerik/5470/Kisisel-Verileri-Koruma-Kurulu-nun-Yeni-Yayinlanan-Karari*, (Erişim Tarihi: 05.03.2025).

[182] EUR-Lex GDPR Metni, https://eur-lex.europa.eu/eli/reg/2016/679/oj, (Erişim Tarihi: 05.03.2025).

[183] Kişisel Verilerin Korunmasına İlişkin Düzenlemeler Çerçevesinde Uluslararası Veri Aktarımı Yeni Gelişmeler ve Uygulamaya İlişkin Hukuki Değerlendirmeler, İstanbul, *https://itlaw.bilgi.edu.tr/media/2020/3/30/Final%20Veri_Aktarimi_Raporu_30.03.2020.pdf*, s.17, (Erişim Tarihi: 05.03.2025).

[184] Avrupa Komisyonu'nun Yeterlilik Kararları Sayfası, *https://commission.europa.eu/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en, (*Erişim Tarihi: 05.03.2025).

ABD için özel bir durum söz konusudur. AB-ABD Veri Gizliliği Çerçevesi (Data Privacy Framework- DPF) kapsamında belirli şirketlerin yeterlilik kararı çerçevesinde veri almasına izin verilmiştir.[185]

Yeterlilik kararı, Avrupa Komisyonu'nun belirli bir ülkenin, bölgenin, sektörün veya uluslararası kuruluşun AEA ile eşdeğer seviyede bir veri koruma düzenlemesine sahip olduğunu onaylaması anlamına gelir.[186] Bu karar alındığında, ilgili ülkeye veri aktarımı için ek bir izin veya güvenceye gerek kalmaz ve AEA içindeki veri aktarımıyla aynı şekilde değerlendirilir.

*Bir yeterlilik kararının kabulü şunları içerir[187]:*

- *Avrupa Komisyonu'ndan bir öneri;*
- *Avrupa Veri Koruma Kurulu'nun görüşü;*
- *AB ülkelerinin temsilcilerinden bir onay;*
- *kararın Avrupa Komisyonu tarafından kabul edilmesi.*

Avrupa Komisyonu, yeterlilik kararını verirken aşağıdaki kriterleri değerlendirir[188]:

- *Temel veri koruma kavramlarının ve/veya ilkelerinin mevcut olması,*
- *Verinin hukuka uygun, adil ve meşru bir şekilde işlenmesi,*
- *Verinin belirli bir amaçla sınırlı olarak işlenmesi (Amaçla Sınırlı Olma İlkesi),*
- *Verinin doğru ve güncel olması (Veri Kalitesi İlkesi),*
- *Verinin işleme amacıyla orantılı olması (Orantılılık İlkesi),*
- *Verinin işleme amacının gerçekleştirilmesi için yeterli olan süreden fazla saklanmaması (Veri Saklama İlkesi),*
- *Verinin güvenliği için teknik ve idari tedbirlerin alınması (Güvenlik ve Mahremiyet İlkesi),*
- *İlgili kişilerin verilerinin işlenmesi konusunda açık bir şekilde bilgilendirilmeleri (Şeffaflık ilkesi),*

[185] https://www.dataprivacyframework.gov
[186] Avrupa Komisyonu'nun Yeterlilik Kararları Sayfası, *https://commission.europa.eu/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en*, (Erişim Tarihi: 05.03.2025).
[187] Avrupa Komisyonu'nun Yeterlilik Kararları Sayfası, *https://commission.europa.eu/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en, (*Erişim Tarihi: 05.03.2025)
[188] Kişisel Verilerin Korunmasına İlişkin Düzenlemeler Çerçevesinde Uluslararası Veri Aktarımı Yeni Gelişmeler ve Uygulamaya İlişkin Hukuki Değerlendirmeler, İstanbul, *https://itlaw.bilgi.edu.tr/media/2020/3/30/Final%20Veri_Aktarimi_Raporu_30.03.2020.pdf*, s.17, (Erişim Tarihi: 05.03.2025).

- *İlgili kişinin erişim, düzeltme, silme ve itiraz haklarının bulunması,*
- *Veri aktarımının ilk alıcısı tarafından yapılacak aktarımlara, diğer alıcının, yeterli düzeyde koruma sağlayan kurallara tabi olması ve veri sorumlusu adına veri işlerken ilgili talimatları izlemesi durumlarında izin verilmesi (İleride gerçekleştirilecek aktarımların kısıtlanması),*
- *Aktarım yapılan ülkenin veri koruma, ulusal güvenlik ve ileriye dönük aktarımlar hakkındaki yasaları ve içtihatları ve bunların pratikte nasıl uygulandığı ve icra edildiği,*
- *Veri koruma yasalarına uyumu sağlayacak ve işbu yasaları icra edecek bağımsız denetleyici otoritelerin varlığı (ya da yokluğu),*
- *Aktarım yapılan ülkenin verilerin korunmasına ilişkin uluslararası taahhütleri.*

Yeterlilik kararı periyodik olarak gözden geçirilir ve ilgili ülkedeki veri koruma seviyesinde olumsuz bir değişiklik olması durumunda askıya alınabilir veya iptal edilebilir. Avrupa Komisyonu, gerektiğinde yeni yeterlilik kararları verebilir veya mevcutları değiştirebilir. Ancak, yeterlilik kararları kesin ve değişmez değildir. Schrems II kararı[189] (C-311/18), bu kararların hukuki çerçevesini belirleyen kritik bir örnektir, bu da yeterlilik kararlarının hukuki denetime açık olduğunu göstermektedir. Avrupa Adalet Divanı, 16 Temmuz 2020'de aldığı kararla AB-ABD Gizlilik Kalkan'ını (Privacy Shield) geçersiz kılmış, böylece ABD'ye yönelik yeterlilik kararının dayanağını ortadan kaldırmıştır. Kararın gerekçesi, ABD'deki istihbarat faaliyetlerinin AB vatandaşlarının kişisel verilerini yeterince korumadığı ve GDPR kapsamında etkin bir denetim ve itiraz mekanizmasının bulunmadığı yönündeydi. Bu karar, yeterlilik kararlarının sadece mevzuat temelinde değil, fiili uygulamalar açısından da sıkı değerlendirmelere tabi tutulması gerektiğini göstermiştir. Yani, Avrupa Komisyonu bir ülkeye yeterlilik kararı vermiş olsa bile, bu karar Avrupa Adalet Divanı tarafından iptal edilebilir[190]. ABD örneğinde olduğu gibi, bu durum veri aktarım süreçlerinde hukuki belirsizliklere yol açabilmektedir.

[189] Schrems II Kararı (C-311/18)- Avrupa Adalet Divanı, *https://curia.europa.eu/juris/liste.jsf?num=C-311/18*, (Erişim Tarihi: 05.03.2025)

[190] Avrupa Veri Koruma Kurulu (EDPB)- Schrems II Sonrası Rehberler, *https://www.edpb.europa.eu/search_en?search=EDPB+Schrems+II*, EDPB Schrems II Rehberi, *https://www.edpb.europa.eu/sites/default/files/files/file1/20200724_edpb_faqoncjeuc31118_en.pdf*, (Erişim Tarihi: 05.03.2025).

## IV. YETERLİ KORUMA BULUNMAYAN ÜLKELERE KİŞİSEL VERİ AKTARIMI

### 1. KVKK m.9/4 KAPSAMINDA YURT DIŞINA AKTARIM KOŞULLARI

Kişisel verilerin yurt dışına aktarılmasına ilişkin süreçte, Kurum, yeterli korumanın bulunduğu ülkeleri belirlerken hem KVKK m.9/f.4 hükmü hem de Kurul'un yayınladığı formda yer alan kriterleri dikkate alacaktır. KVKK m.9/f.4'te, Kurul'un, yurt dışında yeterli veri koruma seviyesinin mevcut olup olmadığını ve m.9/f.3[191] gereğince veri aktarım izni verilip verilmeyeceğini değerlendireceği hüküm altına alınmıştır. Bu bağlamda, Kurul, her iki durumu değerlendirirken aynı ölçütleri dikkate esas alacaktır[192]. Bahsi geçen m.9/f.3'teki koşulların gerçekleşmesi bakımından, çalışmamızın ilgili kısımlarında yapılan açıklamalara atıf yapmaktayız. 7499 sayılı Kanun ile getirilen KVKK m.9/f.4 hükmüne göre, yeterlilik kararı bulunmayan bir durumda kişisel verilerin yurt dışına aktarılabilmesi için iki aşamalı bir sistem ile belirli şartların yerine getirilmesi gerekmektedir. Bu şartlar arasında, KVKK m.5 ve m.6'da belirtilen hukuka uygunluk sebeplerinden birinin gerçekleşmiş olması, veri sahibinin aktarım yapılacak ülkede haklarını kullanabileceği ve etkili bir yasal yola başvurabileceği imkanlarının bulunması, ikinci aşamada ise m.9/f.4'te sıralanan uygun güvence önlemlerinin taraflarca sağlanması yer almaktadır[193]. Bu çerçevede, kişisel verilerin yurt dışına aktarım yapılabilmesine olanak tanıyan durumlar şu şekilde sıralanabilir:

*"(4) Kişisel veriler, yeterlilik kararının bulunmaması durumunda, 5 inci ve 6 ncı maddelerde belirtilen şartlardan birinin varlığı, ilgili kişinin aktarımın yapılacağı ülkede de haklarını kullanma ve etkili kanun yollarına başvurma imkânının bulunması kaydıyla, aşağıda belirtilen uygun güvencelerden birinin taraflarca sağlanması halinde veri sorumluları ve veri işleyenler tarafından yurt dışına aktarılabilir: a) Yurt dışındaki kamu kurum ve kuruluşları veya uluslararası kuruluşlar ile Türkiye'deki kamu kurum ve kuruluşları veya kamu kurumu niteliğindeki meslek kuruluşları arasında yapılan uluslararası sözleşme niteliğinde olmayan anlaşmanın varlığı ve Kurul tarafından aktarıma izin verilmesi. b) Ortak ekonomik faaliyette*

[191] KVKK, m.9/ (3) Yeterlilik kararı verilirken öncelikle aşağıdaki hususlar dikkate alınır: a) Kişisel verilerin aktarılacağı ülke, ülke içerisindeki sektörler veya uluslararası kuruluşlar ile Türkiye arasında kişisel veri aktarımına ilişkin karşılıklılık durumu. b) Kişisel verilerin aktarılacağı ülkenin ilgili mevzuatı ve uygulaması ile kişisel verilerin aktarılacağı uluslararası kuruluşun tâbi olduğu kurallar. c) Kişisel verilerin aktarılacağı ülkede veya uluslararası kuruluşun tâbi olduğu bağımsız ve etkin bir veri koruma kurumunun varlığı ile idari ve adli başvuru yollarının bulunması. ç) Kişisel verilerin aktarılacağı ülkenin veya uluslararası kuruluşun, kişisel verilerin korunmasıyla ilgili uluslararası sözleşmelere taraf veya uluslararası kuruluşlara üye olma durumu. d) Kişisel verilerin aktarılacağı ülkenin veya uluslararası kuruluşun, Türkiye'nin üye olduğu küresel veya bölgesel kuruluşlara üye olma durumu. e) Türkiye'nin taraf olduğu uluslararası sözleşmeler.

[192] Kuyumcu, *op. cit.,* s. 106.

[193] *Ibid* s.114.

*bulunan teşebbüs grubu bünyesindeki şirketlerin uymakla yükümlü oldukları, kişisel verilerin korunmasına ilişkin hükümler ihtiva eden ve Kurul tarafından onaylanan bağlayıcı şirket kurallarının varlığı. c) Kurul tarafından ilan edilen, veri kategorileri, veri aktarımının amaçları, alıcı ve alıcı grupları, veri alıcısı tarafından alınacak teknik ve idari tedbirler, özel nitelikli kişisel veriler için alınan ek önlemler gibi hususları ihtiva eden standart sözleşmenin varlığı. ç) Yeterli korumayı sağlayacak hükümlerin yer aldığı yazılı bir taahhütnamenin varlığı ve Kurul tarafından aktarıma izin verilmesi."*

Öte yandan, KVKK m.9/4 hükmünde atıf yapılan KVKK m.5 ve m.6'da düzenlenen koşullardan en az birinin sağlanması gerektiğine ilişkin daha önce yapılan açıklamalara çalışmamızın ilgili bölümlerinde değinilmiştir. Ancak, "aktarım yapılacak ülkede ilgili kişinin veri haklarını kullanabilmesi ve etkili bir hukuki başvuru yolunun bulunması şartı", veri güvenliği açısından kritik bir unsur olduğundan, bu konunun ayrıca ele alınması gerekmektedir. Bu nedenle, maddede belirtilen güvencelere geçmeden önce, ilgili kişinin yurt dışında kişisel verilerine ilişkin haklarını ne ölçüde koruyabileceği ve hangi yollarla hukuki koruma sağlayabileceği detaylı bir şekilde değerlendirilmelidir.[194] Bu şartların sağlanmasında en büyük sorumluluk, veri aktarımını gerçekleştirecek olan veri sorumlusu veya veri işleyene aittir. Özellikle, ilgili kişinin KVKK m.11 kapsamında sahip olduğu hakların ve m.14 uyarınca öngörülen tazminat hakkının yalnızca teoride değil, fiilen korunup korunmadığının tespit edilmesi gerekmektedir. Bu doğrultuda, veri aktarımını yapan tarafların, aktarımın gerçekleştirileceği üçüncü ülke mevzuatını inceleyerek veri sahibinin haklarının güvence altına alındığını somut olarak belgelendirmesi beklenmektedir. Bu değerlendirme süreci, yalnızca üçüncü ülkenin hukuki düzenlemelerini incelemekle sınırlı değildir. Aynı zamanda, bu ülkede veri sahiplerinin haklarını kullanma konusunda pratikte karşılaşabilecekleri engellerin de dikkate alınmasını gerektirir. Örneğin, ilgili ülkede bağımsız bir veri koruma otoritesinin bulunup bulunmadığı, veri sahiplerinin başvuru süreçlerinin etkinliği ve mahkemelere erişim hakları gibi unsurların da detaylı şekilde analiz edilmesi gerekir.[195]

Bu çerçevede, GDPR m.46'da düzenlenen güvence mekanizmaları ile KVKK m.9/4'te yer alan uygun güvenceler arasında önemli benzerlikler bulunmaktadır. GDPR kapsamında yeterlilik kararının bulunmadığı hallerde, veri aktarımının güvenli bir şekilde gerçekleştirilmesi için bağlayıcı kurumsal kurallar, standart sözleşme hükümleri ve ek idari, teknik ve organizasyonel önlemler uygulanarak veri koruma seviyesinin yeterli hale getirilmesi gerekmektedir. KVKK

[194] Kuyumcu, *op. cit.* s. 116.
[195] Öztürk, Çalışkan, Seyhan, *op. cit.* s. 123.

sisteminde de benzer şekilde, aktarımı gerçekleştiren tarafların, aktarımın yapıldığı ülkeye ilişkin risk analizleri yaparak uygun güvenlik önlemlerini uygulamaları gerekmektedir. Bu çerçevede, yeterli korumanın sağlanmadığı ülkelere yapılacak veri aktarımlarında sadece yazılı bir güvencenin varlığı yeterli olmayacak, veri sorumluları veya veri işleyenler, pratikte de etkili bir koruma sağlandığını kanıtlayacak belgelere sahip olmalıdır. GDPR ve KVKK'nın ortak noktasını oluşturan bu güvence yaklaşımı, özellikle Schrems II kararında vurgulanan, "kâğıt üzerinde var olan düzenlemelerin fiiliyatta nasıl uygulandığının" dikkate alınması gerekliliğini bir kez daha ortaya koymaktadır.

Elverişli bir yeterlilik kararının bulunmadığı durumlarda, kişisel verilerin yurt dışına aktarılabilmesi için KVKK m.9/4'te belirtilen alternatif güvenceler sağlanmalıdır. Bu güvenceler, aktarımın hukuka uygun şekilde gerçekleştirilmesini ve ilgili kişinin haklarının korunmasını amaçlamaktadır. Aşağıda, söz konusu bentlerde düzenlenen güvence mekanizmaları detaylı olarak ele alınacaktır.

**a. Yurt Dışındaki Kamu Kurum ve Kuruluşları veya Uluslararası Kuruluşlar veya Kamu Niteliğindeki Meslek Kuruluşları Arasında Yapılan Uluslararası Sözleşme Niteliğinde Olmayan Anlaşmanın Varlığı ve Kurul Tarafından Aktarıma İzin Verilmesi (m.9/4-a)**

Kişisel verilerin yurt dışına aktarımı, yeterli koruma kararının bulunmadığı ülkeler söz konusu olduğunda ancak belirli güvenceler sağlanarak gerçekleştirilebilir. Bu kapsamda, Türkiye'deki kamu kurumları veya kamu kurumu niteliğindeki meslek kuruluşları ile yurt dışında bulunan kamu kurumları, kuruluşlar ya da uluslararası kuruluşlar arasında yapılan ve uluslararası sözleşme niteliği taşımayan anlaşmalar, bir aktarım yöntemi olarak öngörülmüştür. Ancak bu tür bir aktarımın gerçekleşebilmesi için yalnızca böyle bir anlaşmanın varlığı yeterli olmayıp, Kişisel Verileri Koruma Kurulu'nun da aktarıma onay vermesi gerekmektedir.

Kanunun 9. maddesinin 4. fıkrasında yer alan bu düzenleme, kamu kurumları arasında zorunlu olarak gerçekleştirilen veri aktarımlarının güvenli bir şekilde yürütülmesini sağlamak amacıyla getirilmiştir. 7499 sayılı Kanun'un 34. maddesinin gerekçesinde de ifade edildiği üzere, Türkiye'deki bir kamu kurumunun yabancı bir ülkedeki kamu kurumu ile belirli bir iş birliği protokolü çerçevesinde yürüttüğü faaliyetler kapsamında kişisel veri aktarımı yapabilmesi için Kurul'un onayı alınmalıdır.[196] Kurul, bu değerlendirmeyi yaparken, ilgili anlaşmanın kişisel verilerin korunmasına yönelik yeterli güvenceleri içerip içermediğini göz önünde

[196] Kaya, *"KVKK Reformu 2024 Değişiklikleri", op. cit.,* s.53.

bulunduracaktır. Bu düzenleme, Avrupa Birliği Genel Veri Koruma Tüzüğü'nün 46. maddesinin 2. fıkrasının (a) bendinde düzenlenen güvenceler ile benzerlik göstermektedir. GDPR kapsamında da kamu kurumları veya uluslararası kuruluşlar arasında yapılan anlaşmalar çerçevesinde kişisel veri aktarımına izin verilebilmesi için, sözleşmenin taraflarının veri koruma ilkelerine uygunluğu sağlama taahhüdü vermesi gerekmektedir.[197] Avrupa Birliği Veri Koruma Kurulu tarafından yayımlanan rehberlerde, bu tür anlaşmalarda bulunması gereken temel unsurlar belirlenmiştir. Bu unsurlar, GDPR çerçevesinde veri koruma seviyesinin korunmasını sağlamak amacıyla belirlenmiştir. Bunlar arasında[198]: Anlaşmanın amacı, kapsamı ve hukuki dayanağının açıkça belirtilmesi, temel veri koruma ilkelerinin ve ilgili kişilere tanınan hakların korunmasını sağlayacak güvencelerin yer alması, veri işleme faaliyetlerinin amacının net bir şekilde sınırlandırılması ve veri minimizasyonu prensibine uygun hareket edilmesi önemlidir. Ayrıca, kişisel verilerin saklama sürelerine ilişkin hükümlerin anlaşmada yer alması, aktarılan verilerin güvenliğini ve gizliliğini sağlamak için teknik ve idari tedbirlerin alınmasının zorunlu kılınması, veri sahibinin haklarını kullanabilmesini sağlayacak etkili başvuru yollarının öngörülmesi gibi unsurlar da bu tür anlaşmalarda yer almalıdır. Özellikle Schrems II Kararı sonrasında, AB dışına yapılan veri transferlerinde yeterli koruma sağlanıp sağlanmadığının detaylı bir şekilde değerlendirilmesi gerektiği unutulmamalıdır.

KVKK m.9/4-a kapsamında gerçekleştirilecek veri aktarımlarına ilişkin usul ve esaslar, ilgili 10/07/2024 tarihli ve 32598 sayılı Resmî Gazete' de yayımlanarak yürürlüğe giren "Kişisel Verilerin Yurt Dışına Aktarılmasına İlişkin Usul ve Esaslar Hakkında Yönetmelik"[199] ile detaylandırılmaktadır. Özellikle, uluslararası sözleşme niteliğinde olmayan anlaşmalara dayalı veri aktarımlarının hukuki çerçevesinin netleşmesi ve uygulama süreçlerinin belirlenmesi açısından yönetmeliğin 11. maddesi büyük önem taşımaktadır. İlgili maddenin 1. fıkra[200]'sı

---

[197] EDPB, Guidelines 2/2020 on Article 46 (2) (a) and 46 (3) (b) of Regulation 2016/679 for transfer of personal data between EEA and non-EEA public authorities and bodies, 18 January 2020, s. 18, https://www.edpb.europa.eu/sites/default/files/consultation/edpb_guidelines_202002_art46guidelines_internationaltransferspublicbodies_v1.pdf, (Erişim Tarihi: 10.03.2025).

[198] *Ibid*., s.13.

[199] Kişisel Verilerin Yurt Dışına Aktarılmasına İlişkin Usul ve Esaslar Hakkında Yönetmelik, 10.07.2024
Uluslararası sözleşme niteliğinde olmayan anlaşmayla uygun güvencenin sağlanması
MADDE 11- (1) Uluslararası sözleşme niteliğinde olmayan anlaşmada yer verilecek kişisel verilerin korunmasına yönelik hükümler vasıtasıyla, Türkiye'deki kamu kurum ve kuruluşları ile kamu kurumu niteliğindeki meslek kuruluşları ve yabancı ülkedeki kamu kurum ve kuruluşları veya uluslararası kuruluşlar arasında yapılacak kişisel veri aktarımları bakımından uygun güvence sağlanabilir. Anlaşma, kişisel veri aktarımının tarafları arasında akdedilir. https://www.kvkk.gov.tr/SharedFolderServer/CMSFiles/aaf0eeec-9599-4c68-8b7a-33039059ca41.pdf, (E.T:10.03.2025).

[200] KVKK, *"Kişisel Verilerin Yurt Dışına Aktarılması Rehberi*", KVKK Yayınları no:48, Ocak 2025, s.32. https://www.kvkk.gov.tr/Icerik/8142/Kisisel-Verilerin-Yurt-Disina-Aktarilmasi-Rehberi, (Erişim Tarihi: 10.03.2025)

uyarınca, bu tür anlaşmalarda yer alması gereken veri koruma yükümlülükleri arasında kişisel veri aktarımının amacı, kapsamı ve hukuki sebebinin belirlenmesi, kanun ve ilgili mevzuata uygun şekilde temel kavramların tanımlanması ve kanunun genel ilkelerine uyum taahhüdü bulunmaktadır. Ayrıca, ilgili kişilerin anlaşma ve veri aktarımı hakkında bilgilendirilmesine ilişkin düzenlemeler yapılmalı, veri sahibinin hakları güvence altına alınmalı ve başvuru yolları belirlenmelidir. Veri güvenliği tedbirlerinin alınacağına dair taahhüt verilmesi, özel nitelikli kişisel verilerin aktarılması halinde Kurul tarafından belirlenen yeterli önlemlerin sağlanması, kişisel verilerin sonraki aktarımlarına ilişkin kısıtlamaların öngörülmesi de gerekmektedir. Anlaşmanın ihlali durumunda başvurulabilecek hukuki yolların tanımlanması ve veri alıcısının yükümlülüklere uymaması halinde veri aktaranın aktarımı askıya alma veya anlaşmayı feshetme hakkına sahip olması da yönetmelik kapsamında düzenlenen hususlar arasındadır.

Anılan yönetmelik ile bu tür anlaşmalara iş birliği protokolü, mutabakat zaptı veya idari anlaşma şeklinde düzenlenebileceği öngörülmüş ve Türkiye İlaç ve Tıbbi Cihaz Kurumu ile Avrupa Komisyonu arasında yapılan idari anlaşma[201], uluslararası sözleşme niteliğinde olmayan bir düzenlemeye dayalı veri aktarımına somut bir örnek verilmiştir.[202] Bu kapsamda, Türkiye'den kişisel verilerin yurt dışına aktarılacağı durumlarda veri aktaran tarafından Kurul'a izin başvurusunda bulunulması gerekmektedir. Başvuru sürecinde anlaşmanın nihai hali ile birlikte gerekli bilgi ve belgelerin sunulması zorunludur. Kurul'un onay vermesi durumunda, ilgili veri aktarımı yürürlüğe girebilecektir. Bu düzenleme, uluslararası iş birlikleri çerçevesinde yürütülen kamu hizmetlerinin kesintisiz devam etmesini sağlarken, aynı zamanda kişisel verilerin korunması için gerekli güvenceleri de içermektedir. Bu nedenle, ilgili tarafların yalnızca veri aktarımına yönelik bir anlaşma yapmakla yetinmeyip, aynı zamanda veri koruma standartlarına uygun hareket etmeleri büyük önem taşımaktadır.

**b. Ortak Ekonomik Faaliyette Bulunan Teşebbüs Grubu Bünyesindeki Şirketlerin Uymakla Yükümlü Oldukları Kişisel Verilerin Korunmasına İlişkin Hükümler İhtiva Eden ve Kurul Tarafından Onaylanan Bağlayıcı Şirket Kuralları (m.9/4-b)**

Çok uluslu şirket topluluklarının, kişisel verilerin yurt dışına aktarımında uyguladıkları Bağlayıcı Şirket Kuralları (BŞK), Avrupa Birliği'nde yürürlükte olan 2016/679 sayılı Genel Veri Koruma Tüzüğü'ndeki "Bağlayıcı Şirket Kuralları" (BCR) modelinden ilham alınarak geliştirilmiş olup, Türkiye'de de benzer bir sistem uygulanmaya başlanmıştır. Bu sistem, veri

[201] Avrupa Komisyonu (aktaran İdare) ve Türkiye İlaç ve Tıbbi Cihaz Kurumu (TİTCK) (alıcı İdare) arasında kişisel verilerin aktarımına yönelik İdari Anlaşma, https://titck.gov.tr/Dosyalar/VeriKoruma/tr/1IdariAnlasma.pdf, (Erişim Tarihi: 10.03.2025).
[202] KVKK, *"Kişisel Verilerin Yurt Dışına Aktarılması Rehberi"*, *op. cit.,* s.34-35.

sorumlularının yurt dışına veri aktarımı süreçlerinde yeterli koruma sağlamayı taahhüt etmelerini temin etmekte ve veri koruma politikalarının hukuki zeminde güvence altına alınmasını sağlamaktadır. Bağlayıcı Şirket Kuralları, küresel ölçekte veri işleme faaliyetlerinde tutarlılığı sağlamakta ve veri koruma standartlarının uyumlu hale getirilmesine katkıda bulunmaktadır. Bu kapsamda, Kişisel Verileri Koruma Kurulu tarafından yayımlanan "Veri Sorumluları İçin Bağlayıcı Şirket Kuralları Başvuru Formu" ve "Veri Sorumluları İçin Bağlayıcı Şirket Kurallarında Bulunması Gereken Temel Hususlara İlişkin Yardımcı Doküman[203]", GDPR'ın 47. maddesi ve Avrupa Veri Koruma Kurulu'nun WP 256 rev.01 sayılı belgesi[204] ile uyumlu düzenlemeler içermektedir. Kurum, 10.04.2020 tarihli "Bağlayıcı Şirket Kuralları Hakkında Duyuru[205]" ile Türk hukukunda yurt dışına veri aktarımı konusunda başvurulabilecek yeni bir yöntem olarak Bağlayıcı Şirket Kurallarını belirlemiştir. Söz konusu duyuruda, yeterli korumanın sağlanmadığı ülkelerde faaliyet gösteren çok uluslu grup şirketleri için BŞK'nın, veri aktarımı süreçlerinde kullanılan ve yeterli korumanın yazılı olarak garanti edilmesini sağlayan veri koruma politikaları olarak işlev gördüğü belirtilmiştir. Ayrıca, çok uluslu grup şirketleri açısından taahhütname yoluna kıyasla daha pratik bir alternatif sunduğu ifade edilmiştir. Şirket toplulukları içerisindeki kuruluş yapıları, iş modelleri ve operasyonları gereği, grup üyeleri arasında veri akışı kaçınılmaz bir durumdur. Bağlayıcı Şirket Kuralları, grup içi veri aktarım süreçlerini daha hızlı, güvenli ve düzenli bir şekilde yönetmeyi amaçlamakta olup, çok uluslu şirketler için etkin bir uyum aracı olarak öne çıksa da Kurul henüz yeterli koruma seviyesine sahip ülkeleri ilan etmediğinden, BŞK'ların ülkemizde yaygın olarak uygulanan bir yöntem olduğu söylenemez.

KVKK'da doğrudan BŞK'ya ilişkin özel bir hüküm yer almamakla birlikte, 6698 sayılı Kişisel Verilerin Korunması Kanunu'nun 9. maddesinin 4. fıkrasının (b) bendi kapsamında, ortak ekonomik faaliyette bulunan teşebbüs gruplarının, veri koruma yükümlülüklerini içeren ve Kurul tarafından onaylanan bağlayıcı kurallara uymaları şartıyla kişisel veri aktarımı gerçekleştirebileceği düzenlenmiştir.[206] Bu doğrultuda, BŞK'ya ilişkin başvuruların ve uygulama süreçlerinin, KVKK'nın yürürlükteki hükümlerine uygun şekilde şekillendirilmesi

[203] KVKK, Bağlayıcı Şirket Kuralları Yardımcı Kılavuz, https://www.kvkk.gov.tr/Icerik/7935/Veri-Sorumlulari-Icin-Baglayici-Sirket-Kurallarinda-Bulunmasi-Gereken-Temel-Hususlar-Yardimci-Kilavuz, (Erişim Tarihi: 10.03.2025).
[204] Avrupa veri koruma mevzuatı El Kitabı, Lüksemburg, 2018, https://itlaw.bilgi.edu.tr/media/2020/3/30/Bilgi_Avrupa_Veri_Koruma_Mevzuatı_El_Kitabı_2018_TR_v01_16022019.pdf, (Erişim Tarihi: 10.03.2025).
[205] 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: 10.03.2025).
[206] Çelik, *op. cit.,* s.110.

büyük önem taşımaktadır. BŞK'nın etkin bir şekilde uygulanabilmesi için, başvuru sürecinde grup şirketlerinin, veri koruma standartlarını ve yükümlülüklerini açıkça ortaya koyması gerekmektedir.

Kurul tarafından 10/07/2024 tarihli ve 32598 sayılı Resmî Gazete' de yayımlanan "Kişisel Verilerin Yurt Dışına Aktarılmasına İlişkin Usul ve Esaslar Hakkında Yönetmelik" in 12. ve 13. Maddelerinde bağlayıcı şirket kuralları düzenlenmiş olup, 13.maddenin birinci fıkrasında bu kuralların asgari olarak içermesi gereken unsurlar tanımlanmaktadır[207]: Buna göre, topluluk şirketlerinin yapısı, üyeleri ve iletişim bilgileri detaylı bir şekilde belirtilmeli, kişisel verilerin işlenmesine ilişkin temel ilkeler, özel nitelikli kişisel verilerin işlenme koşulları, veri güvenliği tedbirleri, veri ihlali bildirim mekanizmaları ve üçüncü taraflarla veri paylaşımına ilişkin sınırlamalar düzenlenmelidir. Ayrıca, veri aktarımının niteliği, veri kategorileri, aktarım amacı, saklama süresi, ilgili kişi grupları ve aktarım yöntemlerine dair detaylar sunulmalı, kuralların uygulanmasını temin edecek sorumlu bir yetkili atanarak bir Uyumluluk Denetim Programı oluşturulmalıdır. Kişisel verilere erişimi bulunan personel için küresel düzeyde bir eğitim programı uygulanmalı, ilgili kişiler veri koruma konusundaki temel ilkeler, aydınlatma yükümlülüğü, sahip oldukları haklar ve bu hakların kullanımı konusunda bilgilendirilmelidir. Kuralların ihlali sonucu zarar doğması hâlinde grup şirketlerinden biri ya da tamamı tazmin sorumluluğunu üstlenmeli, bağlayıcı şirket kurallarını uygulamaya engel teşkil edebilecek ulusal mevzuatlar veya diğer yasal yükümlülükler beyan edilmelidir. Son olarak, ilgili kişiler tarafından yapılacak taleplerin Türk mahkemeleri ve denetleyici otoriteleri nezdinde görüleceği kabul edilmelidir.

Bağlayıcı Şirket Kurallarına ilişkin başvuru süreci, ilgili şirket topluluğu tarafından Kurul'un yayımladığı başvuru formunun doldurulmasıyla resmen başlatılacaktır. Bu sürecin etkin yürütülebilmesi için, topluluk içerisindeki diğer şirketlerle koordinasyon sağlanarak gerekli bilgilerin bir soru çizelgesi aracılığıyla toplanması gerekmektedir. Hâlihazırda Avrupa Birliği'nde faaliyet gösteren ve GDPR kapsamında bir Bağlayıcı Şirket Kuralları mekanizmasına sahip şirketlerin bu süreci daha hızlı ve sistematik bir şekilde yürütebileceği öngörülmektedir. Kurul, Bağlayıcı Şirket Kuralları başvurularını 12 ay içinde değerlendirmeyi taahhüt etmiştir.[208] Ancak, 6698 sayılı Kişisel Verilerin Korunması Kanunu'nun 9. maddesinin yurtdışına veri aktarımı için Kurul onayı öngörmesi nedeniyle, veri sorumlularının en kısa

[207] KVKK, *"Kişisel Verilerin Yurt Dışına Aktarılması Rehberi*", *op. cit.,* s.42.
[208] KVKK, Bağlayıcı Şirket Kuralları Yardımcı Kılavuz, https://www.kvkk.gov.tr/Icerik/7935/Veri-Sorumlulari-Icin-Baglayici-Sirket-Kurallarinda-Bulunmasi-Gereken-Temel-Hususlar-Yardimci-Kilavuz, s.1-4.

sürede başvuru yapmaları ve fiilen yürütülen veri aktarımlarını hukuki zemine oturtmaları önem arz etmektedir.

**c. Kurul tarafından ilan edilen, veri kategorileri, veri aktarımının amaçları, alıcı ve alıcı grupları, veri alıcısı tarafından alınacak teknik ve idari tedbirler, özel nitelikli kişisel verileri için alınan ek önlemler gibi hususları ihtiva eden Standart Sözleşmelerin varlığı (m.9/4-c)**

Bu bölümde genel olarak standart sözleşmenin hukuki çerçevesi ele alınmış olup, anonim şirketlerde Standart Sözleşme maddelerinin uygulama alanı üçüncü bölümde detaylı olarak incelenecektir.

Küreselleşen dünyada, kişisel verilerin sınır ötesi aktarımı, aktarımın hukuki ve teknik güvence altına alınması, veri sorumluları ve ilgili taraflar için kritik bir gereklilik haline gelmiştir. Kişisel Verileri Koruma Kanunu ve Avrupa Birliği Genel Veri Koruma Tüzüğü uyarınca standart sözleşme, uluslararası veri transferlerinde hukuki güvence sağlayan önemli bir mekanizma olarak kabul edilmektedir. KVKK'da açık bir tanımı yapılmamış olmakla birlikte, ilgili yönetmeliğin 14. maddesi uyarınca standart sözleşme; veri kategorileri, aktarım amacı, alıcı grupları ve teknik-idari tedbirler gibi hususları kapsamaktadır. Özellikle özel nitelikli kişisel verilerin aktarımında ek güvenceler getirilerek, kişisel veri sahiplerinin haklarının korunması sağlanmaktadır.[209] GDPR da benzer bir yaklaşım benimseyerek, kişisel verilerin Avrupa Birliği dışına aktarımını belirli mekanizmalara bağlamış ve bu mekanizmalardan biri olarak standart sözleşme maddelerini düzenlemiştir. Avrupa Komisyonu tarafından önceden onaylanan bu sözleşme modeli, değişiklik yapılmadan kullanıldığı takdirde veri aktarımının hukuka uygun olarak gerçekleşmesini sağlamaktadır.[210]

Standart sözleşmenin hukuki geçerliliği, aktarım taraflarının veya yetkili temsilcilerinin imzası ile sağlanır. Sözleşmenin imzalanmasını takiben beş iş günü içinde Kişisel Verileri Koruma Kurumu'na fiziki veya elektronik yollarla bildirim yapılması zorunludur. Bildirim yükümlülüğünün hangi tarafça yerine getirileceği sözleşmede belirlenebilir. Eğer böyle bir belirleme yapılmamışsa, veri aktaran taraf bu sorumluluğu üstlenir. Standart sözleşmenin geçerliliği ve hukuki uygunluğu, Kurul tarafından denetlenmektedir. Kurul tarafından ilan edilen metinde herhangi bir değişiklik yapılması veya taraflardan birinin geçerli bir imza sunmaması halinde, KVKK'nın 15. maddesi uyarınca inceleme yapılabilir. Ayrıca, bildirime

[209] KVKK, *"Kişisel Verilerin Yurt Dışına Aktarılması Rehberi"*, *op. cit.,* s.50.
[210] https://itlaw.bilgi.edu.tr/media/2020/3/30/Final%20Veri_Aktarimi_Raporu_30.03.2020.pdf s.110.

ek olarak imza yetkisini tevsik eden belgeler ve yabancı dildeki dokümanların noter onaylı çevirisinin sunulması gerekmektedir[211].

Kişisel Verileri Koruma Kurulu, 4 Haziran 2024 tarihli ve 2024/959 sayılı kararıyla farklı veri aktarım senaryolarını kapsayan dört tip standart sözleşme metnini kabul ederek yayımlamıştır.[212] Dijital ekonomide yaşanan gelişmeler, karmaşık veri işleme süreçleri ve uluslararası düzenlemeler göz önünde bulundurularak hazırlanan bu sözleşmeler, veri aktaran ve veri alıcısının rollerine göre farklılık göstermektedir. Birinci sözleşme (SS-1), hem veri aktaran hem de veri alıcısının veri sorumlusu olduğu durumu kapsamaktadır. İkinci sözleşme (SS-2), veri aktaranın veri sorumlusu, veri alıcısının ise veri işleyen olduğu senaryoya yöneliktir. Üçüncü sözleşme (SS-3), her iki tarafın da veri işleyen olduğu durumlar için hazırlanmıştır. Dördüncü sözleşme (SS-4) ise veri aktaranın veri işleyen, veri alıcısının ise veri sorumlusu olduğu durumları içermektedir. Bu sözleşmeler, kişisel verilerin yurt dışına aktarımında tarafların rol ve sorumluluklarını belirleyerek, uyumluluk süreçlerini standart hale getirmek amacıyla düzenlenmiştir. Standart sözleşme, kişisel verilerin korunmasını sağlayan ve uluslararası veri transferini hukuka uygun hale getiren kritik bir mekanizmadır. GDPR ve KVKK kapsamında benzer kurallar öngörülmüş olup, Kurul tarafından belirlenen çerçeveye harfiyen uyulması zorunludur. Bu sayede, bireylerin kişisel verilerinin yurt dışında da güvenli şekilde işlenmesi ve korunması garanti altına alınmaktadır. Teknolojinin hızla geliştiği bu dönemde, veri sorumlularının standart sözleşme esaslarına uygun hareket etmeleri, hukuki uyumluluğun ve bireysel hakların korunmasının temel unsurlarından biri olacaktır.

### d. Yeterli Korumayı Sağlayacak Hükümlerin Yer Aldığı Yazılı Bir Taahhütnamenin Varlığı ve Kurul Tarafından Aktarıma İzin Verilmesi (m.9/4-ç)

KVKK'nın 9. maddesi uyarınca, yeterli korumaya sahip olmadığı belirlenen ülkelere kişisel veri aktarımı, belirli güvencelerin sağlanması koşuluyla gerçekleştirilebilir. Bu kapsamda, eğer aktarım yapılacak ülkeye, üçüncü bir ülke içerisindeki belirli bir sektöre veya uluslararası bir kuruluşa ilişkin Kurul tarafından verilmiş bir yeterlilik kararı bulunmuyorsa, KVKK'nın 5. ve 6. maddelerinde öngörülen şartlardan birinin sağlanması ve ilgili kişinin aktarım yapılan ülkede haklarını kullanabilmesi ile etkili kanun yollarına başvurabilmesi gerekmektedir. Bu koşulların

[211] Daha fazla bilgi için; Veri koruma Derneği, "KVKK Kişisel Verilerin Yurt Dışına Aktarılması Rehberi Soru Cevap Etkinliği", *YouTube*, 15 Mart 2024, https://www.youtube.com/watch?v=l_WnvhXo4uU (Erişim Tarihi: 19.05.2025).

[212] "Standart Sözleşmeler ve Bağlayıcı Şirket Kurallarına İlişkin Dokümanlar Hakkında Kamuoyu Duyurusu", https://kvkk.gov.tr/Icerik/7938/Standart-Sozlesmeler-ve-Baglayici-Sirket-Kurallarina-Iliskin-Dokumanlar-Hakkinda-Kamuoyu-Duyurusu, (Erişim Tarihi: 11.03.2025).

yerine getirilmesi durumunda, yeterli korumayı sağlayan hükümleri içeren yazılı bir taahhütnamenin düzenlenmesi ve Kurul tarafından onaylanması halinde veri aktarımı mümkün olmaktadır.[213] Bu yöntem, 9. maddenin ilk halinde de yer almakta olup, üç ön koşula ek olarak iki alt koşul eklemesi yapılmıştır.[214] Örneğin, Bosch Termoteknik Isıtma ve Klima Sanayi ve Ticaret Anonim Şirketi'nin 15 Şubat 2024 tarihinde yaptığı yurtdışına kişisel veri aktarımıyla ilgili taahhütname başvurusu, Kurul tarafından incelenmiş ve uygun bulunmuştur.[215] Buna ek olarak, ilgili Yönetmelik'in 15. maddesinde taahhütname mekanizması detaylandırılmış ve taahhütnamelerde bulunması gereken asgari unsurlar belirlenmiştir. Ancak taahhütnamelerin incelenme sürecine ilişkin kesin bir zaman sınırı bulunmaması, veri sorumluları açısından belirsizlik yaratmaktadır.[216] Kurul, yurt dışına veri aktarımına ilişkin taahhütnameleri KVKK m.9/f.4'te belirtilen kriterlere göre değerlendirerek izin vermektedir. İlk kez, 9 Şubat 2021'de yayımladığı duyuruda, TEB Arval Araç Filo Kiralama A.Ş. tarafından yapılan taahhütname başvurusuna onay verdiğini kamuoyuna bildirmiştir. Bu duyuruda, ilgili taahhütnamenin kapsamı ve şartları hakkında detaylı bilgi verilmemiştir. Daha sonraki tarihlerde de benzer onaylar[217] verilmiş, ancak bu taahhütnamelerin içeriğine dair ayrıntılar kamuoyu ile paylaşılmamıştır. Bu durum, uygulamada açık rıza dışında yurt dışına veri aktarımı için alternatif bir yolun mümkün olduğunu göstermektedir. Ancak, başvurunun içeriğine dair detaylar paylaşılmamış, sonraki onaylarda da benzer bir yaklaşım benimsenmiştir. Bu durum, açık rıza dışında yurt dışına veri aktarımı için alternatif bir yolun varlığını gösterse de başvuru değerlendirme süresinin belirsizliği ve izin alınmadan aktarımın gerçekleştirilememesi bu yöntemin etkinliğini sınırlandırmaktadır.

---

[213] KVKK, *"Kişisel Verilerin Yurt Dışına Aktarılması Rehberi*", *op. cit.,* s.60.
[214] Kaya, *"KVKK Reformu 2024 Değişiklikleri", op. cit.,* s.43-44.
[215] https://www.kvkk.gov.tr/Icerik/7899/Taahhutname-Basvurusu-Hakkinda-Duyuru, (Erişim Tarihi:12.03.2025).
[216] Çelik, *op. cit.,* s.89-92.
[217] Mehmet Bedii Kaya, Furkan Güven Taştan, *Kişisel Veri Koruma Hukuku,* Ocak, 2025, Çevrimiçi Sürüm, s. 1722. https://mbkaya.com/hukuk/veri-koruma-hukuku.pdf (Erişim Tarihi:12.03.2025).
Yurt Dışına Kişisel Veri Aktarma Süreçleri

- ……
- Bosch Termoteknik Isıtma ve Klima Sanayi ve Ticaret Anonim Şirketi- Taahhütname Başvurusu
- Huawei Telekomünikasyon Dış Ticaret Limited Şirketi- Taahhütname Başvurusu
- Celltrion Healthcare İlaç Sanayi ve Limited Şirketi- Taahhütname Başvurusu
- Google Reklamcılık ve Pazarlama Limited Şirketi- Taahhütname Başvurusu
- Otokoç Otomotiv Ticaret ve Sanayi A.Ş.- Taahhütname Başvurusu
- Türkiye Futbol Federasyonu- Taahhütname Başvurusu
- Decathlon Türkiye- Taahhütname Başvurusu
- TEB Arval- Taahhütname Başvurusu
- Amazon- Taahhütname Başvurusu

Ayrıca, Kurul tarafından yeterli korumaya sahip ülkelerin henüz açıklanmamış olması ve bağlayıcı şirket kurallarından sadece çok uluslu grup şirketlerinin yararlanabilmesi, uygulamada KVKK'ya uygun şekilde yurt dışına veri aktarımı için alternatif yollara olan ihtiyacı artırmaktadır[218].

GDPR'da KVKK'daki taahhütnameye benzer bir mekanizma olarak Madde 46/3, Avrupa Ekonomik Alanı dışına yapılan kişisel veri aktarımlarında yeterli koruma sağlamayan ülkelere veri aktarımı için özel güvenceler belirlenmesini düzenler. Eğer bir ülke GDPR Madde 45'e göre yeterli korumaya sahip değilse, Standart Sözleşme Maddeleri veya Bağlayıcı Şirket Kuralları dışında, ulusal otoritenin önceden onayladığı özel bir sözleşme veya taahhütname ile veri aktarımı mümkündür.[219] Bu hüküm, KVKK'daki taahhütname mekanizmasına benzer olmakla birlikte, GDPR bireysel şirketlerin hazırladığı sözleşmelerin ulusal veri koruma otoritesi tarafından önceden onaylanmasını zorunlu kılarak süreci daha sıkı bir denetime tabi tutmaktadır. Örneğin, Avrupa'da faaliyet gösteren bir anonim şirket, müşteri verilerini işlemek amacıyla ABD'deki bir yan kuruluşuna aktarmak istiyorsa, GDPR m.45 kapsamında yeterlilik kararı bulunmadığından, aktarım ancak m.46/3 çerçevesinde ulusal veri koruma otoritesinin onayına sunulacak özel bir sözleşme veya taahhütname ile mümkün olabilir. Bu mekanizma, KVKK'nın 9. maddesinde düzenlenen taahhütname yoluyla aktarım sistemine benzemektedir. Ancak, GDPR m.46/3 uyarınca bireysel şirketlerin hazırladığı sözleşmelerin önceden onaya tabi olması, GDPR'daki süreci KVKK'dan daha katı bir denetim mekanizmasına dönüştürmektedir. Örneğin, Fransa'da CNIL[220] veya Almanya'da BfDI[221] gibi ulusal veri koruma otoriteleri onay vermezse, anonim şirket ilgili veri aktarımını gerçekleştiremez.

Sonuç olarak, KVKK ve GDPR benzer bir taahhütname mekanizması öngörse de GDPR Madde 46/3 kapsamında getirilen ek onay süreci, Avrupa'daki veri aktarım rejimini daha sıkı bir denetime tabi tutmaktadır.

### 2. ARIZİ VERİ AKTARIMI (m.9/6)

6698 sayılı Kişisel Verilerin Korunması Kanunu'nun 9. maddesinin altıncı fıkrası ile Veri Koruma Yönetmeliği'nin 6. maddesinin ikinci fıkrası ve 16. maddesinin birinci fıkrasında

[218] Çelik, *op. cit.,* s.92.
[219] Öztürk, Çalışkan, Seyhan, *Op. Cit.* s. 127.
[220] Fransız veri koruma otoritesi, Cookies in the Context of the French Data Protection Authority's (CNIL)'ın Google kararı için bknz. https://dergipark.org.tr/tr/download/article-file/2710039, (E.T.: 30.05.2025).
[221] Alman Federal Veri Koruma ve Bilgi Özgürlüğü Komiserliği (Bundesbeauftragter für Datenschutz und Informationsfreiheit – BfDI) Avrupa Veri Koruma Kurulu'nda Almanya'yı temsil eder. Daha fazla bilgi için bknz. https://www.bfdi.bund.de/EN/Home/home_node.html?cms_param3=JSoff&cms_param=1825034415105, (E.T.: 30.05.2025).

belirtildiği üzere, yeterlilik kararının olmadığı ve uygun güvencelerin sağlanamadığı durumlarda, yurtdışına kişisel veri aktarımı yalnızca belirli istisnai koşullar altında gerçekleştirilebilir. Bu çerçevede, veri sorumluları ve veri işleyenler, yalnızca belirli hukuki gerekçelere dayanarak ve sınırlı durumlarda kişisel verileri yurtdışına iletebilir. Bu tür aktarımlar, olağan veri işleme faaliyetleri kapsamında değerlendirilmez; süreklilik taşımayan, öngörülemeyen durumlara özgü ve belirli yasal şartların sağlanması gereken istisnai işlemler olarak kabul edilir.

Avrupa Veri Koruma Kurulu (European Data Protection Board- EDPB) tarafından 25 Mayıs 2018 tarihinde kabul edilen Guidelines 2/2018 on Derogations of Article 49 başlıklı rehberde de istisnai veri aktarımlarının doğası gereği süreklilik arz etmemesi gerektiği vurgulanmaktadır. Buna göre, istisnai veri aktarımları yalnızca geçici durumlar için öngörülmüş olup, veri aktarımının sürekli hale gelmesi durumunda uygun güvencelerin sağlanması zorunlu hale gelecektir[222].

İstisnai veri aktarımı yalnızca KVKK'nın 9. maddesinin altıncı fıkrasında belirtilen sınırlı hallerin varlığı halinde mümkündür:

*a) İlgili kişinin, muhtemel riskler hakkında bilgilendirilmesi kaydıyla, aktarıma açık rıza vermesi.*

*b) Aktarımın, ilgili kişi ile veri sorumlusu arasındaki bir sözleşmenin ifası veya ilgili kişinin talebi üzerine alınan sözleşme öncesi tedbirlerin uygulanması için zorunlu olması.*

*c) Aktarımın, ilgili kişi yararına veri sorumlusu ile başka bir gerçek veya tüzel kişi arasında yapılacak bir sözleşmenin kurulması veya ifası için gerekli olması.*

*ç) Aktarımın üstün bir kamu yararı için zorunlu olması.*

*d) Bir hakkın tesisi, kullanılması veya korunması amacıyla kişisel verilerin aktarılmasının zorunlu olması.*

*e) Fiili imkânsızlık nedeniyle rızasını açıklayamayacak durumda bulunan veya rızasına hukuki geçerlilik tanınmayan kişinin ya da bir başkasının hayatı veya beden bütünlüğünün korunması için kişisel verilerin aktarılmasının zorunlu olması.*

[222] EDPB, 2018, s. 4.

*f) Kamuya veya meşru menfaati bulunan kişilere açık bir sicilden, ilgili mevzuata uygun olarak erişim şartlarının sağlanması ve meşru menfaati olan kişinin talep etmesi kaydıyla aktarım yapılması.*

Bu hükümlerin dar yorumlanması gerektiği ve yalnızca belirli, öngörülemeyen koşullar altında uygulanması gerektiği hem KVKK hem de EDPB tarafından açıkça belirtilmektedir. GDPR'in 49. maddesinde yer alan istisnai veri aktarımları da benzer şekilde sınırlayıcı bir çerçevede değerlendirilmekte olup, veri aktarımının geçici ve münferit olması gerektiği vurgulanmaktadır[223].

EDPB, Schrems II davasında Avrupa Adalet Divanı (CJEU) tarafından getirilen yükümlülüklerin, istisnai aktarım mekanizmalarının kullanılması halinde geçerli olmayabileceğine dair bir yorumda bulunmuştur. Schrems II kararında, yeterlilik kararı olmayan ülkelere kişisel veri aktarımı yapılırken, veri sorumlularının ek teknik, idari ve hukuki önlemler alması gerektiği belirtilmiştir. Ancak, EDPB'nin değerlendirmelerine göre, GDPR madde 49 kapsamında düzenlenen istisnai aktarım halleri bu yükümlülüklerden muaf tutulabilir. Bu istisnai aktarım halleri, olağanüstü ve tek seferlik durumlarla sınırlıdır. Örneğin, bir sözleşmenin ifası için zorunlu olan bir veri aktarımı ya da ilgili kişinin açık rızası ile yapılan bir aktarım, Schrems II'de belirtilen ek önlemler gerektirmeyebilir. Bununla birlikte, EDPB istisnai aktarım mekanizmalarının dar bir çerçevede uygulanması gerektiğini ve sürekli veri akışını sağlamaya yönelik bir yöntem olarak kullanılamayacağını vurgulamaktadır. Sonuç olarak, Schrems II kararı yeterlilik kararının olmadığı durumlarda alternatif koruma mekanizmalarını güçlendirmeyi amaçlarken, EDPB istisnai aktarım hükümlerinin bu kapsamda değerlendirilmediğini ifade etmektedir. Ancak, veri sorumlularının istisnai aktarım yöntemine başvururken gerekli şartları titizlikle değerlendirmesi ve bunun sürekli bir uygulama haline gelmemesi gerektiğini göz önünde bulundurması önem taşımaktadır[224].

İstisnai veri aktarımlarının sürekli hale gelmemesi gerektiği, özellikle Eduardo Ustaran ve Hogan Lovells tarafından hazırlanan European Data Protection Law and Practice adlı çalışmada detaylıca ele alınmıştır. Buna göre, sürekli veya sistematik şekilde tekrar eden veri

[223] Christopher Kuner, GDPR Article 49: The EU General Data Protection Regulation: A Commentary Update of Selected Articles, Christopher Kuner, Lee A. Bygrave, Christopher Docksey, Oxford: Oxford University Press, 2021, s. 202-203. https://ssrn.com/abstract=3839645, (Erişim Tarihi:14.03.2025).
[224] *Ibid., s. 202-206.*

aktarımlarında, istisnai aktarım gerekçesi kullanılamaz ve veri sorumlularının yeterlilik kararı veya uygun güvencelerden birini sağlaması gerekmektedir[225].

Arızi nitelikteki veri aktarımı, yalnızca tek seferlik gerçekleştirilen işlemlerle sınırlı değildir. Asıl önemli olan, bu tür aktarımların düzenli ve sistematik bir veri akışı oluşturmayacak şekilde gerçekleşmesidir. Bu çerçevede, her bir aktarımın özel koşulları dikkate alınarak ayrı ayrı değerlendirilmesi gerekmektedir. Özellikle, GDPR'in 49. maddesinde istisnai durumlar için kullanılan "not repetitive" ifadesi, bu tür aktarımların sürekli tekrar eden işlemler niteliğinde olmaması gerektiğini vurgulamaktadır[226]. European Data Protection Board tarafından hazırlanan kılavuzlarda da bu hususa dikkat çekilerek, istisnai aktarımın olağan bir veri işleme yöntemi olarak benimsenmemesi gerektiği belirtilmiştir. Ayrıca, istisnai veri aktarımı, genel veri işleme süreçlerinden farklı bir statüde değerlendirildiği için, ilgili kişilerin temel hak ve özgürlükleri ön planda tutulmalı ve aktarımın sınırları dar bir yorum çerçevesinde belirlenmelidir. EDPB tarafından da belirtildiği üzere, istisnai veri aktarımlarına son çare olarak başvurulmalı, öncelikle yeterlilik kararı veya uygun güvencelerden birinin sağlanıp sağlanamayacağı değerlendirilmelidir. Dolayısıyla, veri sorumlularının istisnai veri aktarımını istisna olmaktan çıkaracak şekilde sistematik ve sürekli hale getirmemesi büyük önem taşımaktadır.

İstisnai veri aktarımlarında KVKK veya ilgili yönetmeliklerde herhangi bir bildirim yükümlülüğü öngörülmemektedir. Ayrıca, bu tür aktarımlar için Kişisel Verileri Koruma Kurulu'nun önceden onayına da ihtiyaç duyulmamaktadır. Ancak, KVKK'nın 9. maddesinin dokuzuncu fıkrası gereği, Türkiye'nin veya ilgili kişinin menfaatinin ciddi şekilde zarar görebileceği durumlarda, uluslararası sözleşme hükümleri saklı kalmak kaydıyla yalnızca ilgili kamu kurum veya kuruluşunun görüşü alınarak Kurul izni ile yurt dışına veri aktarımı mümkündür.

Anonim şirketler açısından arızi veri aktarımı, yalnızca belirli koşullar altında ve süreklilik arz etmeyen durumlarda gerçekleştirilebilir. Örneğin, yurtdışında bulunan bir yatırımcı ile ortaklık görüşmeleri sırasında, şirketin mali durumuna ilişkin bilgilerin paylaşılması gerektiğinde ve bu bilgilerin içerisinde çalışanlara veya müşterilere ait kişisel veriler yer aldığında, bu tür bir aktarım tek seferlik olduğu sürece arızi kabul edilebilir. Benzer şekilde, bir anonim şirketin

[225] KVKK, *"Kişisel Verilerin Yurt Dışına Aktarılması Rehberi*", *op. cit.,* s.65, Eduardo Ustaran ve Hogan Lovells, European Data Protection Law and Pratice, IAPP Publication, 2023, s. 313, Kuner, GDPR Article 49, s. 846, (Aktaran: KVKK, *"Kişisel Verilerin Yurt Dışına Aktarılması Rehberi*", *op. cit.,* s.65).
[226] Kaya, *"KVKK Reformu 2024 Değişiklikleri", op. cit.,* s.44-45.

yurtdışında taraf olduğu hukuki bir süreçte mahkeme tarafından belirli kişisel verilerin talep edilmesi durumunda, bu aktarım sürekli bir veri akışına dönüşmediği sürece istisnai olarak değerlendirilir. Ayrıca, yurtdışında düzenlenen bir fuarda, potansiyel müşterilerle iş bağlantıları kurmak amacıyla müşteri bilgileri paylaşıldığında, bu paylaşım düzenli bir şekilde yapılmadığı sürece arızi veri aktarımı kapsamında ele alınabilir. Ancak bu tür aktarımlar belirli bir sistematik yapı kazandığında veya düzenli hale geldiğinde arızi aktarım olmaktan çıkar ve genel veri aktarımı kurallarına tabi olur. Dolayısıyla, anonim şirketlerin yurtdışına kişisel veri aktarırken bu işlemi tek seferlik veya belirli bir olay çerçevesinde gerçekleştirmesi, düzenli ve sürekli bir veri akışına yol açmaması ve KVKK m. 9'da belirtilen hukuki dayanaklardan birine dayanması gerekmektedir.

### a. İlgili Kişinin Aktarıma Açık Rıza Vermesi (m.9/6-a)

6698 sayılı Kişisel Verilerin Korunması Kanunu'ndaki değişiklikler öncesinde, yurtdışına veri aktarımı için en yaygın hukuki gerekçelerden biri açık rıza olarak kabul edilmekteydi. Ancak yapılan düzenlemelerle birlikte, açık rızaya dayanarak veri aktarımı yapabilmek için bir dizi ek şartın sağlanması zorunlu hale getirilmiştir. Buna göre, öncelikle aktarım yapılacak ülkeye ilişkin bir yeterlilik kararının bulunmaması, ayrıca ilgili ülkede uygun güvencelerin sağlanmamış olması ve gerçekleştirilecek aktarımın istisnai nitelik taşıması gerekmektedir[227]. Bu değişiklikler, açık rızaya dayalı veri aktarımının uygulama alanını önemli ölçüde daraltmış ve veri sorumlularının alternatif hukuki dayanaklara yönelme ihtiyacını artırmıştır.

Avrupa Birliği Genel Veri Koruma Tüzüğü'nün 49. maddesinde de benzer şekilde, istisnai hallerde açık rıza temelinde veri aktarımına olanak tanınmaktadır. Ancak bu tür aktarımlar, süreklilik arz etmemeli ve yalnızca özel durumlarla sınırlı kalmalıdır. EDPB 2/2018 sayılı kılavuzunda da açık rıza ile gerçekleştirilecek veri aktarımlarında ilgili kişinin riskler hakkında tam ve şeffaf bir şekilde bilgilendirilmesi gerektiği vurgulanmıştır. Buna göre, veri sorumluları yalnızca kişilerin bilinçli ve özgür iradeyle rıza göstermesi halinde, belirli koşullar altında veri aktarımı gerçekleştirebilecektir.

Kanunda yapılan değişiklikler kapsamında, geçici bir düzenlemeyle eski hükmün belirli bir süre daha yürürlükte kalması sağlanmış ve açık rızaya dayalı veri aktarımının 1 Eylül 2024 tarihine kadar eski kurallara göre devam etmesine olanak tanınmıştır. Ancak bu tarihten itibaren, yurtdışına kişisel veri aktarımı mutlaka güncellenen kanun hükümlerine uygun şekilde

[227] Mehmet Bedi Kaya, "KVKK Reformu 2024 Değişiklikleri", Dijital Baskı v1.0- Mart 2024, s.75. *https://mbkaya.com/hukuk/kvkk-reformu.pdf,* (Erişim Tarihi:13.01.2025).

yürütülmek zorundadır. Ayrıca, açık rızaya dayalı veri aktarımlarında ilgili kişiye yönelik özel bir aydınlatma yükümlülüğü getirilmiştir. Kanun metninden de anlaşılacağı üzere, veri sorumlularının, yurtdışına aktarımın olası riskleri konusunda kişileri ayrıntılı bir şekilde bilgilendirmesi zorunludur.[228] Bu bilgilendirmenin, ilgili kişinin aktarımın sonuçlarını tam olarak anlayabileceği şekilde yapılması gerekmektedir.

Bu çerçevede, 1 Eylül 2024 sonrası dönemde veri sorumlularının, yurtdışına veri aktarımı süreçlerini gözden geçirmesi, alternatif hukuki dayanakları değerlendirmesi ve açık rıza temelinde gerçekleştirilecek aktarımlar için gerekli aydınlatma prosedürlerini eksiksiz yerine getirmesi gerekmektedir. Aksi takdirde hem KVKK hem de GDPR kapsamındaki yaptırımlarla karşı karşıya kalınabilir. Anonim şirketler açısından yurtdışına veri aktarımında açık rızanın daraltılması, özellikle çok uluslu şirketler veya yurtdışında iş ortakları bulunan firmalar için önemli sonuçlar doğurmaktadır. Örneğin, Türkiye'de faaliyet gösteren bir anonim şirketin, yurtdışındaki bir grup şirketine çalışanlarının veya müşterilerinin kişisel verilerini aktarmak istemesi durumunda, eskiden yalnızca açık rıza yeterli bir hukuki dayanak olarak kabul edilirken, yeni düzenlemeyle birlikte açık rızaya dayalı veri aktarımının belirli şartlara tabi olduğu görülmektedir. Bir anonim şirket, yurtdışındaki bir iştirakine çalışanlarının maaş ödemeleriyle ilgili bilgileri aktarmak istiyorsa, artık sadece açık rızaya dayanarak bu aktarımı gerçekleştirmesi mümkün olmayabilir. Bunun yerine, aktarımı mümkün kılacak diğer hukuki dayanakları değerlendirmesi veya yeterlilik kararı ve uygun güvenceler çerçevesinde hareket etmesi gerekecektir.

Kişisel verilerin yurt dışına aktarımı için ilgili kişinin açık rızasının alınması, KVKK m.9/6-a bendinde düzenlenen temel hukuki dayanaklardan biri olsa da açık rıza alınması, veri sorumlusu açısından risk taşımaktadır; çünkü rızanın hukuka uygun, özgür iradeye dayalı, bilgilendirilmiş ve spesifik olması gerekmektedir. Bu nedenle, anonim şirketler, açık rıza temelinde yurt dışına veri aktarımı yapmadan önce kapsamlı bir risk değerlendirmesi ve olası riskler hakkında aydınlatma yapmış olması gerekmektedir[229]. Örneğin, bir teknoloji şirketi, kullanıcılarından pazarlama amaçlı yurt dışı iş ortaklarına veri aktarımı için açık rıza aldığında, aktarılacak verilerin hassasiyeti, alıcı ülkedeki veri koruma düzeyi, aktarım yöntemlerinin güvenliği ve olası veri ihlallerinin etkileri değerlendirilmelidir. Ayrıca, kullanıcıların rızasını geri çekme hakları ve bu sürecin işletilme şekli de analiz edilmelidir. Bu risk değerlendirmesi sonucunda, şirket gerekli güvenlik önlemlerini almalı ve aktarım sürecinde hesap verebilirlik ilkesine

[228] Öztürk, Çalışkan, Seyhan, *op. cit.* s. 128.
[229] *Ibid.,* s.128.

uygun olarak kayıtlar tutmalıdır. Böylece, açık rızaya dayalı veri aktarımı hem hukuken sağlam temellere oturur hem de olası veri koruma riskleri minimize edilmiş olur.

### b. İlgili Kişi ile Veri Sorumlusu Arasındaki Bir Sözleşmenin İfası veya İlgili Kişinin Talebi Üzerine Alınan Sözleşme Öncesi Tedbirlerin Uygulanması (m.9/6-b)

KVKK'nın 9. maddesinin 6. fıkrasının (b) bendi, kişisel verilerin işlenmesinin hukuka uygun olduğu hallerden birini düzenlemektedir. Bu hüküm, veri sorumlusunun, ilgili kişiyle arasındaki bir sözleşmeyi yerine getirebilmesi veya ilgili kişinin talebi doğrultusunda sözleşme öncesi hazırlık işlemlerini gerçekleştirebilmesi için kişisel verileri işleyebilmesine olanak tanımaktadır. Bu hukuki dayanak, günlük hayatta sıklıkla karşılaştığımız birçok veri işleme faaliyetinin temelini oluşturmaktadır. Örneğin, bir e-ticaret platformundan ürün satın aldığımızda, adımızın, soyadımızın, adresimizin ve iletişim bilgilerimizin işlenmesi, aramızdaki satış sözleşmesinin ifası için zorunludur. Bir e-ticaret platformu işleten XYZ Anonim Şirketi, Türkiye'de mukimdir ve uluslararası satış yapmaktadır. Platform üzerinden bir Alman vatandaşı, Türkiye'den ürün satın almak için sipariş oluşturur. Siparişin işlenebilmesi ve teslim edilebilmesi için, müşteriye ait ad, soyad, iletişim ve teslimat adresi gibi kişisel veriler, XYZ A.Ş. tarafından yurt dışındaki lojistik hizmet sağlayıcısına (örneğin Almanya'daki bir kargo şirketine) aktarılır. Bu durumda veri aktarımı, ilgili kişi (müşteri) ile XYZ A.Ş. arasında kurulan satış sözleşmesinin ifası için zorunlu bir veri işleme faaliyeti niteliğindedir. Dolayısıyla, KVKK m.9/6-b hükmü uyarınca bu veri aktarımı, açık rıza aranmaksızın ve Kurul izni gerekmeksizin hukuka uygun kabul edilecektir. Aynı şekilde, bir Türk vatandaşının yurt dışında bir eğitim kurumuna kayıt yaptırmak istemesi hâlinde, Türkiye'deki bir özel eğitim danışmanlığı hizmeti sunan ABC A.Ş., öğrencinin başvurusu doğrultusunda öğrenciye ait kimlik, not dökümü ve iletişim bilgilerini yurt dışındaki üniversiteye aktardığında da benzer şekilde sözleşme öncesi tedbirin uygulanması kapsamında veri aktarımı meşru olacaktır. Bu ve benzeri durumlarda, kişisel verilerin işlenmesi, sözleşme ilişkisinin kurulması ve yürütülmesi için kaçınılmaz bir gereklilik olarak ortaya çıkar. Ancak bu hukuki dayanağın sınırları da bulunmaktadır. KVKK, kişisel verilerin yalnızca sözleşmenin ifası veya sözleşme öncesi tedbirlerin uygulanması için gerekli olduğu ölçüde işlenmesine izin vermektedir[230]. Bu amaçlar

[230] Kişisel Verileri Koruma Kurulu'nun 02.08.2018 tarihli, "İşlenme Amacının Gerektirdiğinden Fazla Kişisel Veri İşlenmesi/Aktarılması (Veri Minimizasyonu İlkesine Aykırılık)" konulu kararında; mahkemenin veri sorumlusundan ilgili kişi hakkında talep ettiği kişisel verilerin, Kanun'un 9. maddesinin 1. fıkrasının (b) bendi kapsamında yani "ilgili kişi ile veri sorumlusu arasındaki bir sözleşmenin ifası veya ilgili kişinin talebi üzerine alınan sözleşme öncesi tedbirlerin uygulanması" amacıyla zorunlu olması gerekirken, veri sorumlusunun gereğinden fazla kişisel veri aktarımında bulunmasının bu şartı sağlamadığı belirtilmiştir. Bu durum, Kanun'un 4. maddesinin 1. fıkrasının (ç) bendindeki "işlendikleri amaçla bağlantılı, sınırlı ve ölçülü olma" ilkesine aykırı olup,

dışında kalan veya gereksiz olan kişisel veri işlenmesi bu kapsamda değerlendirilemez. Veri sorumlusu, sözleşme ilişkisi veya sözleşme öncesi süreçlerle doğrudan ilgisi olmayan kişisel verileri işlememeli ve ilgili kişilerin mahremiyetine saygı göstermelidir[231]. Sonuç olarak, KVKK'nın 9/6-b maddesi, sözleşme ilişkilerinin kurulması ve yürütülmesi açısından kritik bir öneme sahiptir. Bu hüküm sayesinde, veri sorumluları, ilgili kişilerle olan sözleşmelerini etkin bir şekilde yerine getirebilir ve potansiyel sözleşme ilişkileri için gerekli hazırlıkları yapabilirler. Ancak bu yetkinin, kişisel verilerin korunması ilkesiyle dengeli bir şekilde kullanılması ve yalnızca zorunlu hallerde veri işlenmesi gerektiği unutulmamalıdır. Bu denge hem ticari faaliyetlerin sürdürülebilirliği hem de bireylerin temel hak ve özgürlüklerinin korunması açısından hayati önem taşımaktadır.

Örneğin, bir grup anonim şirketi bünyesinde faaliyet gösteren şirketlerden A Anonim Şirketi, müşterileriyle yaptığı sözleşme kapsamında elde ettiği kişisel verileri, sözleşme ifası için gereken sınırlar dahilinde B Anonim Şirketi ile paylaşabilir. Ancak, B Anonim Şirketi bu verileri, sözleşmenin kapsamında belirtilmeyen pazarlama faaliyetleri veya farklı ticari amaçlarla kullanması halinde, bu durum KVKK m.9/6-b hükmüne aykırı olur. Böyle bir aktarım, hem sözleşme amacını aşan gereksiz veri işleme olarak kabul edilir hem de kişisel verilerin hukuka aykırı kullanımı kapsamında değerlendirilir. Bu nedenle grup şirketleri, yurt dışına veri aktarırken sözleşmenin sınırlarına uygun hareket etmeli, veri işleme amaçlarını açıkça belirlemeli ve gerektiğinde ilgili kişilerden yeni rızalar almalıdır.

### c. İlgili Kişi Yararına Veri Sorumlusu ve Diğer Bir Gerçek veya Tüzel Kişi Arasında Yapılacak Bir Sözleşmenin Kurulması veya İfası İçin Zorunlu Olması (m.9/6-c)

6698 sayılı Kişisel Verilerin Korunması Kanunu'nun 9. maddesinin 6. fıkrasının (c) bendi, kişisel verilerin yurt dışına aktarımına açık rıza olmaksızın izin verilen istisnai durumlardan biridir. Buna göre, veri sorumlusu ile başka bir gerçek veya tüzel kişi arasında yapılacak bir sözleşmenin ilgili kişi yararına kurulması veya ifası için kişisel verilerin aktarılmasının zorunlu olması hâlinde, açık rıza aranmaksızın yurt dışına veri aktarımı mümkündür. Burada önemli olan, sözleşmenin veri sahibinin doğrudan menfaatini gözetiyor olması ve aktarımın bu sözleşmenin kurulması ya da ifası için gerçekten gerekli bulunmasıdır[232]. Ancak burada dikkat

veri sorumlusunun ilgili kişiye ait kişisel verilerin güvenliğini sağlamaması sebebiyle Kanun'un 12. maddesinin 1. fıkrası ve 18. maddesi uyarınca idari yaptırım uygulanmasına karar verilmiştir.

[231] Kişisel Verilerin Korunması Kanunu, m.5/2; Kişisel Verilerin Korunması Kurulu, "Kişisel Verilerin İşlenme Şartları," (Erişim Tarihi: 24.05.2025).

[232] Öztürk, Bahri, Elif Altınok Çalışkan, Serkan Seyhan, *op. cit.,* s.129.

edilmesi gereken diğer bir husus, bu tür aktarımların sürekli bir veri aktarım politikası olarak değil, arızi (tekil ve zorunlu durumlar) kapsamında değerlendirilmesidir. Zira bu bentte düzenlenen hâller, veri aktarımının olağan ve sistematik bir şekilde sürdürülmesini değil, ilgili kişinin belirli bir işlemden faydalanmasını sağlayan sınırlı ve geçici veri paylaşımlarını kapsar. Örneğin, Türkiye'de mukim bir bireyin, Avrupa'daki bir anonim şirketten satın aldığı ürünün teslimi için gönderim yapılması gerektiğinde, alıcı bilgileri (isim, adres, telefon numarası gibi) lojistik sağlayıcıya aktarılabilir. Bu aktarım, ilgili kişinin yararına kurulan bir satış ve teslimat sözleşmesinin ifası için zorunlu olduğundan, KVKK m.9/6-c kapsamında değerlendirilebilir. Aynı şekilde, bir Türkiye merkezli anonim şirketin, yurt dışında yaşayan müşterisi adına üçüncü bir ülkede otel rezervasyonu yaparken, müşterinin kimlik ve iletişim bilgilerinin ilgili otelle paylaşılması da benzer biçimde, ilgili kişinin yararına kurulan hizmet sözleşmesinin ifası amacıyla ve arızi nitelikte gerçekleşen bir veri aktarımıdır.

Yine yurt dışında yaşayan bir kişinin bir Türk bankasında bulunan hesabına, başka bir ülke bankasından gönderim yapılması sırasında, alıcı olarak ilgili kişinin bilgileri yabancı bankayla paylaşılabilir. Benzer şekilde, yurt dışı menşeili bir havayolu şirketinden Türkiye'de ikamet eden kişi adına bilet satın alınması sırasında, ilgili kişinin kimlik ve iletişim bilgilerinin söz konusu şirkete aktarılması da bu kapsama girer. Aktarımın amacı sözleşmenin ifası olduğu ve ilgili kişinin doğrudan yararına olduğu için, bu bent çerçevesinde açık rıza aranmaz.

Bir X Turizm A.Ş. unvanlı bir seyahat acentesi, Türkiye'de yerleşik bir anonim şirkettir. Bu şirket, müşterisi adına yurt dışı uçak bileti ve otel rezervasyonu işlemleri gerçekleştirmektedir. Müşteri, Paris'e yapacağı bir seyahat için bu X Turizm A.Ş.'ye başvurduğunda, şirket, müşteriye ait pasaport bilgileri, iletişim bilgileri ve seyahat tercihleri gibi kişisel verileri, yurt dışında yerleşik havayolu şirketine ve otel zincirine aktarmak zorundadır. Bu durumda, veri aktarımı, ilgili kişinin (müşterinin) doğrudan tarafı olmadığı ancak yararına kurulacak bir sözleşmenin (örneğin uçuş sözleşmesi veya otel rezervasyonu sözleşmesi) ifası için zorunludur. Bu nedenle X Turizm A.Ş., müşteriye ait verileri, KVKK m.9/6-c uyarınca açık rıza olmaksızın yurt dışına aktarabilir.

Benzer şekilde, bir Y A.Ş. unvanlı bir ihracat firması, müşterisi olan bir kişinin siparişi üzerine, yurtdışında yerleşik bir üretici şirketle sözleşme yaparak ürün tedariği sağlamaktadır. Bu kapsamda, müşteriye ilişkin teslimat adresi, iletişim bilgileri ve özel isteklerine dair kişisel veriler, söz konusu üretici firmaya aktarılmaktadır. Bu aktarım da ilgili kişinin yararına yapılacak bir sözleşmenin ifası için zorunlu olması nedeniyle KVKK m.9/6-c uyarınca hukuka uygundur.

Bu istisnai aktarım kapsamında, veri sorumlusunun yurt dışı alıcı ile sözleşme yapması, veri aktarımının hukuka uygun ve sınırlandırılmış olmasını sağlamak amacıyla önem taşır. Bu noktada, KVKK'nın 12. maddesiyle düzenlenen hesap verilebilirlik ilkesi devreye girer; veri sorumlusu, bu aktarım sürecinde hem teknik hem idari tedbirler alarak, kişisel verilerin güvenliğini sağlamalı ve aktarımın şeffaflığını temin etmelidir. Benzer şekilde, GDPR' nın 5/2 ve 24. maddeleri uyarınca veri sorumluları, kişisel verilerin işlenmesinde sadece kanuni dayanak sağlamakla kalmayıp, bu süreçlerde hesap verebilirlik sistemleri kurarak uyum sağladıklarını kanıtlamak zorundadırlar. Dolayısıyla, m.9/6-c bendinde öngörülen aktarım durumlarında, veri sorumlularının KVKK m.12 ve GDPR'daki hesap verilebilirlik ilkesi doğrultusunda, söz konusu aktarımı sınırlandırması, denetlemesi ve olası risklere karşı uygun tedbirleri alması gerekmektedir. Bu yaklaşım hem ilgili kişinin menfaatinin korunmasını hem de kişisel verilerin uluslararası arenada hukuka uygun şekilde işlenmesini mümkün kılar.

**d. Aktarımın Üstün Kamu Yararı İçin Zorunlu Olması (madde 9/6-ç)**

Madde 9/6-ç'ye göre, kişisel verilerin aktarılabilmesi için bu aktarımın kamu yararına ve toplumun genel çıkarlarına hizmet etmesi gerekir. Bu durumda, veri sahibinin rızasına gerek olmadan kişisel veriler, hukuken belirli bir kamu yararı ve kamu düzeni için ilgili mercilere veya kişilere aktarılabilir. Örneğin, kamu güvenliği ya da suçların önlenmesi amacıyla verilerin aktarılması, sağlık ve güvenlik gibi toplum sağlığını ilgilendiren durumlar, kriz ve afet gibi olağanüstü hallerde kişisel verilerin aktarılması bu kapsamda değerlendirilebilir. Bu istisna, kişisel verilerin korunması ilkesine rağmen, bazı özel durumlarda daha geniş kamu çıkarlarını korumak için bir denge sağlar. Ancak, verilerin aktarılabilmesi için aktarımın gerçekten zorunlu olması ve yalnızca belirli durumlarla sınırlı olması gerekir. Verilerin aktarımı her zaman zorunlu ve orantılı olmalı, sadece üstün kamu yararına dayalı durumlarda bu hak kullanılabilir.

Türkiye'de faaliyet gösteren ve sağlık alanında araştırmalar yapan XGen A.Ş. unvanlı bir anonim şirket, yerli gönüllülerin katılımıyla gerçekleştirdiği epidemiyolojik bir klinik araştırma projesi kapsamında, toplanan verileri uluslararası bir sağlık otoritesiyle (örneğin Dünya Sağlık Örgütü- WHO) paylaşmak zorundadır. Araştırma, halk sağlığını ilgilendiren yeni bir enfeksiyon hastalığına karşı geliştirilecek koruyucu önlemlerin belirlenmesine yöneliktir. Bu bağlamda, gönüllülerin yaş, cinsiyet, klinik bulguları, tıbbi geçmişi gibi kişisel sağlık verileri, sınırlı ve anonimleştirme ilkelerine uygun olarak yurt dışına aktarılacaktır. Bu aktarım, bireylerin değil toplumun genel sağlığının korunması, ulusal ve uluslararası salgınla mücadele stratejilerinin geliştirilmesi ve üstün kamu yararının sağlanması amacıyla zorunludur.

Dolayısıyla, bu tür bir veri aktarımı, KVKK m.9/6-ç kapsamında değerlendirilerek, açık rıza olmaksızın ve Kurul iznine tabi olmadan hukuka uygun kabul edilebilir.

**e. Bir Hakkın Tesisi, Kullanılması veya Korunması İçin Kişisel Verilerin Aktarılmasının Zorunlu Olması (m.9/6-d)**

KVKK madde 9/f.6-d, bir hakkın tesisi, kullanılması veya korunması için kişisel verilerin aktarılmasının zorunlu olabileceğini belirtir. Bu durumda, kişisel verilerin aktarılması, bir bireyin hukuki haklarını kullanabilmesi veya savunabilmesi için gerekli olabilir. Örneğin, bir kişi bir dava açtığında, davanın seyrine ilişkin verilerin ilgili mahkemeye veya avukata aktarılması gerekebilir. Bu tür verilerin aktarımı, veri sahibinin rızasına gerek olmadan, yalnızca hakkın kullanılması ya da korunması için gerekli olduğu durumlarda gerçekleşebilir. Ancak, verilerin aktarılması, yalnızca belirli bir hakkın tesisi, kullanılması ya da korunması için gerçekten zorunlu ise mümkündür. Bu durum, kişisel verilerin korunması ilkesine bir istisna teşkil eder ve yalnızca ilgili hakkın korunabilmesi için gerekli olan veriler aktarılabilir.

Afetle mücadele kapsamında faaliyet gösteren anonim şirketler için bu hüküm önemli bir istisna oluşturmaktadır. Örneğin, uluslararası insani yardım faaliyetlerinde bulunan bir anonim şirket, doğal afet sonrasında mağduriyet yaşayan müşterilerinin sağlık durumları, iletişim bilgileri ve konum verileri gibi özel nitelikli ve diğer kişisel verilerini, afet bölgesine hızlı ve etkin müdahale sağlanması amacıyla yurt dışındaki ilgili yardım kuruluşları veya devlet kurumlarıyla paylaşabilir. Bu aktarım, mağdurların haklarının korunması ve afetle mücadele sürecinin etkin yönetilmesi için zorunlu olduğundan, KVKK m.9/6-d bendine dayanılarak gerçekleştirilebilir. Böylece, afet mağdurlarının temel haklarının korunması ve gerekli desteklerin sağlanması amacıyla anonim şirketlerin veri aktarımı yapması hukuki zemine oturtulmuş olur.

Türkiye'de faaliyet gösteren X Teknoloji A.Ş., yurt dışındaki bir yazılım sağlayıcısına karşı, sözleşmeden doğan alacaklarının ödenmemesi nedeniyle, Almanya'da dava açmak üzere bir hukuk bürosuna vekâlet verir. Dava sürecinde, söz konusu şirketin alacaklarının kanıtlanabilmesi için Türkiye'deki müşteriye ait sözleşme belgeleri, fatura kayıtları ve ticari işlem geçmişi gibi belgeler ve belgelerde yer alan müşteriye ait kişisel veriler, şirketin yurt dışındaki avukatına iletilmek zorundadır. Bu aktarım işlemi, X Teknoloji A.Ş.'nin hukuki alacağını tahsil etmek için bir hakkın kullanılmasına yönelik bir işlem olduğundan ve bu hakkın kullanılabilmesi için kişisel verilerin aktarımı zorunlu olduğundan, KVKK m.9/6-d hükmü uyarınca açık rıza aranmaksızın ve Kurul iznine gerek kalmaksızın yurt dışına veri aktarımı yapılabilir.

**f. Fiili İmkânsızlık Nedeniyle Rızasını Açıklayamayacak Durumda Bulunan veya Rızasına Hukuki Geçerlilik Tanınmayan Kişinin Kendisi ya da Bir Başkasının Hayatın veya Beden Bütünlüğünün Korunması İçin Kişisel Verilerin Aktarılmasının Zorunlu Olması (m.9/6-e)**

KVKK madde 9/f.6-e, fiili imkansızlık nedeniyle rızasını açıklayamayan veya rızasına hukuki geçerlilik tanınmayan kişilerin, kendilerinin ya da başkalarının hayatının veya beden bütünlüğünün korunabilmesi amacıyla kişisel verilerinin aktarılmasını zorunlu kılar. Bu durumda, veri sahibinin rızası alınamadan, ancak bir kişinin acil sağlık durumu veya tehlikede olan hayatının korunması gibi durumlarla ilgili olarak, kişisel veriler, sağlık hizmetleri sağlayıcıları veya yetkili mercilerle paylaşılabilir. Örneğin, bir kişi bilinçsiz haldeyken, hayatını kurtarmak amacıyla gerekli tıbbi bilgilere sağlık profesyonelleri erişebilir. Bu tür bir aktarım, rıza alınamadığı veya hukuken geçerli rıza sağlanamadığı durumlarda bile, sadece hayatın veya beden bütünlüğünün korunması için yapılabilir.

Türkiye'de faaliyet gösteren XGlobalMed Sağlık Hizmetleri A.Ş. unvanlı bir anonim şirket, yurt dışından Türkiye'ye gelen turistlere özel sağlık hizmeti sunmaktadır. İstanbul'da tatilde olan ve ciddi bir trafik kazası geçiren bir Alman vatandaşı, bilinci kapalı şekilde hastaneye getirilmiştir. Hayati tehlike arz eden tıbbi müdahale sürecinde, hastanın yurtdışındaki özel sağlık sigortası şirketine bilgi verilmesi ve hastaya ait tıbbi geçmiş, kimlik ve mevcut sağlık durumu verilerinin aktarılması gerekmiştir. Bu durumda, hastanın rızası alınamamaktadır (fiili imkânsızlık) ve veri aktarımı, hayatının veya beden bütünlüğünün korunması amacıyla acilen gereklidir. Ayrıca sigorta teminatının sağlanabilmesi ve sağlık hizmetinin aksamadan sürdürülebilmesi için veri aktarımı zorunludur. Dolayısıyla bu aktarım, KVKK m.9/6-e hükmü uyarınca, açık rıza aranmaksızın ve Kurul iznine tabi olmadan hukuka uygun şekilde gerçekleştirilebilir.

**g. Kamuya ve Meşru Menfaati Bulunan Kişilere Açık Bir Sicilden İlgili Mevzuatta Sicile Erişmek İçin Gereken Şartların Sağlanması ve Meşru Menfaati Olan Kişinin Talep Etmesi Kaydıyla Aktarım Yapılması (m.9/6-f)**

KVKK madde 9/f.6-f, kamuya ve meşru menfaati bulunan kişilere açık bir sicilden, ilgili mevzuatta sicile erişmek için gereken şartların sağlanması ve meşru menfaati olan kişinin talep etmesi kaydıyla kişisel verilerin aktarılmasını düzenler. Bu durumda, kamuya açık olan bir

sicilde yer alan kişisel veriler[233], sicile erişim hakkı bulunan ve meşru menfaati olan kişiler tarafından talep edildiğinde, belirli yasal şartlar çerçevesinde aktarılabilir. Örneğin, ticaret sicilinde yer alan bilgiler, ticaretle ilgili bir menfaati bulunan kişilere, yasal gereklilikleri yerine getirdikleri takdirde sağlanabilir. Bu aktarım, sadece meşru bir menfaatin varlığına dayalı olarak ve ilgili mevzuatta belirlenen şartlara uyularak yapılabilir.

Türkiye'de faaliyet gösteren XYZ Global Danışmanlık A.Ş., uluslararası yatırımcılara Türkiye'deki şirketler hakkında mali ve ticari bilgi sağlayan bir anonim şirkettir. Şirket, Avrupa'daki bir yatırımcı firmanın talebi üzerine, Türkiye'de yerleşik bir anonim şirkete ait ticaret unvanı, faaliyet konusu, sermaye miktarı, yönetim kurulu bilgileri ve tescil bilgileri gibi verileri, Türkiye Ticaret Sicili Gazetesi ve MERSİS gibi kamuya açık sicil kayıtlarından temin ederek ilgili yabancı yatırımcıya iletir. Bu aktarım, Ticaret Sicili Yönetmeliği gereğince kamuya açık olan ve belirli şartları sağlayan herkes tarafından erişilebilen verilerden oluşmaktadır. Ayrıca, veriyi talep eden yabancı yatırımcı şirketin, bu bilgilere dayalı olarak meşru yatırım değerlendirmesi yapma menfaati de bulunmaktadır. Bu nedenle yapılan aktarım, KVKK m.9/6-f kapsamında değerlendirilerek, açık rıza aranmaksızın ve Kurul iznine gerek olmaksızın hukuka uygun kabul edilir.

### 3. KAMU KURUM VE KURULUŞLARININ KAMU HUKUKU TABİ FAALİYETLERİ YÖNÜNDEN SINIFLANDIRMA (m.9/7)

KVKK'nın 9. maddesinin 7. fıkrası, kamu kurum ve kuruluşlarının kamu hukuku tabi faaliyetleri çerçevesinde kişisel verileri yurt dışına aktarırken, belirli koşullar altında bazı istisnalar getirir. Bu istisnalar, özellikle kamu yararının ön planda olduğu durumlarda, veri aktarımının daha hızlı ve etkin bir şekilde gerçekleştirilmesini amaçlar. Kamu kurumları, yurt dışına veri aktarımı yaparken öncelikle aktarımın yapılacağı ülkenin KVKK tarafından yeterli koruma sağlayan ülkeler listesinde olup olmadığını kontrol etmelidir. Eğer aktarım yapılacak ülke bu listede yer almıyorsa, kamu kurumu uygun güvenceler sağlamak zorundadır. Bu bağlamda, KVKK'nın 9/7 maddesi, kamu kurum ve kuruluşlarının kamu hukuku tabi faaliyetleri kapsamında yurt dışına veri aktarımı yaparken, bazı durumlarda ilgili kişinin açık

[233] Burada sözü edilen siciller, yalnızca kamu otoriteleri tarafından tutulan nüfus, tapu ya da adli sicil kayıtlarıyla sınırlı olmayıp; ticaret sicili, marka-patent sicili, dernek ve vakıf sicili gibi özel hukuk tüzel kişiliklerine ilişkin ve kamunun erişimine açık veri tabanlarını da kapsayabilir. Örneğin, bir anonim şirketin birleşme veya devralma işlemlerinde, taraf şirketlerden birinin ya da üçüncü bir yatırımcının, Türkiye Ticaret Sicili Gazetesi'nde yayımlanmış veya ticaret sicili kayıtlarında yer alan bilgileri, ilgili mevzuatta öngörülen şartlar sağlandığında elde etmesi mümkündür. Bu aktarım işlemi, yalnızca açık ve belirli bir menfaate dayanmalı ve sicile erişim koşulları objektif ve hukuken öngörülebilir şekilde sağlanmalıdır. Böylece kişisel veri aktarımı hem şeffaflık hem de veri güvenliği ilkeleri çerçevesinde gerçekleştirilmiş olur.

rızasını aramaktan veya sözleşme gerekliliklerine uymaktan muaf tutulabileceğini öngörür. Bu istisnalar, genellikle milli güvenlik, kamu sağlığı, suç soruşturması veya uluslararası iş birliği gibi önemli kamu menfaatlerinin söz konusu olduğu hallerde geçerlidir[234]. Örneğin, bir kamu kurumu, uluslararası bir suç örgütüyle mücadele amacıyla yabancı bir ülkenin emniyet teşkilatıyla veri paylaşımında bulunabilir. Bu durumda, veri aktarımının hızlı ve etkin bir şekilde gerçekleştirilmesi, suçla mücadeledeki başarı için kritik öneme sahip olabilir. Bu nedenle, KVKK, bu tür durumlarda ilgili kişinin açık rızasını aramaktan veya sözleşme gerekliliklerine uymaktan muafiyet tanıyabilir. Ancak, bu istisnaların uygulanması, kamu kurum ve kuruluşlarının keyfi davranabileceği anlamına gelmez. Veri aktarımının, KVKK'nın temel ilkelerine ve amaçlarına uygun olması, ölçülü ve orantılı olması, ilgili kişinin temel hak ve özgürlüklerine saygı gösterilmesi gibi hususlar, her zaman gözetilmelidir. Ayrıca, veri aktarımı hakkında ilgili kişilerin bilgilendirilmesi ve gerekli güvenlik önlemlerinin alınması da önemlidir.

Türkiye'de faaliyet gösteren ve ilaç üretimi yapan XPharmaMed İlaç Sanayi A.Ş., Sağlık Bakanlığı'nın ruhsat denetimine tabi bir anonim şirketini örnek olarak ele alalım. Bu şirketin üretim süreçlerine ilişkin veriler, Sağlık Bakanlığı tarafından uluslararası ilaç denetim birliği olan PIC/S (Pharmaceutical Inspection Co-operation Scheme) ile yapılan resmi iş birliği çerçevesinde, ilaç güvenliği ve ruhsatlandırma standartlarının uyumlaştırılması amacıyla yurt dışına aktarılmaktadır. Bu aktarım, XPharmaMed A.Ş.'nin değil, kamu otoritesinin kamu hukuku çerçevesindeki bir görevini — yani halk sağlığını koruma ve uluslararası denetim iş birliklerini yürütme yükümlülüğünü — yerine getirmesi için yapılmaktadır. Dolayısıyla, verilerin yurt dışına aktarımı, KVKK m.9/7 uyarınca değerlendirilir ve kamu kurumunun kamu görevi kapsamında gerçekleştirdiği bu faaliyet nedeniyle, ayrıca açık rıza veya Kurul izni aranmaksızın mümkündür.

## 4. SONRAKİ AKTARIMLARDA VERİ GÜVENLİĞİ (m.9/8)

Kişisel verilerin yurtdışına aktarımı sürecinde, veri sorumluları ve veri işleyenler yalnızca ilk aktarımı değil, sonraki aktarımları da gözetmekle yükümlüdür. KVKK'nın 9. maddesinin sekizinci fıkrası ve GDPR'daki benzer düzenlemeler doğrultusunda, yurtdışına aktarılan kişisel verilerin daha sonra başka bir ülkeye veya uluslararası kuruluşlara iletilmesi halinde de KVKK'daki güvencelerin sağlanması zorunludur. Yeni düzenlemelerle birlikte, veri

[234] Kişisel Verileri Koruma Kurumu, *Kişisel Verilerin Yurt Dışına Aktarılması Rehberi*, Ankara, 2021, s. 12-13, https://www.kvkk.gov.tr/Icerik/8142/Kisisel-Verilerin-Yurt-Disina-Aktarilmasi-Rehberi, Erişim Tarihi: 04.05.2025.

sorumluları ve veri işleyenlerin, kişisel verilerin aktarılacağı ülke veya organizasyonun veri koruma rejimi hakkında daha detaylı bilgi edinmeleri ve uygun tedbirleri almaları gerekmektedir. Bu bağlamda, veri aktarımı yapılan ülkenin veya organizasyonun yeterli veri koruma seviyesine sahip olup olmadığını ve aktarımın risklerini değerlendirmek amacıyla Veri Transferi Etki Analizi (Transfer Impact Assessment- TIA) yapılması zorunlu hale gelmiştir. GDPR'ın 49. maddesi[235] veri aktarımı sırasında "uygun güvenceler" sağlanmasını şart koşarken, Schrems II kararı sonrasında Avrupa Adalet Divanı, AB dışına veri aktarımı yapan şirketlerin yalnızca Standart Sözleşme Maddeleri (SCC) ile yetinmeyip, TIA yaparak ek önlemler almasını gerektirmiştir[236]. GDPR kapsamında TIA'nın temel unsurları arasında aktarımın hukuki dayanağının belirlenmesi, alıcı ülkenin mevzuatının değerlendirilmesi, yetkili makamların erişim yetkilerinin incelenmesi ve ek güvencelerin sağlanması bulunmaktadır[237]. EDPB' de bu sürece ilişkin rehberler[238] yayımlayarak, aktarım zincirinin haritalandırılması, üçüncü ülkenin hukuki çerçevesinin incelenmesi, SCC ve BCR kullanımının değerlendirilmesi gibi adımların izlenmesi gerektiğini vurgulamaktadır. KVKK'da doğrudan TIA zorunluluğuna ilişkin bir hüküm bulunmasa da 9. maddenin 8. fıkrası gereğince sonraki aktarımlar açısından da KVKK güvencelerinin sağlanması zorunludur. Bu çerçevede, veri sorumluları ve işleyenlerin kişisel verilerin akışını uçtan uca izlemeleri, ilgili ülkelerin veri koruma seviyelerini değerlendirmeleri, riskleri belirleyerek teknik, sözleşmesel ve organizasyonel güvenlik önlemleri almaları gerekmektedir[239]. GDPR ve KVKK düzenlemeleri doğrultusunda, uluslararası veri transfer zinciri boyunca kişisel verilerin korunmasını sağlamak, yalnızca ilk aktarımı gerçekleştiren tarafların değil, veriyi alan tarafların da sorumluluğundadır.

## 5. TÜRKİYE'NİN VEYA İLGİLİ KİŞİNİN MENFAATİNİN CİDDİ BİR ŞEKİLDE ZARAR GÖRECEĞİ DURUMLARDA VERİ AKTARIMI (m.9/9)

KVKK Reform Yasası kapsamında, eski 9. maddenin beşinci fıkrasında yer alan özel kısıtlama korunmuş ve veri aktarımına yönelik belirli şartlar sıkılaştırılmıştır[240]. Bu düzenlemeye göre, kişisel verilerin yurt dışına aktarımı, uluslararası sözleşme hükümleri saklı kalmak kaydıyla,

---

[235] Avrupa Veri Koruma Kurulu (EDPB), Guidelines 2/2018 on derogations of Article 49 under Regulation 2016/679, 25 Mayıs 2018.
[236] Avrupa Adalet Divanı (Court of Justice of the European Union- CJEU), Schrems II Kararı: Data Protection Commissioner v Facebook Ireland Ltd and Maximillian Schrems (C-311/18), 16 Temmuz 2020.
[237] European Data Protection Supervisor (EDPS), Transfer Impact Assessments (TIA) and Data Protection Impact Assessments (DPIA) Guidelines, 2021
[238] Avrupa Veri Koruma Kurulu (EDPB), Guidelines 2/2018 on derogations of Article 49 under Regulation 2016/679, 25 Mayıs 2018.
[239] Mehmet Bedi Kaya, "KVKK Reformu 2024 Değişiklikleri", Dijital Baskı v1.0- Mart 2024, s.37. *https://mbkaya.com/hukuk/kvkk-reformu.pdf,* (Erişim Tarihi:13.01.2025).
[240] Kaya, *"KVKK Reformu 2024 Değişiklikleri", op. cit.,* s.52.

Türkiye'nin veya ilgili kişinin menfaatlerinin ciddi şekilde zarar görebileceği durumlarda ancak belirli bir prosedür izlenerek gerçekleştirilebilir. Özellikle, bu tür aktarım işlemlerinde ilgili kamu kurum veya kuruluşunun görüşü alınmalı ve nihai karar Kişisel Verileri Koruma Kurulu tarafından verilmelidir. Bu düzenleme, kişisel verilerin yurt dışına çıkışını belirli durumlarda sınırlandırarak, ulusal güvenlik, ekonomik çıkarlar veya bireylerin temel hak ve özgürlüklerinin korunmasını amaçlamaktadır. Özellikle devlet güvenliği, kamu düzeni, ticari sırların korunması veya stratejik sektörlerde faaliyet gösteren kurum ve bireylerin menfaatlerinin korunması açısından bu hüküm kritik bir öneme sahiptir. Bununla birlikte, GDPR ile kıyaslandığında, KVKK'nın bu düzenlemesi daha katı bir ulusal güvenlik yaklaşımı benimsemektedir. GDPR'ın 49. maddesinde, uluslararası veri transferlerinde "zorunlu kamu yararı" ve "istisnai durumlar" kapsamında belirli esneklikler tanınırken, KVKK'da yurt dışına aktarımın belirli bir prosedüre tabi tutulması ve kamu otoritelerinin değerlendirmesine bırakılması, Türkiye'nin veri koruma rejiminde daha kontrollü bir yaklaşım sergilendiğini göstermektedir. Bu bağlamda, veri sorumluları ve veri işleyenler, Türkiye'nin veya ilgili kişilerin menfaatlerinin zarar görme ihtimalini içeren veri aktarımlarında mutlaka ilgili kamu otoritesine danışmalı ve Kurul'un iznini almalıdır. Bu süreçte, KVK Kurulu'nun hangi kriterlere göre değerlendirme yapacağı ve kamu kurumlarının görüş bildirme sürecinin ne şekilde işleyeceği hususları, uygulamada netleştirilmesi gereken konular arasında yer almaktadır.

### 6. DİĞER KANUN HÜKÜMLERİ (m.9/10)

İlgili hüküm, KVKK'nın diğer özel kanunlarla çelişmesini önleyerek, farklı sektörlerde yürürlükte bulunan özel veri aktarım düzenlemelerinin uygulanmasına imkân tanımaktadır. Böylece, belirli alanlarda faaliyet gösteren kurum ve kuruluşlar, KVKK hükümlerine ek olarak kendi sektörlerine özgü yasal düzenlemelere de tabi olmaya devam edeceklerdir.

Özellikle finans, havacılık ve elektronik haberleşme gibi düzenlemeye tabi sektörlerde, kişisel verilerin yurt dışına aktarımına yönelik özel hükümler bulunmaktadır. Örneğin, 2920 sayılı Türk Sivil Havacılık Kanunu'nun 40. maddesi kapsamında, yolcu bilgilerinin havayolu işletmeleri veya kurumlar tarafından üçüncü ülkelere aktarımı İçişleri Bakanlığı'nın uygun görüşüne tabi tutulmuştur. İçişleri Bakanlığı, bu aktarım taleplerini değerlendirirken ilgili kurumlarla koordinasyon sağlamakta ve mütekabiliyet esasına göre karar vermektedir. Bu düzenleme, yolcu bilgilerinin yurt dışına aktarımı konusunda KVKK ile paralel bir koruma mekanizması oluşturmuştur. Benzer şekilde, 5411 sayılı Bankacılık Kanunu'nun 73. maddesinde, KVKK uyarınca müşterinin açık rızası alınsa dahi, müşteri tarafından açık bir

talimat verilmedikçe finansal bilgilerin yurt içindeki veya yurt dışındaki üçüncü kişilerle paylaşılamayacağı hükme bağlanmıştır. Bu düzenleme, kişisel verilerin korunmasını güçlendiren ek bir güvence sunmaktadır. Ayrıca, 5809 sayılı Elektronik Haberleşme Kanunu'nun 51. maddesi de kişisel verilerin yurt dışına aktarımı konusunda özel bir çerçeve getirmektedir. Bu maddeye göre, trafik ve konum verileri, yalnızca ilgili kişilerin açık rızaları alınarak yurt dışına aktarılabilir ve ilgili mevzuatta yer alan hükümler saklı kalmaktadır[241].

KVKK 9/10 hükmü, farklı sektörlerde yürürlükte olan özel düzenlemelerin uygulanmasına olanak tanırken, kişisel veri aktarım süreçlerinde sektör bazlı ek güvenceler sağlamaktadır. Bu doğrultuda, veri sorumlularının, KVKK'nın genel hükümleriyle birlikte, faaliyet gösterdikleri sektöre özgü mevzuatı da dikkate alarak yurt dışına veri aktarım süreçlerini yönetmeleri gerekmektedir. Özellikle düzenleyici otoriteler tarafından belirlenen sektörel veri koruma yükümlülüklerine uyum sağlanması, kişisel veri güvenliği açısından kritik bir unsur olarak değerlendirilmektedir.

## 7. KİŞİSEL VERİLERİN YURTDIŞINA AKTARILMASINA İLİŞKİN İKİNCİL MEVZUAT (m.9/11)

KVKK Reform Yasası ile 9. maddenin on birinci fıkrasına yapılan ekleme ile Kişisel Verileri Koruma Kurulu'na kişisel verilerin yurt dışına aktarımına ilişkin usul ve esasları belirleme yetkisi verilmiştir. Bu yetki, veri sorumluları ve veri işleyenler için yurt dışına veri aktarımı süreçlerinin daha belirgin hale getirilmesini sağlayacak ve uygulamada karşılaşılan belirsizliklerin giderilmesine katkı sunacaktır. KVK Kurulu, bu yetki çerçevesinde çıkaracağı yönetmelikler, rehberler ve ikincil düzenlemeler aracılığıyla, kişisel verilerin yurt dışına aktarım süreçlerinde uyulması gereken prosedürleri ayrıntılı olarak belirleyebilecektir. Bu düzenlemeler, özellikle yeterlilik kararları, bağlayıcı şirket kuralları (BCR), standart sözleşme maddeleri (SCC) ve uluslararası kuruluşlarla veri paylaşımı gibi konularda açıklık sağlayacaktır. Ayrıca, veri aktarımında uygun güvencelerin nasıl sağlanacağı, alınması gereken teknik ve organizasyonel tedbirler ile veri aktarımı etki analizleri (TIA) gibi konulara ilişkin detaylar da KVK Kurulu tarafından oluşturulacak rehberlerde netleştirilecektir. Bu yetkilendirme, özellikle GDPR ile uyumlu bir düzenleyici çerçeve oluşturulmasını mümkün kılacaktır. Avrupa Veri Koruma Kurulu tarafından yayımlanan uluslararası veri aktarımına ilişkin rehberler gibi, KVK Kurulu'nun da benzer detaylı rehberler ve kriterler belirleyerek,

[241] *Ibid.,* s.52-53.

Türkiye'den yurt dışına veri aktarımı süreçlerini düzenlemesi beklenmektedir. Özellikle Schrems II kararının ardından, uluslararası veri transferlerinde güvence mekanizmalarının detaylı incelenmesi gerekliliği artmış olup, KVK Kurulu'nun bu çerçevede çıkaracağı düzenlemeler hem özel sektör hem de kamu kurumları açısından yol gösterici olacaktır. Böylece, veri sorumluları ve veri işleyenler, sadece genel hukuki dayanakları değil, aynı zamanda KVK Kurulu tarafından belirlenen somut kriterleri ve uygulama esaslarını takip ederek yurt dışına veri aktarım süreçlerini hukuka uygun bir şekilde yönetebileceklerdir.

Sonuç olarak, 9. maddenin on birinci fıkrasıyla getirilen bu yetki, kişisel verilerin yurt dışına aktarımı konusunda daha öngörülebilir ve uygulanabilir bir yapı oluşturmayı amaçlamakta olup, KVK Kurulu'nun yapacağı düzenlemelerle kişisel veri güvenliğinin artırılması hedeflenmektedir.

# ÜÇÜNCÜ BÖLÜM

# 6698 SAYILI KANUN KAPSAMINDA ANONİM ŞİRKETLERİN YURT DIŞINA KİŞİSEL VERİ AKTARIMLARINDA STANDART SÖZLEŞME HÜKÜMLERİNİN HUKUKİ DAYANAĞI VE UYGULAMADAKİ YANSIMALARI

Türkiye'de kişisel verilerin korunmasına yönelik en temel düzenleme olan 6698 sayılı Kişisel Verilerin Korunması Kanunu, kişisel verilerin yurt dışına aktarımını belirli şartlara bağlamış ve bu çerçevede veri güvenliğini sağlamak amacıyla çeşitli mekanizmalar öngörmüştür. Bu mekanizmalardan biri de standart sözleşmelerdir. Standart sözleşmeler, anonim şirketler başta olmak üzere veri sorumlularının, kişisel verileri yurt dışına aktarırken uyacakları kuralları belirlemekte ve bu sürecin hukuka uygunluğunu sağlamaktadır. Bu bölümde, 6698 sayılı Kanun çerçevesinde kişisel verilerin yurt dışına aktarımı sürecinde standart sözleşmelerin rolü ele alınacaktır. Öncelikle anonim şirketlerin veri sorumlusu olarak hukuki konumu, ardından KVKK kapsamında anonim şirketlerin yurt dışına veri aktarımı için izlemeleri gereken hukuki süreçler ve yurt dışına veri aktarımı süreçleri ve bu süreçlerde standart sözleşmelerin taşıdığı rol detaylı şekilde ele alınacaktır.

## I. ANONİM ŞİRKETLERİN VERİ SORUMLUSU OLARAK HUKUKİ KONUMU

### A. GENEL OLARAK

6698 sayılı Kişisel Verilerin Korunması Kanunu, anonim şirketler gibi tüzel kişileri veri sorumlusu sıfatıyla belirli yükümlülükler altına sokmaktadır. KVKK'nın 3. maddesi uyarınca, veri sorumlusu; "işlediği kişisel verilerin işleme amaçlarını ve yöntemlerini belirleyen gerçek veya tüzel kişidir". Anonim şirketler, yürüttükleri ticari faaliyetler kapsamında çalışanlarına, müşterilerine ve iş ortaklarına ait çeşitli kişisel verileri işlerken veri sorumlusu sıfatına haiz olmakta ve bu sıfatla çeşitli hukuki yükümlülüklere tabi olmaktadır.

Çalışmamızın bu bölümünde, öncelikle anonim şirketlerin Türk hukukundaki hukuki konumu, anonim şirketlerin temsili ve yönetimi kısaca ele alınacak, ardından KVKK kapsamında veri sorumlusu olarak sahip oldukları sorumluluklar incelenecektir. Devamında ise, anonim şirketlerin faaliyet alanları çerçevesinde işledikleri kişisel veri kategorilerine değinilecektir.

## 1. ANONİM ŞİRKETLERDE YÖNETİM ve TEMSİL

Anonim şirketler, 6102 sayılı Türk Ticaret Kanunu'nun 329. maddesi uyarınca, *sermayesi belirli ve paylara bölünmüş, ortakların sadece taahhüt ettikleri sermaye paylarıyla sorumlu oldukları bir sermaye şirketi* olarak tanımlanmaktadır. Bir sermaye şirketi türü olan anonim şirkette, şahıs şirketlerinden farklı olarak, yönetim ve temsil fonksiyonları, şirketin tüzel kişiliğini oluşturan ve kanunen düzenlenen organlar eliyle yürütülmektedir[242]. Tüzel kişiliğe sahip olan anonim şirketler gerek ulusal gerekse uluslararası ticarette yaygın olarak kullanılan bir şirket türüdür. Anonim şirketler, tüzel kişilik kazanabilmek için ticaret siciline tescil edilmek zorundadır. Şirketin kuruluş sürecinde, eğer mevzuat gereği belirli bir izin alınması gerekiyorsa, ilgili resmi mercilerden onay alındıktan sonra tescil işlemi yapılmalıdır. Bunun dışında kalan anonim şirketlerde ise, esas sözleşmenin noter onayı ya da ticaret sicili müdürlüğü huzurunda imzalanmasını takip eden otuz gün içinde, şirketin merkezinin bulunduğu yerin ticaret siciline kaydedilmesi gerekir (TTK 335/1)[243]. Tescil işleminin ardından, hukuki şeffaflığın sağlanması amacıyla şirketin kuruluşu Ticaret Sicil Gazetesi'nde duyurulur. Tüzel kişiliğin kazanılmasıyla birlikte anonim şirket, hukuki hak ve yükümlülüklere sahip bağımsız bir varlık hâline gelir ve TTK çerçevesinde faaliyetlerini sürdürür. Türk Medeni Kanunu'nun 49. maddesi uyarınca, tüzel kişilerin fiil ehliyetine sahip olabilmeleri için kanuna ve kuruluş belgelerine uygun şekilde zorunlu organlarını oluşturmaları gerekir[244]. Bu organlar kurulmadığı sürece, tüzel kişi sadece hak ehliyetine sahip sayılır; fiil ehliyeti kazanılamaz. TMK m. 50/1'e göre, tüzel kişi ancak organları aracılığıyla irade açıklayabilir[245]. Organlar, tüzel kişiliğin parçası olup, kendi adlarına değil tüzel kişi adına işlem yapar. Bu işlemler ve görev sırasında işlenen haksız fiiller, doğrudan

---

[242] Ünal Tekinalp, Reha Poroy, Ersin Çamoğlu, *Ortaklıklar Hukuku*, 14. Baskı, Vedat Kitapçılık, İstanbul, 2019, s.358; Rıza Ayhan, Hayrettin Çağlar, Mehmet Özdamar, *Şirketler Hukuku Genel Esaslar*, 4.baskı, Ankara: Yetkin Yayınevi, 2022, s. 136; Aytekin Çelik, *Ticaret Hukuku*, 13. baskı, Ankara: Seçkin Yayıncılık, 2023, s. 113; Hakan Çebi, *Şirketler Hukuku*, 1. baskı, Ankara: Seçkin Yayıncılık, 2020, s. 42.

[243] İsmail Kırca, Feyzan Hayal Şehirali Çelik, Çağlar Manavgat, *"Anonim Şirketler Hukuku",* Cilt 1, Temel Kavramlar ve İlkeler, Kuruluş, Yönetim Kurulu, Ankara, Banka ve Ticaret Hukuku Araştırma Enstitüsü, 2013, s. 289; Soner Altaş, *"Uygulamalı Anonim Şirketler Hukuku",* Ankara, Seçkin Hukuk, 2021, s.44.

[244] M. Kemal Oğuzman; Özer Seliçi ve Saibe Oktay, Kişiler Hukuku (Gerçek ve Tüzel Kişiler), İstanbul, Filiz Kitabevi, 2002, s.187, Tamer Bozkurt, "*Şirketler Hukuku"*, Legem Yayıncılık, 2018, s.237, Zikrullah Özbağ, "*Anonim Şirket Yönetim Kurulu Üyelerinin Cezai Sorumlulukla Bağlantılı Hukuki Sorumluluğu",* Ankara, Adalet Yayınevi, 2024, s.61.

[245] Hasan Pulaşlı, "*Şirketler Hukuku Genel Esaslar",* Adalet Yayınevi, 4. Baskı, 2016, s.351.

tüzel kişiyi bağlar (TMK. m.50/2, TTK m. 371/5). Bu nedenle organlar, Borçlar Kanunu anlamında yardımcı kişi, müstahdem ya da klasik temsilci sayılmaz; yetkileri kişilik hukukuna özgü olup doğrudan kanuna dayanır[246]. Anonim şirketlerde organ kavramı, özellikle sorumluluk hukukuna ilişkin meselelerde belirleyici bir rol oynamaktadır. Şirketin gerçekleştirdiği hukuki işlemler ya da organlar aracılığıyla ortaya çıkan haksız fiiller açısından kimin organ sayılacağı, hangi yetkilerin devredilebileceği ve bu kişilerin hangi sorumluluk hükümlerine tabi olacağı, ancak organın neyi ifade ettiğinin açıklığa kavuşturulmasıyla doğru biçimde değerlendirilebilir[247]. Bu bağlamda TTK sistemine göre anonim şirketlerde genel kurul ve yönetim kurulu olmak üzere mutlak anlamda zorunlu iki organ bulunmaktadır[248]. 6762 sayılı mülga TTK döneminde denetçiler, anonim şirketlerin zorunlu organı olarak kabul edilmekteydi. Ancak 6102 sayılı TTK ile birlikte denetim kurumu köklü şekilde yeniden yapılandırıldı. Yeni sistemde denetim, bağımsız dış denetim esasına bağlandı (TTK m. 397 vd.) ve organ olma niteliği büyük ölçüde kaldırıldı. Öğretide ağırlıklı görüş denetçilerin artık organ olmadığı yönündeyken[249] bir diğer zıt görüş denetçilerin "organ benzeri" bir konumu[250] olduğu yönündedir. Bu organlar, şirketin tüzel kişiliğinin devamı için gerekli olup, yoklukları halinde TTK m.530 uyarınca şirketin feshine yönelik dava açılması mümkündür. Anonim şirketler hukuku açısından organ kavramı, yalnızca yasal veya sözleşmesel düzenlemelerle yetkilendirilmiş kişileri değil, şirket adına karar verme, yürütme, denetim, gözetim ve temsil faaliyetlerinde bulunan tüm yapıları kapsayacak şekilde geniş yorumlanmaktadır[251]. Bu kapsamda, kanun, esas sözleşme veya iç düzenlemelerde açıkça belirtilmeyen ya da şirket

[246] Hasan Pulaşlı, "Anonim Ortaklık Yönetim Kurulunda Yönetim Kurulu Üyeliğinin Temsili", *Prof. Dr. Fahiman Tekil'in Anısına Armağan*, İstanbul, MÜ Hukuk Fakültesi Yayınları, 2003, s.173; M. Kemal Oğuzman ve Turgut Öz, *Borçlar Hukuku Genel Hükümler*, İstanbul: Filiz Kitabevi, 2000, s.162.

[247] Nihan Palta, Türk ve İsviçre Anonim Şirketler Hukukunda Organ Kavramı, *Akdeniz Üniversitesi Hukuk Fakültesi Dergisi,* Haziran 2022, cilt 12, Sayı:1, s.357-391.

[248] Mehmet Bahtiyar, "Ortaklıklar Hukuku" Ankara, Beta Yayıncılık, 15. Bası, 2021, s.144.

[249] Öğretide baskın görüş, TTK m. 397 ve devamı ile getirilen yeni düzenleme uyarınca, denetçilerin artık anonim şirketin bir organı olmadığını ifade etmektedir. Zira denetim, içsel bir fonksiyon olmaktan çıkarılmış, dışarıdan hizmet temini esasına bağlanmıştır. Bu doğrultuda bknz. Ünal Tekinalp, Tek Kişi Ortaklık, s.106; Çamoğlu, Poroy ve Tekinalp, *op. cit.* s. 538; Hasan Pulaşlı, Şirketler Hukuku Şerhi, Cilt I, Ankara: Adalet Yayınevi, 2018, s. 806; Mehmet Bahtiyar, Ortaklıklar Hukuku, İstanbul, Beta Yayıncılık, 2020, s.149-264; Şükrü Yıldız, Türk Ticaret Kanunu Tasarısına Göre Limited Şirketler Hukuku, İstanbul, Arıkan Yayınevi, 2007, s.200; Bilgili ve Demirkapı, Şirketler Hukuku, 9. bs., Bursa, Dora Yayıncılık, Ocak 2013, s.211; Suat Yıldırım, "Türk Ticaret Kanunu'na Göre Anonim Şirketlerde Denetçi", Mali Çözüm Dergisi, Cilt 21, S. 106, 2011, s. 44-45. Köksal, Aytaç: Bağımsız Denetim Sözleşmesi, 1. Bası, Beta, İstanbul 2009; Aytaç: Türk Ticaret Kanunu Tasarısının 397 ila 406. Maddeleri Arasında düzenlenen Denetçinin Anonim Ortaklığın Organı Olup Olmadığı Sorunu, Prof. Dr. Fırat Öztan'a Armağan Cilt 1.

[250] Öğretide denetçinin organ benzeri bir konumu olduğunu ifade eden yazarlar için bknz. İbrahim Kaplan, "Bağımsız Denetim Kuruluşu Yönetim Kurulu ve Denetçileri ile Bağımsız Denetim Kuruluşunun Hukuki Sorumluluğu", *Batider*, C. XXVIII, Sayı 2, 1961, s.18.

[251] Doğan, Beşir Fatih. *6102 Sayılı Türk Ticaret Kanunu'na Göre Anonim Şirket Yönetim Kurulunun Organizasyonu ve Yönetim Yetkisinin Devri*. İstanbul, Vedat Kitapçılık, 2011, s.6.

içinde resmî bir atamaya tabi tutulmamış olsalar bile, tüzel kişinin iradesinin oluşumuna katkı sağlayan veya fiilen yönetim ve temsil işlevlerinde rol üstlenen kişiler de organ statüsünde değerlendirilebilmektedir[252]. Farklı hukuk sistemleri, anonim şirketlerde organlar arasındaki ilişkiye yönelik çeşitli teoriler geliştirmiştir[253]. Mehaz İsviçre Borçlar Kanunu m. 698 genel kurulu "en üst organ" olarak tanımlasa da bu ifade farklı şekillerde yorumlanmıştır. Hakimiyet teorisi, genel kurula sınırsız karar yetkisi tanırken, sınırlandırılmış üstünlük teorisi yalnızca istisnai durumlarda müdahaleye izin verir. Almanya'da uygulama alanı bulan Führerprinzip ise yönetim kurulunun üstünlüğünü savunur[254]. İsviçre'de en çok kabul gören eşitlik (işlevler ayrılığı) teorisi, organlar arasında hiyerarşi bulunmadığını, her birinin kendi yetki alanında bağımsız olduğunu kabul eder. Bu anlayış, kuvvetler ayrılığı ilkesine dayanmaktadır[255]. TTK'da bu ilişkinin niteliğine dair açık bir hüküm bulunmamakla birlikte, TTK m. 374, 375 ve 408'deki düzenlemeler ve gerekçeleri dikkate alındığında, genel kurulun üst organ olmadığı[256], organlar arasındaki ilişkide görev ve yetkilerin ayrımına dayanan bir işlevsel denge gözetildiği ve bu çerçevede TTK'nın işlevsel eşitlik ilkesine dayalı bir sistemi benimsediği, öğretide hâkim görüştür[257]. Bu kapsamda *"Genel kurul, karar verme yetkisini kanundan ve kanun hükümleri çerçevesinde esas sözleşmeden alır"*[258]. Genel kurul pay sahiplerinin katılımıyla oluşan iç organdır ve yürütmeye ilişkin fonksiyonu bulunmaz[259]. TTK m. 408 gereğince şirketin temel stratejik kararları, genel kurulda alınır ve yönetim kurulunun seçimi ve azli, finansal tabloların onaylanması, kar payı dağıtım kararları alınması gibi yetkileri vardır[260]. Ancak bahsettiğimiz gibi genel kurulun yönetim kurulunu seçmesi ve görevden alması, ona üstünlük tanımaz; yalnızca bir seçim ve azil organı olduğunu gösterir. Yönetim kurulu ise TTK m. 365-375 uyarınca şirketin yönetim ve temsil organı olup, hem iç yönetim fonksiyonlarını yerine getirir

[252] Nihan Palta, *op. cit*., s.363, ATF 107 II 349, s. 354, p. 5a; ATF 121 III 176, s. 179, p. 5.
[253] Organlar arasındaki yetki dağılımına ilişkin öğretide üç temel yaklaşım öne çıkmaktadır. Sözleşme teorisi, şirketin pay sahiplerinin iradesiyle kurulduğunu ve organlara yetkinin vekâlet ilişkisiyle devredildiğini savunur. Buna karşılık kurum teorisi, organları şirket yapısı içinde bağımsız ve kalıcı unsurlar olarak değerlendirir. Karma teori ise her iki görüşü birleştirerek, anonim şirketin iç işleyişinde organların belirli yetkiler çerçevesinde ve eşit statüyle faaliyet gösterdiğini kabul eder. İsviçre ve Türk hukukunda benimsenen bu yaklaşım, organların hukuken değil, işlevsel olarak ayrıldığı bir sistem öngörür. Tekinalp, Poroy ve Çamoğlu, *op. cit.,* s.358, Pulaşlı, *Şirketler*, *op. cit.,* s. 319-320.
[254] Pulaşlı, *Şirketler*, *op. cit.,* s. 805; Doğan, *op. cit.,* s.18, Tekinalp, Poroy ve Çamoğlu, *op. cit.,* s.359.
[255] Altaş, *op. cit.* s.49; Palta, *op.cit.,* s.367.
[256] Hasan Pulaşlı, *Şirketler Hukuku Şerhi*, *Cilt II*, Ankara, Adalet Yayınevi, 2018, s. 1285; Çamoğlu, Poroy ve Tekinalp, *op. cit.*, s. 529; Kırca, Şehirali Çelik ve Manavgat, *op. cit.*, s.536; Tamer Bozkurt, "Şirketler Hukuku", Ankara, Legem Yayıncılık, Şubat 2018, s.238.
[257] İsmail Kırca, Feyzan Hayal Şehirali Çelik, Çağlar Manavgat, *op. cit.,* s.395; Pulaşlı, *op. cit.*s.805; Necla Akdağ Güney, "*Anonim Şirket Yönetim Kurulu"*, 2. Baskı, İstanbul, Vedat Kitapçılık, 2016, s.6.
[258] TTK 408. Maddenin 1. Fıkrasının gerekçesi.
[259] Hakan Çebi, "*Şirketler Hukuku",* Ankara, Seçkin Hukuk, 2020, s.131.
[260] Şaban Kayıhan, "*Şirketler Hukuku",* Ankara, Seçkin Hukuk, 2024, s.191.

hem de şirketi üçüncü kişilere karşı temsil etmekle görevlidir[261]. TTK m. 375 uyarınca yönetim kurulu, şirketin üst düzeyde yönetimi, organizasyon yapısının belirlenmesi, finansal ve stratejik planlamanın oluşturulması gibi hayati öneme sahip görev ve yetkileri doğrudan kendisi kullanmak zorundadır. Bu kapsamda, kanunda açıkça sayılan görevler devredilemez ve bu görevlerin ifası bakımından nihai sorumluluk yönetim kuruluna aittir[262]. Yönetime ilişkin kararları alır ve bunları uygular. Yönetsel sorumlulukları dolayısıyla, görevlerini yerine getirirken ihtiyatlı bir yöneticinin özeniyle hareket etmek zorundadır. Genel kurul şirketin irade organı iken, yönetim kurulu icrai kararları uygulayan yürütme organıdır. Esas sözleşme ile zorunlu organlara ek olarak ihtiyari organlar oluşturulabilir. Ancak bu organlara, yönetim kurulu ve genel kurula ait devredilemez yetkiler tanınamaz. İhtiyari organlar genellikle danışma veya yönetimin denetimi ile sınırlı işlevler üstlenebilir[263]. Örneğin, etik kurulları, danışma kurulları veya denetim komiteleri ihtiyari organlar olarak yapılandırılabilir. Yukarıda açıkladığımız üzere TTK sisteminde denetçi, bir şirket organı değildir. Bağımsız denetim belirli şartlar altında zorunlu olmakla birlikte, denetçi şirketin kurumsal yapısının bir parçası değil, hizmet birimi olarak faaliyet gösterir. Şirket ile denetçi arasındaki ilişki, TTK m. 397 ve devamı uyarınca bir sözleşmeye dayanarak yürütülür[264]. Buna karşılık, şirketin duruma bağlı olarak zorunlu şekilde ortaya çıkan tasfiye memurları, kayyımlar ve iflas idaresi; geçici ve özel yetki-sorumluluk taşıyan yapılar olup, öğretide genel olarak organ niteliği taşıdıkları kabul edilmektedir[265]. Bu yapılar, şirketin olağan işleyişinde yer almayıp, ancak sona erme, yönetim boşluğu veya iflas gibi olağanüstü hallerde devreye girerler. Tasfiye memurları özelinde ise, TTK m. 532 ve devamı uyarınca şirketin sona ermesiyle birlikte görevlendirilirler ve bu görevleri tasfiye süreciyle sınırlı olup, ihtiyari bir organ değil, duruma özgü zorunlu bir yapılanmadır. TTK m. 536 uyarınca tasfiye sürecinde tasfiye memurları, yönetim kurulunun yerini almakta ve şirketin tüzel kişiliğinin sona erdirilmesine yönelik işlemleri gerçekleştirmektedir[266]. Türk Ticaret Kanunu'nda yönetim kurulunun çeşitli komite ve komisyonlar kurabileceğine ilişkin düzenlemeler, özellikle üç maddede yer bulmuştur[267]. Bunlardan madde 366/2 ve madde 378, belirli komitelerin oluşturulmasını doğrudan öngörmektedir. Madde 378 kapsamında, anonim şirketlerde risklerin önceden belirlenmesi ve yönetilmesi amacıyla bir komitenin kurulması zorunlu tutulmuştur. Öte yandan, madde 375/c

[261] Tamer Bozkurt, *op.cit.* s.240.
[262] *Ibid*. s.209.
[263] Çebi, *op. cit,* s.131.
[264] Aytekin Çelik, *"Ticaret Hukuku"*, Ankara, Seçkin Hukuk, 2023, s.245.
[265] Palta, *op. cit.,* s.365.
[266] Altaş, *op. cit.* s.51, Tekinalp, 2013, s.184.
[267] Pulaşlı, *"Şirketler Hukuku Genel Esaslar",* Ankara, Adalet Yayınevi, 6. Baskı, 2020, s.400.

ise, şirketin mali yapısının içsel denetimini sağlamak amacıyla bir denetim komitesine işaret eder. Bu komitenin, özellikle muhasebe sisteminden bağımsız şekilde çalışan uzman kişilerden oluşması gerektiği belirtilmektedir[268]. TTK m. 366/2 hükmüne göre yönetim kurulu, karar alma sürecinde kendisine sunulacak konulara dair ön analiz yapılması, rapor hazırlanması veya kararların uygulanmasının izlenmesi gibi amaçlarla, kendi içinden ya da dışarıdan katılımlarla komite veya komisyonlar oluşturabilir. Bu tür yapılar, yönetim yetkisinin devri anlamına gelmeyip, organ içinde daha etkili çalışmayı sağlamak için yapılan bir görev paylaşımıdır[269]. Ayrıca, TTK m. 367 doğrultusunda, yönetim kurulu şirketin idaresini yazılı bir iç yönerge aracılığıyla, üyelerinden bazılarına veya dışarıdan atanacak kişilere kısmen ya da tamamen devredebilir. Ancak bu devredilebilir yönetim yetkisi ile komiteler aracılığıyla yapılan iş bölümü farklıdır. Komiteler, şirketin günlük faaliyetlerine yön vermekten ziyade, örneğin yeni bir şube açılması konusunda analiz yapmak, potansiyel birleşmelerle ilgili ön araştırmalar yürütmek veya bölünme senaryolarına dair alternatif yapılar geliştirmek gibi karar öncesi hazırlık ve danışmanlık görevleri üstlenirler[270]. Sonuç olarak, bu komite ve komisyonlar, doğrudan icrai nitelikte yetkilerle donatılmamış olup, yönetim kurulunun daha bilinçli kararlar almasına katkı sunan, yardımcı nitelikli iç organizasyon birimleri olarak değerlendirilmelidir.

TTK m. 375, yönetim kurulunun devredilemeyecek yetkilerini saymaktadır. Ancak bu hükümdeki sayımın niteliği doktrinde tartışma konusudur[271]. Bir görüşe göre, burada belirtilen yetkiler *sınırlı (tahdidi)* olarak sayılmıştır ve bunların esas sözleşme veya genel kurul kararıyla devri ya da devralınması mümkün değildir. Bu yönüyle düzenleme sınırlayıcı bir nitelik taşır[272]. Ancak, aynı zamanda söz konusu madde, esas sözleşme veya genel kurul kararı ile yeni devredilemez yetkiler belirlenmesini de engellemez. Bu durum, hükmün sadece sayılan yetkilerle sınırlı kalmadığını ve başka devredilemez yetkilerin tanımlanabileceğini göstermektedir. Dolayısıyla devredilemez yetkiler listesi, sabit ve tamamen sınırlı bir yapı arz etmemektedir. Bu bağlamda doktrindeki baskın görüş bu hükmün sınırlayıcı olmadığı yönündedir[273]. Diğer bir ifadeyle, 375. maddede yer almayan fakat fiilen yönetim kuruluna

---

[268] *Ibid.,* s.400.
[269] Kırca, Şehirali Çelik, Manavgat, *op. cit.,* s.478.
[270] Pulaşlı, *"Şirketler Hukuku Genel Esaslar", op. cit.,* s. 401.
[271] Beşir Fatih Doğan, "Yönetim Kurulunun Devredilemez Yetkileri ve Yönetim Yetkisinin Devri", *Dergipark,* Cilt:18, Sayı:2, 2012, s.611; "Umbach, İBK'nın 717-a/I'de sayılan yetkilerin sınırlı bir şekilde sayılmadığı görüşündedir. (Umbach, s. 30)".
[272] Beşir Fatih Doğan, "Yönetim Kurulunun Devredilemez Yetkileri ve Yönetim Yetkisinin Devri, *op. cit.,* s. 611-612; "Bknz. Horber, s. 76; Jud, Guido: Die Überwachung der Unternehmung durch deren Organe, Zürich 1990, s.316. Bu görüş sahipleri, devredilemez ve devralınamaz yetkilere yenilerinin de eklenemeyeceğini, düzenlemenin bu anlamda da sınırlayıcı olduğunu ifade etmektedirler."
[273] Kırca, Şehirali Çelik, Manavgat, *op. cit.,* s. 539-540; Doğan, 2011, s. 173-174, 210.

özgülenmiş bazı münhasır yetkiler de bulunmaktadır. Yönetim kurulunun, TTK m. 375 dışında kalan bazı görev ve yetkileri de kimi zaman doğrudan kanuni düzenlemeler, kimi zaman ise görevlerin mahiyeti gereği devredilmesi mümkün olmayan ve vazgeçilemez nitelikte kabul edilmektedir[274]. Bu durum, TTK m. 367 çerçevesinde yönetim yetkisinin devrine ilişkin bir iç yönerge hazırlanırken hangi görevlerin devre konu olabileceği ya da olamayacağının belirlenmesi açısından büyük önem taşır. Zira, görev veya yetkinin işin doğası gereği yönetim kuruluna ait olduğu hallerde, bu yetkinin açıkça kanunen devredilebilir kılınmadığı sürece başkasına aktarılması mümkün olmayacaktır. Kanun koyucunun tüm bu yetkileri önceden öngörerek tek tek sıralaması mümkün olmadığı için, uygulamada yönetim kurulunun sorumluluğu ve görev alanlarının kapsamı bu maddede yer almayan yetkilerle de genişleyebilir[275]. Bu çerçevede, söz konusu yetkilerin kapsamlı bir şekilde belirlenmesi, hem yönetim kurulunun hukuki sorumluluğunun sınırlarının çizilmesi bakımından hem de şirket ortaklarının ve alacaklılarının hukuki güvencesi açısından önemlidir. Kanaatimizce, TTK m. 375'in saydığı yetkiler mutlak bir sınırlayıcı liste olarak görülmemeli, ancak bu liste asgari bir çerçeve olarak değerlendirilmelidir. Böylece hem uygulamada karşılaşılabilecek farklı durumlar gözetilmiş olur hem de yönetim kurulunun karar alma ve temsil süreçlerindeki sorumluluk sınırları daha açık biçimde belirlenebilir.

TTK m. 375 uyarınca yönetim kurulunun bazı yetkileri devredilemez nitelikte olsa da TTK m. 367 ve 370 hükümleri uyarınca yönetim ve temsil yetkisinin devri belirli şartlar altında mümkündür. Anonim şirketlerde yönetim kurulu, esas sözleşmede aksine bir hüküm bulunmadıkça ve kurul birden fazla üyeden oluşuyorsa, temsil yetkisini çift imza ile kullanır (TTK m.370). Temsil yetkisinin devri ise TTK m. 370/2 ve m. 367 hükümleri gereğince, esas sözleşmede bu yönde bir düzenleme bulunması ve yönetim kurulunca TTK m. 367 uyarınca bir iç yönerge hazırlanması şartına bağlıdır. Bu devir, yönetim yetkisinin devri sırasında, öncesinde veya farklı bir zamanda gerçekleştirilebilir. TTK m. 504/2 hükmü, *"vekaletin, vekilin üstlendiği işin gerektirdiği hukuki işlemleri yapma yetkisini kapsadığını"* belirttiğinden, temsil yetkisinin de yönetim yetkisinin devri kapsamında değerlendirilmesi gerektiği ifade edilmektedir. Bu yaklaşım, ticari hayatta güvenin korunması açısından da önemlidir[276]. Anonim şirketlerde yönetim yetkisinin uzman kişilere devredilmesi, şirket faaliyetlerinin daha hızlı, etkin ve

[274] Duygu Demirel, "Anonim Şirketlerde Yönetim Yetkisinin Devri", *Hacettepe Hukuk Fakültesi Dergisi,* Cilt:12, Sayı:1, 2017, s.222.
[275] Kırca, Şehirali Çelik, Manavgat, *op. cit.,* s. 540.
[276] Süleyman Kalender, *"Anonim Şirketlerde Yönetim ve Temsil Yetkisinin Devri Halinde Yönetim Kurulu Üyelerinin Hukuki Sorumluluğu",* Ankara, Adalet Yayınevi, 2024, s.78.

profesyonel bir şekilde yürütülmesine olanak tanımaktadır. Bu doğrultuda, yönetim kurulu belirli yetkilerini devrederek şirket bünyesinde müdürlük ve muharraslık gibi yapılar oluşturabilmekte ve dışarıdan profesyonel yöneticilere yetki tahsis edebilmektedir[277]. TTK 367. maddesi çerçevesinde, yönetim kurulu, iç yönerge düzenleyerek şirketin yönetimine ilişkin belirli görev ve yetkileri devretme imkanına sahip olduğundan ancak söz konusu yetki devrinin, yalnızca icrai nitelikteki işlemlerle sınırlı olup, devredilemez yetkiler bu kapsamın dışında tutulduğundan bahsetmiştik. Yetki devri, yönetim kurulu ile yöneticiler arasında açık bir iş bölümü oluşturarak, kurumsal yönetim anlayışının güçlenmesine ve yönetim süreçlerinin profesyonelleşmesine katkı sağlamaktadır. Bu bağlamda, yönetim kurulu, TTK m. 375 hükmü uyarınca doğrudan icrai faaliyetleri yürütmekten ziyade, gözetim işlevini yerine getirme sorumluluğunu üstlenmektedir. Ayrıca, yetkinin devredilmesi ile birlikte, bu yetkilerin kullanımına ilişkin sorumluluk da yöneticilere geçmekte olup, yönetim kurulu üyelerinin sorumluluğu, özellikle TTK m. 553/2 hükmü uyarınca, görevlerini yerine getirirken kanuna veya esas sözleşmeye aykırı fiilleriyle şirkete, pay sahiplerine veya alacaklılara zarar vermeleri hâlinde yani gerekli özen ve denetim yükümlülüğünün yerine getirilmemesi durumunda doğmaktadır[278]. Bu sorumluluğun doğabilmesi için, TTK m. 553/3 uyarınca üyelerin kusurlu davranışlarının bulunması ve bu davranışla zarar arasında uygun illiyet bağının kurulması gerekmektedir[279].

---

[277] *Ibid.,* s.78-79; Bozkurt, *op. cit.* s.262.

[278] Daha fazla bilgi için bknz. Oruç Hami Şener, *Teorik ve Uygulamalı Ortaklıklar Hukuku Ders Kitabı*, 4. Baskı, Ankara 2019, s. 419.

[279] Anonim şirketlerde yönetim kurulu üyeleri, kural olarak, esas sözleşmeyi veya kanun hükümlerini ihlal etmeleri nedeniyle doğabilecek zararlardan, TTK m. 557 uyarınca müteselsilen sorumludurlar. Bu sorumluluk, şirketin yurt dışına kişisel veri aktarımı gibi yüksek riskli faaliyetlerinde de geçerliliğini korumaktadır. Özellikle KVKK m.9 kapsamında yapılacak veri aktarımlarında, ilgili kişilerin açık rızasının alınması, yurt dışındaki veri alıcısının gerekli korumayı sağlayacağına ilişkin güvencelerin temin edilmesi ve KVK Kurulu'nun izninin alınması gibi hukuki yükümlülüklerin ihlali hâlinde, doğabilecek zararlardan yönetim kurulu üyeleri sorumlu tutulabilir. Her ne kadar yönetim kurulu, TTK m. 367 uyarınca bazı yönetim yetkilerini şirket içinden görevlendirdiği kişilere devredebilse de veri sorumluluğu, KVKK anlamında tüzel kişilik düzeyinde belirlenmiş bir sorumluluktur ve bu tüzel kişilik adına hareket eden yönetim kurulu üyelerini doğrudan etkilemektedir. Bu kapsamda, veri işleme faaliyetinin organizasyonu, izlenmesi veya koordinasyonu amacıyla şirket bünyesinde veri koruma görevlisi, iç denetim birimi ya da hukuk danışmanı gibi unvanlarla bazı kişilerin görevlendirilmesi mümkündür. Ancak bu kişiler, veri sorumlusu değil, veri sorumlusunun talimatları doğrultusunda hareket eden destek birimleri olarak görev yaparlar. TTK m. 553/2 hükmü uyarınca, kanun veya esas sözleşmeden doğan bir görevi açık kanuni yetkiye dayanarak devreden yönetim kurulu üyeleri, ilke olarak devrettikleri kişinin fiil ve kararlarından sorumlu olmaz. Ancak, **veri koruma görevlisi gibi destek pozisyonlarında çalışan kişiler, bizzat veri sorumlusu sıfatına sahip olmadıklarından**, yönetim kurulu bu kişilere yetki devrinde bulunmakla yalnızca görev dağılımı yapmış olur; veri sorumlusunun hukuki yükümlülükleri ve sorumluluğu ise ortadan kalkmaz. Kaldı ki, aynı hükmün ikinci cümlesi uyarınca, yetki devri yapılan kişilerin seçiminde gereken özenin gösterilmediği ispatlanırsa, tüm yönetim kurulu üyeleri sorumluluktan kurtulamaz. Bu durumda, örneğin şirketin yurt dışına kişisel veri aktarımında görevlendirdiği kişinin gerekli teknik ve idari tedbirleri almaması ve ihlal yaratması hâlinde, yönetim kurulu üyeleri, gerekli denetimi yapmadıkları veya ehil olmayan kişiyi görevlendirdikleri gerekçesiyle, KVKK'dan kaynaklanan zararlardan müteselsilen sorumlu tutulabilirler.

Yönetim kurulu üyeleri, TTK m. 369'da düzenlenen sadakat ve özen yükümlülüğü çerçevesinde hareket etmekle yükümlüdür. Bu yükümlülüğün gereği olarak, yalnızca kendi görev alanlarıyla sınırlı kalmayıp şirketin faaliyetlerinin genel gözetimini sağlamak ve ihmal edilebilecek hukuki veya mali riskleri önceden tespit etmekle de yükümlüdürler[280]. Temsil yetkisinin devrini düzenleyen TTK m. 370/2, en az bir yönetim kurulu üyesinin temsil yetkisini korumasını zorunlu kılarken, yönetim yetkilerinin devrinde böyle bir sınırlama bulunmamaktadır. TTK m. 371 ise temsil yetkisinin kullanımına ve sınırlandırılmasına ilişkin hükümler içermektedir. Temsil yetkisinin sınırlandırılması esas sözleşme veya iç yönergelerle mümkün olsa da TTK m. 371/3, temsil yetkisine getirilecek sınırlamaların, ancak belirli bir şube veya merkezin işleriyle ya da birlikte temsil şartıyla sınırlandırılabileceğini öngörmektedir. Bu nedenle yönetim kurulu üyeleri, şirketi temsilen yaptıkları işlemler nedeniyle hem şirkete hem de üçüncü kişilere karşı sorumluluk doğurabilecek fiillerden kaçınmakla yükümlüdür. Yönetim yetkilerinin devrinde ise böyle bir sınırlandırma getirilmediğinden, yönetim kurulu devrettiği yetkiler üzerinde çeşitli sınırlamalar koyabilir[281]. Bu genel çerçeve kapsamında, anonim şirketlerin yurt dışına kişisel veri aktarması durumunda yönetim kurulu üyelerinin özen yükümlülüğü çok daha hassas bir hâl almaktadır. KVKK m. 9 uyarınca yurt dışına veri aktarımı, yalnızca ilgili kişinin açık rızası veya Kurul'un belirlediği güvenli ülkeler listesi ve yeterli korumanın sağlandığı durumlarda mümkündür. Yönetim kurulu, bu aktarım süreçlerinde gerekli teknik ve idari tedbirlerin alınıp alınmadığını denetlemekle ve veri aktarımına ilişkin prosedürleri doğru şekilde yürütmekle yükümlüdür. Bu bağlamda öğretide de vurgulandığı üzere, şirket içi risklerin erken saptanması ve denetlenmesi için etkin iç denetim mekanizmalarının oluşturulmaması (örneğin TTK m. 378'de öngörülen Riskin Erken Saptanması Komitesi'nin kurulmaması), sorumluluğun doğmasına neden olabilecek unsurlar arasında yer almaktadır. Böyle bir durumda, yönetim kurulu üyeleri yalnızca yaptıkları eylemlerden değil, gerekli önleyici adımları atmama gibi ihmali davranışlardan da dolayı sorumlu tutulabilirler[282].

---

[280] Hayrettin Çağlar, Rıza Ayhan, Mehmet Özdamar, *"Şirketler Hukuku Genel Esaslar",* Ankara, Yetkin Hukuk Yayıncılık, 2019, s.322.

[281] TTK m.367/1 "Yönetim kurulu, düzenleyeceği bir iç yönerge ile, yönetimi kısmen veya tamamen bir veya birkaç yönetim kurulu üyesine veya üçüncü kişilere devredebilir. Ancak bu devrin geçerli olabilmesi için, devredilecek yetki ve görevlerin belirlenmiş olması gerekir." Bu maddede temsil yetkisiyle ilgili TTK m. 370'in aksine, devre konu yönetim yetkilerinin kapsamı ve sınırlarının şirketin kendi iradesiyle (iç yönergeyle) belirlenebileceği açıkça düzenlenmiştir. Yani, yönetim kurulu, iç yönerge aracılığıyla yetkiyi devrettiği kişilere görev sınırları çizebilir, belli alanlarda karar yetkisini kısıtlayabilir veya belirli konuların mutlaka kurul onayından geçmesi gerektiğini kararlaştırabilir.

[282] Örneğin: Bir anonim şirketin, grup şirketi olan yurt dışındaki bir firmaya müşteri verilerini aktarırken KVKK m. 9'a aykırı şekilde açık rıza almadan veya yeterli koruma sağlanmadan bu işlemi gerçekleştirdiği varsayılsın.

## 2. ANONİM ŞİRKETLERİN VERİ SORUMLUSU SIFATI

KVKK kapsamında, anonim şirketlerin veri sorumlusu sıfatı taşıması, işledikleri kişisel verilerin hukuka uygun şekilde işlenmesi, korunması ve aktarılması yükümlülüklerini doğurmaktadır. Bu başlık altında, anonim şirketlerin veri sorumlusu sıfatının kapsamı ve bu sıfatın doğurduğu hukuki sonuçlar ayrıntılı olarak incelenecektir.

Kişisel verilerin işlenme sürecinde iki temel aktör olan veri sorumlusu ve veri işleyen hem Kişisel Verileri Koruma Kanunu hem de Genel Veri Koruma Tüzüğü kapsamında ayrıntılı düzenlemelere tabi tutulmuştur. GDPR m.4/7'ye göre veri sorumlusu ("data controller"), kişisel verilerin hangi amaçlarla ve hangi yöntemlerle işleneceğine tek başına veya başkalarıyla birlikte karar veren gerçek ya da tüzel kişi, kamu otoritesi, kurum veya herhangi bir organı ifade etmektedir[283]. Benzer şekilde KVKK m.3/1'e göre veri sorumlusu, kişisel verilerin işlenme amaçlarını ve vasıtalarını belirleyen, veri kayıt sisteminin kurulmasından ve yönetilmesinden sorumlu olan gerçek veya tüzel kişidir[284]. GDPR ise veri sahibinin gerçek kişi olması gerektiğini, veri sorumlusu olarak ise hem gerçek hem de tüzel kişileri, kamu kurumlarını ve idarelerini kapsadığını belirtir. KVKK, GDPR gibi kamu kurumlarının da veri sorumlusu veya veri işleyen olabileceklerini açıkça ve ayrıca belirtmemiştir[285]. Anonim şirketler, faaliyetleri gereği çalışanlar, müşteriler, iş ortakları ve tedarikçiler gibi birçok kişinin kişisel verilerini işleyen tüzel kişiler olup, asli biçimde veri sorumlusu olarak nitelendirilir[286] ve kişisel veri işleme faaliyetlerini KVKK ve GDPR'ye uygun bir şekilde gerçekleştirme yükümü altındadır. Şirketin tüzel kişiliği gereği, veri sorumluluğu şirketin kendisinde doğar ve bu sorumluluk, şirketin işlediği tüm kişisel verilerin güvenliğini sağlama, verilerin hukuka uygun bir şekilde işlenmesini temin etme ve veri sahiplerinin haklarını koruma yükümlülüklerini içerir. Bu kapsamda, anonim şirketlerin veri sorumlusu olarak kabul edilmesi, veri işleme yöntemleri, veri kategorileri, veri işleme yetkisine sahip birimler ve çalışanlar, kişisel verilerin saklama süresi,

---

Bu durumda, eğer yönetim kurulu üyeleri bu aktarım sürecine dair gerekli kontrol ve denetimi gerçekleştirmemiş, uyum mekanizmalarını kurmamış ya da Kurul'dan gerekli izinlerin alınmasını sağlamamışlarsa; veri ihlali nedeniyle Kurul tarafından şirkete uygulanacak idari para cezasının yanı sıra, müşterilerin uğrayacağı zararlardan dolayı yönetim kurulu üyeleri şahsen sorumlu tutulabilecektir.

[283] Avrupa Parlamentosu ve Konsey'in (AB) 2016/679 sayılı ve 27 Nisan 2016 tarihli Genel Veri Koruma Tüzüğü (GDPR), m. 4/7.

[284] 6698 sayılı Kişisel Verilerin Korunması Kanunu, m. 3/1(ı)

[285] Elif Küzeci, *"Kişisel Verilerin Korunması",* On İki Levha Yayıncılık, İstanbul 2021, s.364-365.

[286] 698 sayılı KVKK'nın 3. maddesinde yer alan tanım uyarınca, kişisel verilerin işlenme amaç ve vasıtalarını belirleyen tüzel kişiler veri sorumlusu sıfatını haizdir. Bu kapsamda anonim şirketler, faaliyetleri gereği çalışanlar, müşteriler, iş ortakları gibi kişilere ait kişisel verileri işleyen organizasyonlar olarak asli veri sorumlusu konumundadır. Bu sıfat, KVKK m. 10 ve 12'de düzenlenen aydınlatma ve veri güvenliği yükümlülüklerinin doğrudan muhatabı olmalarını da beraberinde getirir.

imha veya anonimleştirme prosedürleri gibi konular üzerinde yetki sahibi olduklarını ortaya koymaktadır[287].

Anonim şirketlerin veri sorumlusu olarak kabul edilmesi açısından kritik nokta, veri sorumluluğunun şirket çalışanlarına değil, doğrudan şirketin kendisine ait olmasıdır. Yani veri sorumlusu sıfatı, yalnızca şirketin genel yönetimi için geçerli olup, şirket bünyesindeki birimler veri sorumlusu olamaz. Bu çerçevede veri sorumlusu sıfatı, yalnızca şirketin genel yönetimi için değil, şirket tüzel kişiliği adına geçerlidir; bu kapsamda, şirket bünyesindeki birimler veya yetki devri yapılan kişiler veri sorumlusu olamaz. Yönetim kurulu üyeleri, şirketin organları olarak veri sorumlusu sıfatını şahsen taşımazlar; veri sorumlusu, şirket tüzel kişiliğidir. Dolayısıyla, yetki devri kapsamında veri sorumlusu sıfatının yönetim kurulu üyelerine, ticari temsilcilere veya şirkete hizmet akdiyle bağlı sınırlı yetkili ticari vekillere yüklenmesi mümkün değildir[288]. İleride açıklanacağı üzere anonim şirketlerin yönetim organları, veri sorumluluğuna ilişkin yükümlülüklerin yerine getirilmesi amacıyla belirli birimleri ve çalışanları görevlendirebilir[289]. Ancak bu görevlendirme, veri sorumluluğunun ilgili organ veya çalışanlara devri anlamına gelmemekte olup, sorumluluk şirketin tüzel kişiliği üzerinde kalmaktadır.

KVKK'nın 3. maddesinde, *"Veri sorumlusu, kişisel verilerin işlenme amaçlarını ve vasıtalarını belirleyen, veri kayıt sisteminin kurulmasından ve yönetilmesinden sorumlu olan gerçek veya tüzel kişiyi ifade eder"* şeklinde bir tanım yapılmıştır. Bu doğrultuda, veri sorumlusu olabilmek için gerçek kişi olmak şart değildir, anonim şirketler tüzel kişilik oldukları için veri sorumlusu sıfatını taşır[290]. Şirketin veri sorumluluğu, tüzel kişiliği üzerinden gerçekleşir ve şirketin KVKK'dan doğan yükümlülükleri, anonim şirketin yönetimine ilişkin genel düzenlemeler çerçevesinde ele alınmalıdır. 6698 sayılı Kişisel Verilerin Korunması Kanunu uyarınca anonim şirketlerin "veri sorumlusu" sıfatıyla üstlendikleri yükümlülükler, yalnızca veri koruma hukukunun konusu değil, aynı zamanda şirketin iç yönetim yapısının bir parçası olarak ele alınmalıdır. Bu çerçevede, tüzel kişiliklerin genel hukuki yapısını ele alan TMK ve TTK hükümleriyle birlikte değerlendirme yapılması gerekir. TTK m. 374 uyarınca, anonim şirketin yönetimi ve dışarıya karşı temsili, kural olarak yönetim kuruluna aittir. Bu hüküm, veri sorumluluğundan doğan yükümlülüklerin de şirket adına ve hesabına yönetim kurulu tarafından

[287] Tüze Yılmaz, *op. cit.,* s.73-74.
[288] Kişisel Verileri Koruma Kurulu, Veri Sorumlularına İlişkin Rehber, 2021, s. 15-16.
[289] Bknz. s.109-110.
[290] KVKK'da veri sorumlusu tanımı, 6698 sayılı Kişisel Verilerin Korunması Kanunu'nun 3. maddesinin (ş) bendinde yer alır. Ancak gerçek kişi-tüzel kişi ayrımı açıkça ifade edilmez; veri sorumlusu, "kişisel verilerin işlenme amaçlarını ve vasıtalarını tek başına veya birlikte belirleyen gerçek veya tüzel kişi" olarak tanımlanır.

üstlenileceğini ortaya koyar. Ancak bu noktada, KVKK kapsamındaki işlemlerin doğrudan yönetim kurulu tarafından yerine getirilmesi gerektiği anlamı çıkarılmamalıdır. TTK m. 375'te sayılan ve devredilmesi yasak olan görev ve yetkiler arasında kişisel verilerin korunmasına ilişkin organizasyonel yükümlülüklere yer verilmemiştir. Bu durumda, veri işleme faaliyetlerinin planlanması, yürütülmesi ve denetimi gibi görevlerin uygun bir şekilde iç yönerge ile veya şirket içi görevlendirmelerle başka kişilere devredilmesi mümkündür[291]. Özellikle TTK m. 367 ve devamı hükümler uyarınca, yönetim kurulu, şirketin yönetimi ile ilgili görevleri üyeleri arasından seçeceği kişilere veya üçüncü kişilere devredebileceği gibi; TTK m. 370 çerçevesinde temsil yetkisini sınırlandırarak, şirket adına işlem yapabilecek sınırlı yetkili ticari vekiller de görevlendirebilir[292]. Bu kapsamda, veri güvenliği sorumlusu, KVKK uyum sorumlusu veya veri işleme birimi gibi organizasyonlar, yönetim kurulu kararıyla yapılandırılabilir. Sonuç olarak kanaatimizce; veri sorumlusuna ait yükümlülüklerin icrası bakımından anonim şirketlerde, bu işin organizasyonu yönetim kurulu eliyle yürütülmeli; ancak yetki devri ile içsel bir iş bölümü de oluşturulmalıdır. Bu hem KVKK'nın etkin şekilde uygulanmasını hem de TMK ve TTK'nın öngördüğü kurumsal yönetim ilkeleriyle uyumu sağlayacaktır. Bu bağlamda unutulmamalıdır ki şirket bünyesindeki birimler, yalnızca veri işleyen olarak hareket edebilirler, yani veri sorumlusunun verdiği yetkiye dayalı olarak kişisel verileri işleyebilirler, ancak veri sorumlusu olamazlar.

KVKK ve GDPR uyarınca, kişisel verilerin işlenme amaçlarını ve vasıtalarını belirleyen gerçek veya tüzel kişiler "veri sorumlusu" sıfatını kazanır. Bu tanımdan anlaşılacağı üzere şirketler, vakıf ve dernek gibi tüzel kişiler veri sorumlusu sıfatına haiz olabilir[293]. Şirketler topluluğu[294] söz konusu olduğunda, bir şirketler topluluğunun her bir şirketi ayrı bir tüzel kişilik taşıdığı için, her bir şirket kendi veri sorumlusu olabilir. Dolayısıyla, bir topluluk bünyesinde yer alan hakim şirket, eğer bağlı şirketlerin kişisel verilerini hangi amaçla ve nasıl işleyeceklerine karar veriyorsa, bu durumda yalnızca bağlı şirketler değil, hakim şirket de veri sorumlusu olarak

[291] Hayrettin Çağlar, Rıza Ayhan, Mehmet Özdamar, *op. cit.,* s.317.
[292] Kırca, Şehirali Çelik, Manavgat, *op. cit.,* s. 559-567, *Ibid*. s.318.
[293] Tekin Memiş, "Veri Sorumlusu ve Veri İşleyen Arasındaki İlişkiler ve Sorumluluk Düzeni", *Beykent Üniversitesi Hukuk Fakültesi Dergisi,* Cilt:3, Sayı:6, Aralık 2017, s.9-23.
[294] TTK'da doğrudan şirketler topluluğuna veya grup şirketlere ait bir tanım verilmese de Kurul'un 10 Nisan 2020 tarihinde internet sitesinde yayımladığı "Bağlayıcı Şirket Kuralları Hakkında Duyuru"nun ekleri olan "Veri Sorumluları İçin Bağlayıcı Şirket Kuralları Başvuru Formu" ve "Veri Sorumluları İçin Bağlayıcı Şirket Kurallarında Bulunması Gereken Temel Hususlara İlişkin Yardımcı Dokümanda grup ve grup şirket, *"bir şirketler topluluğuna bağlı olarak ekonomik faaliyetlerini sürdüren bir şirket veya teşebbüs olarak kişisel verilerin işlenmesi konusunda da diğer grup şirketler ile ortak bir ekonomik amaç içeren ve bu sebeple veri işleme faaliyetlerinde bulunan bir veri sorumlusu şirket olarak ele alınmıştır".*

değerlendirilir[295]. GDPR m. 26 kapsamında düzenlenen "joint controllership" (ortak veri sorumluluğu) ilişkisini her ne kadar KVKK açıkça düzenlememiş olsa da KVK Kurulu'nun kararları ve rehber dokümanlarında, benzer sorumluluk paylaşımı kabul edilmektedir. Eğer veri işleme kararları merkezi olarak (örneğin grup politikalarıyla) alınıyorsa, hakim şirket ile bağlı şirketler birlikte sorumlu olabilir[296]. Bu kapsamda, bağlı şirketlerde meydana gelen veri işleme faaliyetlerinin hukuka aykırı olması hâlinde, eğer bu işleme süreci hakim şirketin talimatı veya kontrolü doğrultusunda yürütülüyorsa, ortaya çıkan zararlardan; bağlı şirket, kendi tüzel kişiliğiyle, hakim şirket ise veri sorumlusu olarak veya ortak sorumlu sıfatıyla müteselsilen sorumlu tutulabilir[297]. Bu sorumluluk, TBK m. 61 ve devamındaki haksız fiil hükümleriyle, TTK m. 195 vd. çerçevesindeki hakimiyet ilişkisi ve KVKK m. 12'de yer alan veri güvenliği yükümlülüğü bağlamında birlikte değerlendirilmelidir. Sonuç olarak, topluluk bünyesinde veri işleme amacını ve vasıtalarını belirleyen hakim şirket, bağlı şirketlerdeki kişisel verilerin işlenmesinden doğrudan veri sorumlusu olarak sorumlu hale gelir. Bu durumda, veri işleme faaliyetinin hukuka aykırı olması halinde, hakim şirket de bağlı şirketle birlikte müteselsilen sorumlu tutulabilir.

Öte yandan, kişisel verilerin korunmasına ilişkin yükümlülüklerin ihlali, yalnızca idari sorumluluğa değil, aynı zamanda cezai sorumluluğa da neden olabilmektedir. Bu doğrultuda, hâkim şirketin, bağlı şirketlerin veri işleme süreçlerini doğrudan yönlendirdiği ve bu süreçlerdeki hukuka aykırılıklar nedeniyle mağduriyet doğduğu durumlarda, TCK m.136 kapsamında ceza sorumluluğu da gündeme gelebilecektir.

Veri işleyen kişilerin durumuna bakacak olursak, veri sorumlusunun verdiği yetkiyle, veri sorumlusunun organizasyonu dışındaki gerçek veya tüzel kişiler olarak, yalnızca verilen talimatlara uygun şekilde kişisel verileri işlerler. Bu doğrultuda anonim şirketler, veri sorumlusu sıfatıyla, verilerin güvenliğini sağlamak, ilgili yasal yükümlülükleri yerine getirmek ve veri sahiplerinin haklarını korumak için gerekli tüm adımları atmak zorundadır. Bu

[295] 27.02.2020 Tarihli, 2020/173 Sayılı KVK Kurul Kararı: Bir şirketler topluluğu bünyesinde yer alan şirketlerin, iş başvurusunda bulunan bir adayın açık rızası olmadan kişisel verilerini aynı veri tabanında paylaşması durumunda, her bir şirketin ayrı ayrı veri sorumlusu olduğu ve bu nedenle her birinin sorumluluğunun bulunduğu belirtilmiştir. Bu karar, topluluk şirketleri arasında kişisel verilerin paylaşımında, her bir şirketin veri sorumlusu olarak sorumluluğunun bulunduğunu ve hâkim şirketin de veri sorumlusu olarak değerlendirilebileceğini göstermektedir. https://www.kvkk.gov.tr/Icerik/5410/Is-Basvurusu-Surecinde-Islenen-Kisisel-Verilerin-Hukuka-Aykiri-Sekilde-Paylasilmasi, (E.T.: 25.05.2025).

[296] Örneğin, çok uluslu bir grup şirketin Türkiye'deki bağlı şirketi, personel verilerini ana merkeze aktarıyorsa ve bu aktarımın amacı, yöntemi ve süresi grup genel merkezince belirleniyorsa, olası bir veri ihlalinde hem Türkiye'deki şirket hem de hakim şirket, veri sorumlusu olarak sorumlu tutulabilir.

[297] Dülger, *op. cit*. s.25.

sorumluluk, yalnızca verilerin doğru şekilde işlenmesi değil, aynı zamanda verilerin güvenliğinin sağlanması ve veri sahiplerinin haklarının korunması anlamına gelir. Kişisel verilerin yurt dışına aktarılması durumunda anonim şirketlerin yükümlülükleri daha da artmaktadır, çünkü yurt dışında farklı hukuk sistemlerine ve güvenlik standartlarına tabi olabilecek verilerin korunması daha büyük bir önem taşır. Anonim şirketlerin veri sorumlusu olarak yükümlülüklerini yerine getirirken veri politikalarını oluşturması, veri sahiplerini bilgilendirmesi, veri güvenliği tedbirlerini alması, veri işleme faaliyetlerini kayıt altına alması ve uluslararası veri transferlerinde GDPR ve KVKK ile uyumluluğu sağlaması gerekmektedir.

TTK 367. maddesi uyarınca yönetim kurulunun iç yönerge düzenleyerek şirketin yönetimine ilişkin belirli görev ve yetkileri devretme imkanına sahip olduğunu üst başlıkta açıklamıştık. Bu kapsamda anonim şirketler, kişisel verilerin korunması alanında da benzer bir yetki devri mekanizmasını uygulamaktadır. KVKK ve ilgili ikincil düzenlemeler uyarınca, veri sorumlusu sıfatına sahip olan anonim şirketler, kişisel verilerin işlenmesi ve korunmasına yönelik uyum süreçlerini yürütmek üzere KVKK uyum komisyonları veya kişisel veri koruma birimleri oluşturmaktadır[298]. Yönetim kurulu, kişisel veri işleme faaliyetlerinin mevzuata uygunluğunu sağlamak, KVKK kapsamındaki gereklilikleri yerine getirmek amacıyla bu birimlere belirli yetkiler devredebilmekte; böylece veri sorumlusu olarak üstlendiği yükümlülükleri profesyonel bir çerçevede yerine getirebilmektedir. Ancak, veri sorumlusu sıfatı doğrudan yönetim kuruluna ait olduğundan, bu yetki devri, sorumluluğun tamamen ortadan kalkması sonucunu doğurmamakta; yönetim kurulu, atadığı yöneticilerin ve KVKK komisyonlarının faaliyetlerini gözetme ve denetleme yükümlülüğünü sürdürmektedir. Bu tür yapılanmalar, şirketlerin veri koruma süreçlerini daha etkin yönetmesine ve KVKK'ya uyumluluğu kurumsal bir çerçevede sağlamasına katkı sunmaktadır. Anonim şirketlerde uyum kavramı Türk hukukunda açıkça düzenlenmese de "compliance" kavramı ile ifade edilmekte ve uygulamada şirketler, şirketin genel denetiminden ve yönetiminden sorumlu en yüksek organ olan yönetim kurulu aracılığıyla uyum/compliance birimleri kurarak şirketin faaliyetlerinin, yasal düzenlemelere, iç politikalara, etik kurallara ve sektör normlarına uygun olmasını sağlama sürecini yönetmektedirler[299].

[298] Örneğin; bknz., Niğde Ömer Halisdemir Üniversitesi Kişisel Verilerin Korunması ve İşlenmesi Politikası, https://ohu.edu.tr/kvkk/sayfa/kvk-ve-islenmesi-politikasi, İstanbul Gelişim Üniversitesi Kişisel Verileri Koruma Komisyonu Çalışma Usul Ve Esaslarına İlişkin Yönerge, https://resim.gelisim.edu.tr/YONETMELIK_YONERGE/kisiselverilerikorumakomisyonucalismausulveesaslarinailiskinyonerge_09_06_2023.pdf, (Erişim Tarihi:02.04.2025).

[299] Ali Paslı, *"Compliance" Kavramının Anonim Ortaklıklar Hukukundaki Anlamı ve Sorumluluk Sistemine Etkisi",* İÜHFM, Cit 71, Sayı 2, 2013, s. 317; Hasan Pulaşlı, *"Compliance Kavramı ve Yönetim Organının Compliance Sorumluluğu"*, BATIDER, Cilt 35, Sayı 2, 2019, s. 689; Yaşar, Anonim Şirketler Hukukunda Uyum (Compliance), s. 9; Pulaşlı, *op.cit*. s. 31.

TTK'ya göre, şirketin yasal düzenlemelere uygunluğu, mali raporlama ve finansal şeffaflık gibi önemli konularda Yönetim Kurulu'nun sorumluluğu bulunmaktadır. Compliance biriminin oluşturulması ve işlevselliği de Yönetim Kurulu tarafından belirlenir. Compliance, özellikle şirketlerin hukuki sorumluluklarını yerine getirmeleri ve riskleri minimize etmeleri, bir bakımdan önleyici hukuk etkisi göstermesi açısından önemlidir[300]. Yönetim Kurulu, şirketin günlük işleyişinde compliance biriminin fonksiyonlarını yerine getirebilmesi için belirli yetkileri devredebilir. Bu yetkiler genellikle şirket içi denetim ve kontrol süreçlerini içerir. Yönetim Kurulu, compliance biriminin faaliyetlerini denetlerken, uyum ihlallerinin tespit edilmesi durumunda sorumluluğu üstlenir[301]. Uyum yükümlülüğü, şirketin mümkün olan en iyi organizasyonla sorumluluğundan muaf tutulması anlamına gelmektedir ve doğru şekilde uygulandığında, veri sorumlusu şirketi sorumluluktan kurtarabilmektedir. Bu durum, Kişisel Verileri Koruma Kurulu'nun verdiği kararlarda da açıkça görülmektedir. Kurul kararlarında, veri sorumlusunun uygun iç denetim ve uyum mekanizmaları kurarak kişisel verilerin korunmasına yönelik gerekli tedbirleri alması durumunda, olası veri ihlali sonucu şirketin sorumluluğunun sınırlanabileceği görülmektedir[302]. Bu karar, şirketin veri sorumlusunu ataması ve uygun uyum süreçlerini oluşturması halinde sorumluluğunun daha fazla sorgulanamayacağını göstermektedir.

GDPR'a göre veri sorumlusu kavramı ise kanunun 4. maddesinin 7. fıkrası uyarınca kişisel verilerin işlenme amaçlarını ve araçlarını belirleyen gerçek veya tüzel kişi, kamu kurumu, ajans veya diğer herhangi bir kuruluştur. Veri sorumlusu, veri işleme faaliyetlerinin temel belirleyicisi olup kişisel verilerin hukuka uygun şekilde işlenmesini sağlamakla yükümlüdür. Bu kapsamda veri sorumlularının GDPR'ın temel ilkelerine (Hukuka uygunluk ilkesi, şeffaflık ve hesap verilebilirlik ilkesi, teknik ve idari önlemler, ilgili kişi haklarına saygı ilkeleri gibi) uygun bir şekilde kişisel veri işleme yükümlülükleri bulunmaktadır. GDPR, doğrudan AB üyesi olmayan ülkelerdeki şirketler için bağlayıcı olmasa da belirli koşullar altında Türkiye'de faaliyet gösteren anonim şirketleri de kapsayabilir[303]. GDPR'ın 3. maddesi, tüzüğün coğrafi uygulama alanını yalnızca AB sınırları içerisinde yerleşik veri sorumlularıyla sınırlı tutmamaktadır. Bu madde uyarınca, AB dışında yer alan veri sorumluları da belirli koşullar altında GDPR'a tabi olabilmektedir. Özellikle AB'de bulunan gerçek kişilere mal veya hizmet

[300] *Ibid.*
[301] Çekin, *op. cit.*
[302] Bknz. KVKK, 05.05.2020, 2020/344 sayılı karar. https://www.kvkk.gov.tr/Icerik/6764/2020-344, (Erişim Tarihi:03.04.2025).
[303] Kuner, *op. cit. s.*

sunulması ya da bu kişilerin davranışlarının izlenmesi gibi faaliyetler söz konusu olduğunda, GDPR hükümleri devreye girmektedir[304]. Bu çerçevede, Türkiye'de kurulu anonim şirketlerin GDPR'a tabi olup olmadıkları, belirli kriterler üzerinden değerlendirilmektedir. Söz konusu kriterler arasında; AB'de bulunan gerçek kişilere yönelik mal veya hizmet sunulması, bu kişilerin davranışlarının izlenmesi ve AB içerisinde bir şube, ofis ya da temsilciliğin bulunması yer almaktadır. Örneğin bir Türk anonim şirketi, AB'de mukim tüketicilere yönelik e-ticaret faaliyetinde bulunuyor ve bu süreçte kişisel verilerini topluyorsa, GDPR yükümlülükleri gündeme gelmektedir[305]. Aynı şekilde, AB'deki bireylerin çevrim içi davranışlarını çerezler (cookies) veya analitik araçlar vasıtasıyla izleyen şirketler de GDPR kapsamında değerlendirilmektedir[306]. Ayrıca, Avrupa Birliği sınırları içinde şube, temsilcilik veya yetkilendirilmiş bir kişi aracılığıyla faaliyet gösteren anonim şirketler açısından da GDPR hükümlerinin uygulanabilirliği söz konusudur[307]. Buna ek olarak, AB ile doğrudan ticari ilişkileri bulunan ancak AB sınırları içinde fiziki bir varlığı bulunmayan Türk şirketlerinin, veri aktarımı veya işleme faaliyetleri bakımından dolaylı GDPR yükümlülükleriyle karşılaşmaları mümkündür[308]. Türk anonim şirketlerinin GDPR'a uyum sağlayabilmeleri için bir dizi teknik ve hukuki önlem almaları gerekmektedir. Bunlar arasında öncelikle, kişisel veri işleme faaliyetlerinin sistematik biçimde belgelendiği bir Kişisel Veri İşleme Envanteri hazırlanmalı; işlenen verilerin türü, işleme amacı, saklama süresi ve aktarım biçimi gibi hususlar açıkça ortaya konmalıdır[309]. Ayrıca, veri sahiplerinden açık rıza alınması ve bu rızanın GDPR'ın şeffaflık, bilgilendirme ve özgürlük ilkeleri çerçevesinde sağlanması gerekmektedir[310].Bunların yanında, şirketler kişisel verilerin korunmasını temin etmek amacıyla teknik ve organizasyonel güvenlik önlemleri almak zorundadır. Bu tedbirler; veri şifreleme, erişim kontrolü, düzenli sızma testleri gibi uygulamaları içerebilir[311]. Özellikle büyük ölçekli veri işleme faaliyetleri

---

[304] Regulation (EU) 2016/679 of the European Parliament and of the Council (GDPR), Article 3.
[305] Prighter, "AB GDPR İşletmeniz İçin Geçerli mi?", https://prighter.com/tr/resources/does-the-gdpr-apply-to-me/ , (E.T: 25 Nisan 2025).
[306] Kuner, C., *Transborder Data Flows and Data Privacy Law*, Oxford University Press, 2020, s. 104.
[307] GDPR, md. 27.
[308] KVKK, *"Yurtdışında yerleşik Tüzel kişilerin Türkiye'deki Şubeleri ile İlgili Değerlendirme",* https://www.kvkk.gov.tr/Icerik/5545/2019-225, (E.T: 25 Nisan 2025).
[309] KVKK, *Kişisel Veri İşleme Envanteri Hazırlama Rehberi*, 2020, https://www.kvkk.gov.tr/Icerik/5446/Kisisel-Veri-Isleme-Envanteri-Hazirlama-Rehberi, (E.T: 25 Nisan 2025).
[310] GDPR, md. 7.
[311] Kişisel Verileri Koruma Kurulu, 09.10.2020 tarih ve 2020/787 sayılı Karar, Erişim: https://www.kvkk.gov.tr/Icerik/6939/Kurul-Kararlari (E.T. 21.05.2025).
Kişisel Verileri Koruma Kurulu'nun 09.10.2020 tarihli ve 2020/787 sayılı kararında, bir anonim şirketin veri güvenliği konusunda almış olduğu çeşitli teknik ve idari tedbirler örnek gösterilmiş ve bu uygulamaların "makul tedbirler" kapsamında olduğu değerlendirilmiştir. ISO 27001 tabanlı eğitimler, sızma testleri, ağ güvenliği, kurumsal politika geliştirme ve iç denetimler gibi önlemler, veri sorumlularının Kanun'un 12. maddesi kapsamında almakla yükümlü olduğu güvenlik tedbirlerine somut bir örnek teşkil eder. Bu karar, özellikle veri güvenliği düzeyinin belirlenmesinde Kurul'un hangi kriterlere dikkat ettiğini göstermesi açısından önemlidir.

yürüten şirketlerin, GDPR'ın 37. maddesi uyarınca bir Veri Koruma Görevlisi (Data Protection Officer – DPO) atamaları gerekebilir[312]. Bu yükümlülüklere uyum sağlanması, yalnızca idari yaptırımlardan kaçınmak açısından değil, aynı zamanda Avrupa pazarıyla sürdürülebilir ilişkiler tesis edilmesi bakımından da önem taşımaktadır.

Sonuç olarak, anonim şirketler, kişisel verilerin işlenmesi sürecinde veri sorumlusu sıfatıyla hareket etmekte olup, KVKK ve GDPR kapsamında tanımlanan tüm yükümlülüklere tabidir. Veri işleme faaliyetlerinin ilgili mevzuata uygun bir şekilde yürütülmesini sağlamak amacıyla etkin bir veri yönetim sisteminin kurulması ve sürekli denetim mekanizmalarının işletilmesi kritik bir gerekliliktir. Türk anonim şirketleri, özellikle AB'deki bireylere yönelik hizmet sunuyorsa veya onların verilerini işliyorsa, GDPR'a tabi olabilir. Bu çerçevede, Türk anonim şirketlerinin GDPR'a uyum sağlamak için gerekli teknik ve hukuki önlemleri alması büyük önem arz etmektedir. Uyum sürecinin etkin şekilde yönetilmesi, şirketlerin uluslararası pazarda rekabet gücünü artırırken, veri güvenliği ve hukuka uygunluk konularında da güçlü bir yapı oluşturmasına katkı sağlayacaktır.

## 3. ANONİM ŞİRKETLER TARAFINDAN İŞLENEN KİŞİSEL VERİ KATEGORİLERİ

Anonim şirketler, faaliyet gösterdikleri sektöre bağlı olarak farklı türde kişisel verileri işlemektedir. Bu bölümde, anonim şirketlerin çeşitli ticari faaliyetleri çerçevesinde işledikleri kişisel veri kategorileri sınıflandırılarak ele alınacak ve bu verilerin hangi amaçlarla işlendiği değerlendirilecektir.

İlk bölümde açıkladığımız üzere kişisel veri, 6698 sayılı Kişisel Verilerin Korunması Kanunu uyarınca, *kimliği belirli veya belirlenebilir gerçek kişiye ilişkin her türlü bilgi* olarak tanımlanmaktadır (m.3/1-d). Kanunda yer alan bu tanım doğrultusunda, kişisel verinin yalnızca gerçek kişilerle sınırlı olduğu ve tüzel kişilere ait bilgilerin ancak gerçek kişilerle ilişkilendirildiği ölçüde kişisel veri olarak nitelendirilebileceği sonucuna ulaşılmaktadır. Bu çerçevede, bir anonim şirkete ait ticaret unvanı, adres veya vergi numarası gibi bilgiler kişisel veri kapsamında değerlendirilmezken, bu bilgilerin gerçek kişilerle ilişkilendirilmesi halinde kişisel veri niteliği kazanabileceği kabul edilmektedir[313]. Örneğin, bir işletmenin sahibi olan

[312] GDPR, md. 37–39.
Veri Koruma Görevlisi, bir kuruluşun kişisel veri işleme süreçlerini izleyen, bu süreçlerin mevzuata uygunluğunu sağlayan ve düzenleyici kurumlarla iletişimi yürüten sorumlu kişidir.
[313] Kişisel Verileri Koruma Kurulu, 25/03/2019 tarihli ve 2019/81 sayılı Karar Özeti, https://www.kvkk.gov.tr/Icerik/5496/2019-81-165 (Erişim: 17 Mayıs 2025).

kişinin ticari faaliyetlerine dair bilgiler, doğrudan şahıs ile ilişkilendirildiğinde kişisel veri niteliği taşıyabilir. Kişisel veri kavramı, yalnızca bireylerin kimlik bilgilerinden ibaret olmayıp, gerçek kişiye ilişkin her türlü bilgiyi kapsamaktadır[314]. Bu bağlamda, bir gerçek kişiyi tanımlayan ad, soyad, T.C. kimlik numarası, iletişim bilgileri gibi temel unsurların yanı sıra, gerçek kişiye ait sağlık verileri, finansal bilgiler, iletişim bilgileri, mesleki ve biyometrik veriler, fiziksel, psikolojik, ekonomik, kültürel ya da sosyal kimliğine dair her türlü veri de kişisel veri kapsamında değerlendirilmektedir[315].

Anonim şirketler, Türkiye'de geniş bir sektörel yelpazede faaliyet gösteren kurumsal işletmelerdir. KVKK ve ilgili ikincil düzenlemeler çerçevesinde, anonim şirketlerin faaliyet alanlarına bağlı olarak işleyebileceği kişisel veriler çeşitli kategorilere ayrılmaktadır. Anonim şirketlerin işleyebileceği kişisel veri kategorileri arasında kimlik bilgileri (ad, soyad, T.C. kimlik numarası, doğum tarihi), iletişim bilgileri (telefon numarası, e-posta adresi, ikamet adresi), finansal veriler (banka hesap bilgileri, kredi kartı bilgileri, ödeme geçmişi, gelir bilgileri), sağlık verileri (hastalık geçmişi, laboratuvar sonuçları, reçeteler, tıbbi teşhisler), biyometrik ve genetik veriler (parmak izi, retina taraması, ses kayıtları), mesleki ve eğitim verileri (diploma bilgileri, meslek unvanı, çalışma geçmişi) ile dijital ve teknolojik veriler (IP adresleri, çerez kayıtları, giriş-çıkış zamanları, sosyal medya hesap bilgileri) yer almaktadır[316]. Şirketin kurulduğu faaliyet alanı ise şirketin konusunu oluşturur[317]. Bankacılık, sigortacılık, perakende, enerji, e-ticaret, sağlık ve telekomünikasyon gibi birçok alanda faaliyet gösteren anonim şirketler, sundukları hizmetler çerçevesinde bireylerin kişisel verilerini işleyebilmektedir. Bu veriler, şirketin faaliyet konusuna bağlı olarak farklı kategorilere ayrılmaktadır. Örneğin, finans sektörü içerisinde faaliyet gösteren bankalar ve sigorta şirketleri, müşterilerine ait kimlik bilgilerini, kredi ve ödeme geçmişlerini, finansal verilerini ve risk analizlerine yönelik bilgileri işlemektedir. Sağlık sektöründe faaliyet gösteren özel hastaneler veya ilaç şirketleri ise hastalara ait tıbbi verileri, reçete bilgilerini ve sağlık geçmişlerini işlemektedir. Perakende ve e-ticaret sektörlerinde faaliyet gösteren anonim şirketler, müşteri

[314] Kişisel Verilerin Korunması Kanunu (Kanun No. 6698), m. 3/1(d).
[315] Kişisel Verileri Koruma Kurumu, *Kişisel Veri Kavramı Hakkında Rehber*, 2020, s.4-5, https://kvkk.gov.tr/Icerik/6649/Kisisel-Veri-Kavrami-Hakkinda-Rehber. (Erişim: 17 Mayıs 2025).
[316] Kişisel Verileri Koruma Kurumu, "Kişisel Veri Nedir?", https://www.kvkk.gov.tr/Icerik/3785/Kisisel-Veri-Nedir- (Erişim: 17 Mayıs 2025).
[317] Selma Çetiner, Armağan Ebru Bozkurt Yüksel, *"Ticari İşletme ve Şirketler Hukuku"*, Ankara, Seçkin Yayıncılık, 2024, s.242.

sadakat programları kapsamında isim, soy isim, iletişim bilgileri, satın alma geçmişi ve ödeme bilgileri gibi verileri toplayarak kişiselleştirilmiş hizmetler sunmaktadır.

KVKK'nın 5. maddesi kapsamında, kişisel verilerin işlenebilmesi için ilgili kişinin açık rızasının alınması esas olmakla birlikte, belirli şartlar altında açık rıza aranmaksızın da işleme faaliyetleri gerçekleştirilebilir. Bu kapsamda, kanunlarda açıkça öngörülmesi, bir sözleşmenin kurulması veya ifasıyla doğrudan ilgili olması, veri sorumlusunun hukuki yükümlülüğünü yerine getirebilmesi, bir hakkın tesisi, kullanılması veya korunması için işleme faaliyetinin zorunlu olması gibi hukuki sebeplerin varlığı halinde kişisel veriler işlenebilir. Örneğin, bir bankanın müşteriyle kredi sözleşmesi yaparken T.C. kimlik numarası, adres, gelir bilgisi gibi kişisel verileri işlemesi, sözleşmenin ifasıyla doğrudan ilgili olduğundan, açık rıza alınmaksızın gerçekleştirilebilir[318]. KVKK'nın 6. maddesi, sağlık verileri ve biyometrik veriler gibi özel nitelikli kişisel verilerin işlenmesine ilişkin daha sıkı düzenlemeler içermektedir. Kanuna göre, özel nitelikli kişisel verilerin işlenmesi, kural olarak ilgili kişinin açık rızasına tabidir. Ancak sağlık ve cinsel hayata ilişkin veriler, yalnızca kamu sağlığının korunması, koruyucu hekimlik, tıbbi teşhis, tedavi ve bakım hizmetlerinin yürütülmesi gibi sebeplerle, sır saklama yükümlülüğü altındaki kişiler veya yetkili kurumlar tarafından açık rıza aranmaksızın işlenebilir. Örneğin, bir özel hastanenin hastalarına sunduğu sağlık hizmetleri kapsamında, teşhis ve tedavi sürecinde elde ettiği laboratuvar sonuçlarını işlemesi, açık rıza alınmaksızın gerçekleştirilebilir. Ancak hastanenin bu verileri başka bir amaçla üçüncü taraflarla paylaşması, ilgili kişinin açık rızasını gerektirebilir[319]. Anonim şirketlerin faaliyet gösterdiği sektörlere bağlı olarak işlenen veriler değişiklik gösterebileceğinden, her bir işleme faaliyetinin KVKK'nın 4. maddesinde düzenlenen genel ilkelere uygun olması gerekmektedir. Bu çerçevede veri işleme faaliyetlerinin hukuka ve dürüstlük kurallarına uygun olması, doğru ve

[318] Bir bankanın, müşterisiyle kredi sözleşmesi yaparken T.C. kimlik numarası, adres, gelir bilgisi gibi kişisel verileri işlemesi, 6698 sayılı Kişisel Verilerin Korunması Kanunu'nun 5. maddesinin 2. fıkrası uyarınca, "bir sözleşmenin kurulması veya ifasıyla doğrudan ilgili olması" veri işleme şartına dayandığı için, açık rıza alınmaksızın gerçekleştirilebilir. Bu durum hem Kurul kararlarında hem de bankaların uygulama politikalarında açıkça belirtilmiştir. Bknz: Kişisel Verileri Koruma Kurulu, 02.03.2021 tarihli karar özetleri, https://www.kvkk.gov.tr/Icerik/7264/2021-1107, (E.T.:17.05.2025); Türkiye Halk Bankası A.Ş., "Kişisel Verilerin Korunması ve İşlenmesi Politikası", s. 7, https://www.halkbank.com.tr/content/dam/corporate-website/tr/dokumanlar/dijital-bankacilik/kvkk/kisisel-verilerin-korunmasi-ve-islenmesi-politikasi.pdf,(E.T.:17.05.2025).

[319] Bu husus, Kişisel Verileri Koruma Kurulu'nun 05.12.2018 tarihli ve 2018/143 sayılı kararında açıkça belirtilmiştir. https://www.kvkk.gov.tr/Icerik/5364/2018-143. Ayrıca, Kişisel Verileri Koruma Kurulu'nun 02.05.2023 tarihli ve 2023/692 sayılı kararında da benzer bir değerlendirme yapılmıştır. Kararda, özel sağlık kuruluşlarının, sundukları sağlık hizmetlerini açık rıza şartına bağlamalarının hukuka aykırı olduğu belirtilmiştir. Bu durum, sağlık hizmetlerinin sunulması için açık rıza alınmasının zorunlu olmadığını, ancak verilerin başka amaçlarla işlenmesi veya paylaşılması durumunda açık rızanın gerekli olduğunu göstermektedir. https://www.kvkk.gov.tr/Icerik/7691/2023-692. (Erişim Tarihi: 17.05.2025).

güncel tutulması, belirli, açık ve meşru amaçlar için işlenmesi, işlendikleri amaçla bağlantılı, sınırlı ve ölçülü olması ve ilgili mevzuatta öngörülen süre kadar muhafaza edilmesi gerekmektedir. Örneğin, bir e-ticaret platformunun müşterilerinin alışveriş geçmişini analiz ederek kişiselleştirilmiş reklam ve kampanyalar sunması, ancak bu verileri süresiz olarak saklaması veya müşterinin rızası dışında üçüncü taraflarla paylaşması, KVKK'nın veri işleme ilkelerine aykırı olacaktır[320].

Anonim şirketler tarafından işlenen kişisel veriler, veri kategorilerine ek olarak işleme amacına göre de farklılaşmaktadır. Çalışan verileri, iş sözleşmesinin kurulması ve ifası, bordro süreçlerinin yürütülmesi, sosyal hakların sağlanması ve iş güvenliği tedbirlerinin alınması gibi amaçlarla işlenmektedir. Örneğin, bir anonim şirketin insan kaynakları departmanı, çalışanların kimlik ve iletişim bilgilerini kayıt altına alarak maaş ödemeleri için finansal bilgilerini işleyebilir. Müşteri verileri, şirketin sunduğu mal veya hizmetlerden faydalanan bireylerin kimlik ve iletişim bilgilerinin yanı sıra, satın alma geçmişleri ve pazarlama tercihlerini içerebilir. Örneğin, bir e-ticaret sitesinin müşterilere kişiselleştirilmiş kampanyalar sunabilmesi için sipariş geçmişini analiz etmesi, KVKK'nın 5. maddesi kapsamında meşru menfaat ilkesine dayalı bir veri işleme faaliyeti olarak değerlendirilebilir. Tedarikçi ve iş ortağı verileri, ticari faaliyetlerin yürütülebilmesi amacıyla sözleşme süreçlerinin yönetilmesi, ödeme işlemlerinin gerçekleştirilmesi ve muhasebe kayıtlarının tutulması gibi nedenlerle işlenmektedir. Örneğin, bir anonim şirketin, düzenli olarak hizmet aldığı bir yazılım firmasının banka hesap bilgilerini işleyerek ödeme süreçlerini yönetmesi bu kapsamda değerlendirilebilir. Finansal veriler ise faturalandırma, muhasebe ve yasal yükümlülüklerin yerine getirilmesi amacıyla işlenmektedir. Özellikle bankacılık ve sigortacılık sektöründe faaliyet gösteren anonim şirketler, müşterilerin kredi kartı ve hesap bilgilerini, ödeme işlemlerinin güvenli bir şekilde gerçekleştirilmesi amacıyla işlemektedir[321]. Anonim şirketler tarafından işlenen kişisel veriler, şirketin faaliyet gösterdiği sektöre ve işleyiş amacına göre de farklılık göstermektedir. Sektörel örnekler, özel nitelikli kişisel veriler ve günlük işleyişten senaryolar kapsamında, çeşitli sektörlerin kişisel veri işleme süreçleri şu şekilde özetlenebilir: Sağlık sektöründe, özel hastaneler, ilaç şirketleri ve sigorta firmaları, hastaların sağlık geçmişi, laboratuvar sonuçları, reçeteleri ve tıbbi

[320] Kişisel Verileri Koruma Kurulu, 03.08.2022 tarihli ve 2022/774 sayılı Karar Özeti,
Bu karar, e-ticaret platformlarının kişisel veri işleme faaliyetlerinde KVKK'nın belirlediği ilkelere uyulmasının önemini vurgulamaktadır. Özellikle, kişisel verilerin işlenmesi için ilgili kişilerin açık rızasının alınması ve verilerin yalnızca işlendikleri amaç için gerekli olan süre kadar muhafaza edilmesi gerekmektedir. https://www.kvkk.gov.tr/Icerik/7571/2022-774. (Erişim Tarihi: 17.05.2025).

[321] Kişisel Verileri Koruma Kurulu, 25.11.2021 tarihli ve 2021/1262 sayılı Karar, https://www.kvkk.gov.tr/Icerik/7287/2021-1262, Kişisel Verileri Koruma Kurulu, 26.01.2023 tarihli ve 2023/78 sayılı Karar, https://www.kvkk.gov.tr/Icerik/7596/2023-78, (E.T. 17.05.2025).

teşhislerini işleyerek doğru tedavi süreçleri sunar. Örneğin, bir özel hastane, hastalarının sağlık verilerini kayıt altına alarak doktorlarla paylaşır[322]. E-ticaret ve perakende alanında, online alışveriş platformları müşteri sipariş geçmişi, ödeme bilgileri, IP adresi ve gezinti alışkanlıklarını analiz ederek kişiselleştirilmiş reklam ve kampanyalar sunar. Örneğin, bir e-ticaret sitesi, müşterisinin en çok satın aldığı ürünleri baz alarak özel indirimler sağlayabilir.

Finans ve bankacılık sektöründeki anonim şirketler (bankalar, sigorta şirketleri, yatırım firmaları vb.), müşteri bilgilerini, mevzuata uygun olarak kimlik doğrulama ve güvenlik (hesap açılışı, iş güvenliği, dolandırıcılık önleme), kredi risk analizleri, sigorta poliçeleri oluşturma, regülatif uyumluluk, kara parayı önleme (Anti Money Laundering- AML[323]) ve terör finansmanının önlenmesi, pazarlama ve müşteriye özel teklifler ile finans danışmanlığı gibi sebeplerle işlemektedir. Bankalar, müşterilerinin kimlik bilgileri, kredi notu, hesap hareketleri ve yatırım işlemlerini işleyerek kredi risk değerlendirmesi yapar. Örneğin, bir banka, kredi başvurusu yapan kişinin kredi notunu analiz ederek uygun faiz oranını belirleyebilir. Bu süreçte, özellikle "Müşterini Tanı" (Know Your Customer- KYC) ilkesi büyük bir önem arz etmektedir. KYC süreci, finansal kuruluşların müşterilerini tanıması, kimliklerini doğrulaması ve finansal risklerini değerlendirmesi için uyguladığı bir dizi prosedürü içermektedir. KYC sürecinin ilk aşamasını kimlik tespiti oluşturmaktadır[324]. Bu kapsamda, müşterilerin kimlik belgeleri (nüfus cüzdanı, pasaport veya ehliyet gibi resmi belgeler) ve adres bilgileri talep edilerek doğrulama süreçlerinden geçirilmektedir. Bu işlemler hem manuel hem de elektronik yöntemler aracılığıyla gerçekleştirilmekte olup, kimlik sahtekarlığı ve dolandırıcılık girişimlerinin önlenmesi açısından kritik bir öneme sahiptir. İkinci aşamada, müşteri profilleme ve risk değerlendirme süreçleri devreye girmektedir. Bu süreçte müşterinin finansal geçmişi, gelir kaynakları ve işlem alışkanlıkları analiz edilerek olası risk faktörleri belirlenmekte ve bu doğrultuda önlemler alınmaktadır. Finansal kurumlar, kara para aklama ve terör finansmanı ile mücadele kapsamında, müşteri işlemlerini sürekli olarak izleyerek olağan dışı hareketleri tespit

[322] Kişisel Verileri Koruma Kurulu, 25.03.2019 tarihli ve 2019/78 sayılı Karar, https://www.kvkk.gov.tr/Icerik/6786/2019-78 , E.T. 17.05.2025; Kişisel Sağlık Verileri Hakkında Yönetmelik, RG, T. 21.06.2019, S. 30808, m. 4, 5, 6.

[323] Detaylı bilgi için bknz. Basel Committee on Banking Supervision (2017). Sound Management of Risks Related to Money Laundering and Financing of Terrorism. https://www.bis.org/bcbs/publ/d505.pdf, Financial Action Task Force (FATF) (2021). Anti-Money Laundering and Counter-Terrorist Financing Measures, https://www.fatf-gafi.org/en/countries/detail/Turkey.html, (Erişim Tarihi: 03.04.2025).

[324] Ali Batan, A Quick Overview of Know Your Customer (KYC) in Financial Industry, https://www.researchgate.net/publication/357173989_A_Quick_Overview_of_Know_Your_Customer_KYC_in_Financial_Industry, (Erişim Tarihi:03.04.2025)

etmekte ve gerekli durumlarda yetkili makamlara bildirimde bulunmaktadır[325]. Kişisel veri işleme süreçleri, yalnızca müşteri kimlik doğrulama ve risk analizleri ile sınırlı kalmamakta, aynı zamanda müşteri hizmetleri ve pazarlama faaliyetlerinde de önemli bir yer tutmaktadır. Finansal kuruluşlar, müşterilere özelleştirilmiş hizmetler sunabilmek ve onların ihtiyaçlarına uygun finansal ürünler geliştirebilmek amacıyla kişisel verileri analiz etmekte ve değerlendirmektedir. Ancak, bu süreçte müşteri gizliliği ve veri güvenliği en üst düzeyde korunmalıdır. KVKK ve GDPR gibi düzenlemeler, finans kuruluşlarına belirli yükümlülükler getirmekte ve kişisel verilerin işlenmesine yönelik çeşitli kısıtlamalar ve prensipler belirlemektedir. Finans sektörüne ek olarak, diğer sektörlerde de kişisel veri işleme süreçleri büyük önem taşımaktadır. Turizm ve konaklama sektöründe, oteller müşterilerinin kimlik bilgilerini, rezervasyon geçmişlerini, özel isteklerini ve ödeme detaylarını saklayarak hizmet kalitesini artırabilir. Örneğin, bir otel, önceki konaklamasında vejetaryen yemek talep eden bir müşteriye, sonraki ziyaretinde aynı hizmeti sunabilmek için bu bilgiyi saklar[326]. Telekomünikasyon alanında ise GSM operatörleri, kullanıcıların çağrı kayıtlarını, internet kullanım verilerini ve fatura bilgilerini işleyerek müşteri hizmetleri sunar. Örneğin, bir mobil operatör, müşterisinin internet kullanım alışkanlıklarını analiz ederek ona özel bir tarife önerisi yapabilir[327]. Bu çerçevede, finans ve diğer sektörlerde faaliyet gösteren anonim şirketlerin veri işleme faaliyetlerinde hukuki çerçeveye tam uyum sağlaması gerekmektedir. Kişisel veriler, ilgili bireyin açık rızası alınmadan işlenemez ve belirlenen amaç dışında kullanılamaz. Ayrıca, verilerin saklanması ve işlenmesi süreçlerinde şeffaflık ilkesine bağlı kalınarak müşterilere gerekli bilgilendirme yapılmalı ve hesap verebilirlik sağlanmalıdır. Buna ek olarak, yetkisiz erişimi önlemek amacıyla veri güvenliği önlemleri alınmalı ve siber güvenlik tehditlerine karşı gerekli teknik tedbirler uygulanmalıdır. Müşteriler, belirli şartlar altında kişisel verilerinin silinmesi veya anonim hale getirilmesini talep edebilir ve finansal kuruluşlar bu talepleri yasal süreler içinde yerine getirmekle yükümlüdür.

---

[325] Allıy Bello, Davıd Amoah Oduro, Emmanuel Opoku, Adepeju Deborah Bello, Adenıjı Omotayo Leo, Chıoma Emmanuel Ukatu, Nonso Okıka, Enhancing Know Your Customer (Kyc) And Anti-Money Laundering (Aml) Compliance Using Blockchain: A Business Analysis Approach. Iconıc Research And Engıneerıng Journals, Volume 8 Issue 9, Mar 2025. https://www.researchgate.net/publication/389814116_Enhancing_Know_Your_Customer_KYC_and_Anti-Money_Laundering_AML_Compliance_Using_Blockchain_A_Business_Analysis_Approach, (Erişim Tarihi:03.04.2025)

[326] Kişisel Verileri Koruma Kurulu, 03.08.2023 tarihli ve 2023/1327 sayılı Karar, https://www.kvkk.gov.tr/Icerik/7778/2023-1327. (E.T. 17.05.2025).

[327] Kişisel Verileri Koruma Kurulu, 27.08.2019 tarihli ve 2019/296 sayılı Karar, https://www.kvkk.gov.tr/Icerik/6557/2019-296, (E.T. 17.05.2025).

Özel nitelikli kişisel verilere ilişkin örnekler arasında biyometrik ve genetik verilerin kullanımı yer alır. Örneğin, bir şirket, giriş-çıkış güvenliğini artırmak amacıyla çalışanlarının yüz tanıma veya parmak izi sistemlerini kullanabilir[328]. Genetik veriler bağlamında ise bir sigorta şirketi, bireylerin genetik hastalık risklerini analiz ederek sigorta primlerini belirlemek isteyebilir. Ancak, KVKK'nın 6. maddesi gereğince bu tür hassas verilerin işlenmesi yalnızca açık rıza ile veya yasal zorunluluklar kapsamında mümkündür. Günlük işleyişte şirketler, lojistik süreçleri optimize etmek için araçlarını GPS ile takip edebilir, bu da şoförlerin konum bilgilerinin işlenmesini gerektirir. AVM'ler, iş yerleri ve fabrikalar güvenlik amacıyla kamera kayıtları alabilir, ancak bu kayıtların süresiz saklanmaması önemlidir. Pazarlama ve reklamcılık alanında ise şirketler, müşterilerinin iletişim bilgilerini ve alışveriş geçmişini kullanarak e-posta veya SMS yoluyla kampanyalar yürütebilir. Ancak KVKK kapsamında müşterilere istedikleri zaman pazarlama iletişimlerini durdurma hakkı sunulmalıdır. Ek olarak, eğitim sektöründe özel okullar ve üniversiteler, öğrencilerin akademik kayıtlarını, sınav sonuçlarını ve sağlık bilgilerini saklarken, insan kaynakları departmanları çalışanların performans değerlendirmelerini, devamsızlık kayıtlarını ve sağlık raporlarını saklayarak iş süreçlerini yönetmektedir. Tüm bu veri işleme faaliyetleri, KVKK'nın ilgili hükümlerine uygun olarak yürütülmeli ve özellikle açık rıza gerektiren durumlarda veri sahiplerinin bilgilendirilmesi sağlanmalıdır.

## 4. ANONİM ŞİRKETLERDE VERBİS KAYDI ve KİŞİSEL VERİ ENVANTERİ HAZIRLAMA YÜKÜMLÜLÜĞÜ

6698 sayılı Kişisel Verilerin Korunması Kanunu kapsamında anonim şirketlerin işledikleri kişisel verileri kategorilere ayırmaları ve bu veriler üzerinde sistematik bir kontrol sağlamaları, hukuki bir zorunluluk hâline gelmiştir. Bu bağlamda, kişisel veri envanteri oluşturulması ve Veri Sorumluları Sicili' ne (VERBİS) kayıt yükümlülüğü, şirketlerin hangi tür kişisel verileri işlediklerini, bu verilerin hangi amaçlarla kullanıldığını, kimlere aktarıldığını ve ne kadar süreyle muhafaza edildiğini açıkça belirlemelerini zorunlu kılmaktadır. Bu düzenlemeler hem şeffaflığın sağlanması hem de kişisel veri işleme faaliyetlerinin hukuka uygun yürütülmesi açısından kritik öneme sahiptir.

[328] Kişisel Verileri Koruma Kurulu, 27.02.2020 tarihli ve 2020/167 sayılı Karar, https://www.kvkk.gov.tr/Icerik/6738/2020-167, Kişisel Verileri Koruma Kurulu, 03.08.2023 tarihli ve 2023/1310 sayılı Karar, https://www.kvkk.gov.tr/Icerik/7775/2023-1310, (E.T. 17.05.2025).

Üst başlıkta açıkladığımız üzere anonim şirketlerin iş süreçleri çerçevesinde işledikleri kişisel veriler; çalışanlara ait verilerinden müşteri ve tedarikçi bilgilerine, pazarlama faaliyetlerine konu edilen tercihlerden dijital etkileşim verilerine kadar geniş bir yelpazeye yayılmaktadır. Bu verilerin hangi kategorilerde toplandığı ve işlendiği, yalnızca veri güvenliği ve uyum bakımından değil, aynı zamanda yasal bildirim yükümlülükleri açısından da belirleyici niteliktedir. Bu kapsamda, 6698 sayılı Kişisel Verilerin Korunması Kanunu ile getirilen en temel yükümlülüklerden biri olan Veri Sorumluları Sicili' ne kayıt zorunluluğu, anonim şirketler açısından sistematik bir sorumluluk alanı yaratmaktadır[329]. VERBİS'e kayıt, şirketlerin hangi kişisel verileri ne amaçla işlediklerini, kimlere aktardıklarını ve ne kadar süreyle sakladıklarını kamuoyuna ve denetim otoritelerine şeffaf şekilde beyan etmelerini sağlayan temel bir düzenlemedir. 6698 sayılı Kişisel Verilerin Korunması Kanunu'nun 16. maddesi uyarınca, kişisel veri işleyen gerçek ve tüzel kişilerin, veri işlemeye başlamadan önce Veri Sorumluları Sicili' ne kaydolmaları gerekmektedir. Bu yükümlülüğün temel amacı, veri sorumlularının kişisel veri işleme faaliyetlerini şeffaf ve denetlenebilir hale getirmektir. Kayıt sırasında, şirketlerin işledikleri kişisel verilerin kategorileri, işleme amaçları, verilerin saklanacağı süreler, aktarım yapılan alıcı grupları ve alınan güvenlik önlemleri gibi bilgiler sistematik şekilde beyan edilmek zorundadır[330]. Veri sorumluları, bu kayıt yükümlülüğünü KVKK tarafından belirlenen usul ve esaslara göre yerine getirmekle yükümlüdür. Anonim şirketler açısından VERBİS kaydı, yalnızca bir bildirim yükümlülüğü değil, aynı zamanda bir uyum göstergesi olarak değerlendirilmektedir. Bu kayıt, şirketin iç veri işleme politikalarının sistematik bir envanter ile desteklenmesini ve düzenli olarak güncellenmesini de gerektirir[331]. Ancak her veri sorumlusu VERBİS'e kayıt yükümlülüğü altında değildir. Kişisel Verileri Koruma Kurulu'nun aldığı karar doğrultusunda; yıllık çalışan sayısı 50'nin altında ve yıllık mali bilanço toplamı 25 milyon TL'nin altında olan veri sorumluları, eğer ana faaliyet konusu özel nitelikli kişisel veri işlemek değilse, VERBİS'e kayıt yükümlülüğünden muaf tutulmuştur[332]. Özel nitelikli kişisel veri işleyen veri sorumlularının, faaliyet alanları ve işledikleri veri türüne bakılmaksızın, Veri Sorumluları Siciline kaydolmaları zorunludur. Örneğin, sağlık verisi işleyen bir sigorta şirketi bu kapsamda VERBİS'e kayıt yükümlülüğüne

[329] Kişisel Verilerin Korunması Kanunu, m. 16.
[330] Kişisel Verilerin Korunması Kanunu, 6698 s., md. 16.
[331] Kişisel Verileri Koruma Kurumu, "Veri Sorumluları Sicil Bilgi Sistemi (VERBİS) Hakkında Sıkça Sorulan Sorular", https://www.kvkk.gov.tr/Icerik/5414/VERBIS-Sikca-Sorulan-Sorular, (Erişim Tarihi:25.04.2025)
[332] Kişisel Verileri Koruma Kurulu, 02.04.2018 tarihli ve 2018/87 sayılı Karar, https://www.kvkk.gov.tr/Icerik/5395/2018-87, (Erişim Tarihi:25.04.2025).

tabidir[333]. VERBİS'e kayıt süreci, şirketin veri sorumlusu veya yetkilendirilmiş bir temsilcisi tarafından gerçekleştirilir. Bu süreçte, işlenen kişisel verilere ilişkin kategoriler, saklama süreleri ve aktarım bilgileri gibi hususlar sisteme kaydedilir[334]. Bununla birlikte, kayıt yükümlülüğüne uymayan veri sorumluları hakkında Kanun'un 18. maddesi uyarınca idari para cezaları uygulanmaktadır. 2024 yılı itibarıyla VERBİS'e kayıt yükümlülüğüne aykırı hareket eden veri sorumluları hakkında 331.080 TL ile 6.621.633 TL arasında değişen idari para cezaları uygulanabilmektedir[335]. Bu durum, anonim şirketler açısından VERBİS kaydının sadece biçimsel değil, aynı zamanda ciddi sonuçları olan bir yasal yükümlülük olduğunu ortaya koymaktadır. VERBİS'e kayıt süreci, anonim şirketlerin kişisel verileri işleme süreçlerini düzenleyip şeffaflaştırmalarını sağlamak için kritik bir aşamadır. Kayıt işlemi, şirketlerin veri işleme faaliyetlerinin ne şekilde gerçekleştiğini, hangi tür verilerin işlendiğini ve bu verilerin güvenliğini sağlamak adına hangi tedbirlerin alındığını göstermektedir. Bu süreç, yalnızca yasal bir zorunluluk değil, aynı zamanda şirketlerin veri koruma bilincini geliştirmeleri açısından da önemlidir. Veri sorumluları, VERBİS üzerinden beyan ettikleri bilgilerin doğru ve güncel olması gerektiği gibi, bu bilgilerin düzenli olarak güncellenmesi de gerekmektedir[336]. Veri sorumlularının, kişisel veri işleme süreçlerinin şeffaflığını artırmak ve uyum süreçlerini kolaylaştırmak amacıyla doğru bir şekilde kayıt yapmaları büyük önem taşır. Özellikle kişisel verilerin yurt dışına aktarımı gibi önemli değişikliklerde, verilerin artık Türkiye'de barındırılacak olması ya da yeni bir aktarım rejiminin yürürlüğe girmesi durumunda VERBİS kayıtlarında gerekli güncellemelerin yapılması zorunludur. Bu bağlamda, yapılan değişikliklerin ve uygulamaya alındıkları tarihin ayrıntılı biçimde versiyonlanarak kaydedilmesi, yalnızca hukuki uyumun sağlanmasına değil, aynı zamanda şirketin kurumsal hafızasının korunmasına da hizmet etmektedir[337]. Böylece veri sorumluları, hem hesap verebilirlik ilkesini yerine getirmiş olmakta hem de olası denetim süreçlerine hazırlıklı hale gelmektedir. Ancak burada dikkate alınması gereken en önemli husus, kayıt işleminin sadece

---

[333] Kişisel Verileri Koruma Kurumu, "Veri Sorumluları Siciline (VERBİS) Kayıt ve Bildirim Yükümlülüğü," https://www.kvkk.gov.tr/Icerik/6598/Veri-Sorumlululari-Siciline-VERBIS-Kayit-ve-Bildirim-Yukumlulugu, (Erişim Tarihi: 17 Mayıs 2025).

[334] Sorularla Veri Sorumluları Sicil Bilgi Sistemi (VERBİS), https://verbis.kvkk.gov.tr/UploadedFiles/SORULARLA_VERBİS.pdf, (Erişim Tarihi:03.04.2025)

[335] Bknz. KVKK, Kamuoyu Duyurusu (Veri Sorumluları Sicili Hakkında) https://kvkk.gov.tr/Icerik/7980/KAMUOYU-DUYURUSU-Veri-Sorumlulari-Sicili-01082024, (Erişim Tarihi:03.04.2025).

[336] Zeynep Yürük, "Veri Sorumlusunun Veri Güvenliğine İlişkin İdari ve Teknik Tedbirleri Alma Yükümlülüğü", *İstanbul Ticaret Üniversitesi Sosyal Bilimler Dergisi*, C. 22, S. 48, 2023, s. 899-920, https://doi.org/10.46928/iticusbe.1218693, (E.T. 20.05.2025).

[337] Mehmet Bedi Kaya, "KVKK Reformu 2024 Değişiklikleri", Dijital Baskı v1.0- Mart 2024, s.75-76. https://mbkaya.com/hukuk/kvkk-reformu.pdf, (Erişim Tarihi:13.05.2025).

bir yükümlülük değil, bir işlevsel envanter oluşturma süreci olduğudur[338]. Veri işleme faaliyetlerini detaylı şekilde belgeleyen anonim şirketler, sadece yasal sorumluluklarını yerine getirmekle kalmaz, aynı zamanda veri güvenliği ve şirket içi denetim mekanizmalarını güçlendirmiş olurlar. Bu sayede olası veri ihlalleri veya güvenlik açıkları en aza indirgenebilir. Öte yandan, VERBİS kaydının yapılması sürecinde anonim şirketler, karşılaştıkları bazı zorluklarla da başa çıkmak zorundadır. Veri işleme faaliyetlerinin kapsamı ve türü çok geniş olan büyük ölçekli anonim şirketler, veri envanterlerini doğru şekilde oluşturma konusunda daha fazla zorlukla karşılaşabilmektedirler. Özellikle çok sayıda farklı departman ve şube ile faaliyet gösteren şirketlerde, her bir veri işleme faaliyetinin kayıtlara doğru bir şekilde yansıması karmaşıklaşabilir. Bu sebeple, şirketlerin veri sorumlusu sıfatıyla kayıt yükümlülüğünü yerine getirirken, veri koruma görevlisi (DPO) atanması ve şirket içindeki veri işleme süreçlerinin sistematik olarak izlenmesi, uyum sürecinin verimli şekilde yönetilmesini sağlayabilir[339]. Ayrıca, VERBİS kaydının yalnızca başlangıçtaki bir yükümlülük değil, sürekli bir güncellenme süreci olduğuna da dikkat edilmelidir. Şirketler, veri işleme faaliyetlerinde herhangi bir değişiklik meydana geldiğinde, bu değişiklikleri değişikliğin gerçekleştiği tarihten itibaren yedi gün içinde VERBİS üzerinden bildirmekle yükümlüdür[340]. Bu, veri güvenliği açısından kritik bir adımdır çünkü kişisel verilerin işlenmesi, transferi veya saklanmasında meydana gelen herhangi bir değişiklik, yeni riskler doğurabilir. Veri sorumlularının bu tür değişiklikleri düzenli olarak bildirmemesi hem yasal yaptırımların hem de güvenlik açıklarının önünü açabilir. Son olarak, VERBİS'e kaydın ihmal edilmesi, yalnızca cezai sorumlulukları değil, aynı zamanda şirketin itibarını da zedeleyebilir. Kamuoyu nezdinde kişisel verilerin korunmasına dair şeffaflık ve sorumluluk anlayışının yerleşmesi, şirketlerin marka değerini ve müşteri güvenini de doğrudan etkileyen faktörlerdir. Kişisel veri ihlallerinin ve yetersiz uyum süreçlerinin olumsuz etkileri, özellikle müşteri ilişkileri ve şirket imajı açısından uzun vadeli olumsuz sonuçlar doğurabilir. Buna paralel olarak, veri envanteri oluşturulması da anonim şirketlerin, sahip oldukları veri varlıklarını doğru kategorilere ayırarak işleme faaliyetlerini kayıt altına almalarını ve KVKK'ya uyum süreçlerini sistematik hâle getirmelerini zorunlu

[338] Kişisel Verileri Koruma Kurumu, "VERBİS Kayıt ve Güncelleme Yükümlülüğü," https://www.kvkk.gov.tr/Icerik/6598/Veri-Sorumlululari-Siciline-VERBIS-Kayit-ve-Bildirim-Yukumlulugu, (Erişim Tarihi: 17 Mayıs 2025).

[339] Kişisel Verileri Koruma Kurumu, "Veri Koruma Görevlisi (DPO) Rehberi," https://www.kvkk.gov.tr/Icerik/6597/Veri-Koruma-Gorevlisi-DPO, (Erişim Tarihi: 17 Mayıs 2025).

[340] Veri Sorumluları Sicili Hakkında Yönetmelik, m. 13, RG: 30.12.2017, Sayı: 30286; Sorularla Veri Sorumluları Sicil Bilgi Sistemi (VERBİS) https://verbis.kvkk.gov.tr/UploadedFiles/SORULARLA_VERBİS.pdf, soru:52, sayfa:22.

kılmaktadır[341]. Bu nedenle, kişisel verilerin işlenmesine ilişkin kategori bazlı analizler yalnızca operasyonel yönetim açısından değil, aynı zamanda yasal yükümlülüklerin eksiksiz yerine getirilmesi açısından da kritik bir öneme sahiptir. Bu bağlamda, Veri Sorumluları Sicili Hakkında Yönetmelik'in 5. maddesinin 1. fıkrasının (ç) bendi uyarınca, VERBİS'e kayıt yükümlülüğü bulunan veri sorumluları, kişisel veri işleme envanteri oluşturma zorunluluğuna sahiptir[342]. Bu envanter, şirketlerin veri işleme faaliyetlerini sistematik şekilde belgelerken, aynı zamanda GDPR ve KVKK'ya uyumu sağlamak adına önemli bir adımdır. Ayrıca, veri sorumlularının kişisel veri işleme faaliyetlerini şeffaf bir şekilde ortaya koymasını sağlar ve hem denetim hem de yasal uyumluluk açısından büyük önem taşır. Kişisel veri işleme envanterinin içeriğinde, bu verilerin işlenme amaçları, verilerin hangi süreçlerde ve nasıl işlendiği, veri aktarımı yapılan alıcı grupları ile alınan teknik ve idari güvenlik tedbirlerine ilişkin bilgilere yer verilmesi gerekmektedir[343]. Kişisel veri işleme envanterinin oluşturulması, veri sorumlularının veri işleme faaliyetlerini daha etkin bir şekilde yönetmesine ve kişisel verilerin korunması konusunda hukuki yükümlülüklerini yerine getirmelerine yardımcı olur. VERBİS başvuru süreci sırasında sağlanacak bilgiler, bu envantere uygun olacak şekilde sunulacaktır. Aynı maddenin 1/d fıkrasına göre, KVKK'nın 10. maddesinde veri sorumlularına yüklenen kişisel verileri toplarken ilgili kişilere verilerin hangi amaçla işleneceği, hangi verilerin toplanacağı, verilerin kimlerle paylaşılacağı gibi hususlarda aydınlatma yükümlülüğü taşıması, 13. maddede belirtilen ilgili kişinin kişisel verilerin doğruluğunu kontrol etme, silinmesi veya düzeltilmesi talepleri gibi isteklerinin belirtildiği başvurularına verilen yanıtlar ve ilgili kişilerin açık rızalarının kapsamı, kişisel veri işleme envanterine dayalı olarak VERBİS'e bildirilen ve burada yayımlanan bilgiler doğrultusunda şekillenir ve veri sorumlularının yasal yükümlülüklerini daha da ayrıntılı hale getirir[344]. Envanterde, başvuru usulleri, süreçler ve süreler detaylı şekilde belirtilmelidir[345].

Bununla birlikte, kişisel veri kategorilerinin tespit edilmesi ve işleme faaliyetlerinin sistematik hâle getirilmesi yalnızca VERBİS kaydıyla sınırlı olmayıp; anonim şirketlerin veri koruma yükümlülüklerini yerine getirebilmeleri için çeşitli politika ve dokümanlar da hazırlamaları

[341] Abdülhamid Zor, *Veri Sorumlusunun Yükümlülükleri ve Bu Yükümlülükleri İhlalinden Doğan Özel Hukuk Sorumluluğu*, On İki Levha Yayıncılık, İstanbul 2020, s.120-121.
[342] Kişisel Verileri Koruma Kurulu, Karar No: 2020/966, Tarih: 27.10.2020. Erişim Adresi: https://www.kvkk.gov.tr/Icerik/6935/2020-Yili-Kurul-Kararlari, (Erişim Tarihi: 17 Mayıs 2025).
[343] Veri Sorumluları Sicili Hakkında Yönetmelik, RG: 30.12.2017, Sayı: 30286, m. 5.
[344] Çekin, *op. cit.* s.165.
[345] Kişisel Verileri Koruma Kurumu, "Kişisel Veri İşleme Envanteri Hazırlama Rehberi", Erişim Adresi: https://www.kvkk.gov.tr/Icerik/6673/Kisisel-Veri-Isleme-Envanteri-Hazirlama-Rehberi, (E.T.: 17.05.2025).

gerekmektedir. Bu doğrultuda, Kişisel Veri Saklama ve İmha Politikası[346], Kişisel Veri Koruma Politikası[347], Aydınlatma Metni[348], Açık Rıza Metinleri[349], Veri İşleme Envanteri[350] ve Veri İhlali Yönetim Planı gibi belgelerin hazırlanması gerekmektedir[351]. Bu belgeler, hem şirket içi veri işleme faaliyetlerinin sistemli yürütülmesini sağlamakta hem de olası bir veri ihlali veya denetim durumunda anonim şirketlerin hukuki sorumluluklarını yerine getirdiklerini ortaya koyan temel araçlar olarak işlev görmektedir. Bu yükümlülüklere uyulmaması durumunda, idari para cezası uygulanabileceği gibi, ciddi ihlallerde faaliyetin durdurulması gibi yaptırımlar da söz konusu olabilmektedir[352]. Bu nedenle, anonim şirketlerin KVKK'ya uyum süreçlerini eksiksiz bir şekilde tamamlamaları büyük önem taşımaktadır.

Sonuç olarak, anonim şirketler tarafından işlenen kişisel veriler, şirketin faaliyet gösterdiği sektöre ve sunduğu hizmetlere bağlı olarak değişiklik göstermektedir. Bu verilerin işlenmesi sürecinde, anonim şirketlerin KVKK'nın 5. ve 6. maddelerinde belirtilen işleme şartlarına uygun hareket etmesi gerekmektedir. Özellikle özel nitelikli kişisel verilerin işlenmesi söz konusu olduğunda, Kanun'un öngördüğü ilkelere ve ilgili rehberlerde belirtilen teknik ve idari tedbirlere riayet edilmesi zorunludur. Bununla birlikte, kişisel verilerin işlenmesi ve saklanması süreçlerinde şeffaflık, veri güvenliği ve müşteri haklarının korunması temel ilkeler olarak benimsenmelidir. Bu bağlamda, kişisel veri işleme faaliyetlerinin hukuki dayanağının belirlenmesi, gerekli aydınlatma yükümlülüklerinin yerine getirilmesi ve veri güvenliği tedbirlerinin sağlanması, anonim şirketlerin hem yasal uyumluluğunu hem de veri sahiplerinin haklarının korunmasını temin etmektedir. Bu nedenle, KVKK ve ilgili ikincil mevzuat hükümlerine uyumlu hareket edilmesi, hem veri sahiplerinin haklarının korunmasını

[346]Kişisel Verileri Koruma Kurumu, Kişisel Veri Saklama ve İmha Politikası, https://www.kvkk.gov.tr/Icerik/5386/KVKK-KISISEL-VERI-SAKLAMA-ve-IMHA-POLITIKASI, (E.T.: 17.05.2025).

[347] Örneğin, bknz. https://www.mavicompany.com/i/assets/documents/Kisisel_Veri_Koruma_Politikası_22.pdf, (E.T.: 17.05.2025).

[348] Örneğin, bknz. https://www.turkishairlines.com/tr-tr/yasal-uyari/veri-koruma-aydinlatma-metni/, (E.T.: 17.05.2025).

[349] Örneğin, bknz., https://kvkk.subu.edu.tr/tr/acik-riza-formu, (E.T.: 17.05.2025).

[350]Kişisel Verileri Koruma Kurumu, "Kişisel Veri İşleme Envanteri Örneği", https://kvkk.gov.tr/SharedFolderServer/CMSFiles/b5fe209d-3c12-4c70-8dac-a2eaa5742ae6.xlsx, (E.T.: 17.05.2025).

[351] Kişisel Verileri Koruma Kurumu, "Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi Hakkında Rehber", https://www.kvkk.gov.tr/Icerik/6649/Kisisel-Verilerin-Silinmesi-Yok-Edilmesi-veya-Anonim-Hale-Getirilmesi-Hakkinda-Rehber, (E.T.: 17.05.2025).

[352] Kişisel Verilerin Korunması Kanunu, Kanun No: 6698, Kabul Tarihi: 24.03.2016, RG: 07.04.2016, Sayı: 29677, m. 18.

sağlamakta hem de şirketlerin hukuki ve cezai yaptırımlarla karşılaşmasının önüne geçmektedir.

## II. STANDART SÖZLEŞMELERİN ANONİM ŞİRKETLER TARAFINDAN UYGULANMASI

Veri sorumluluğu ve kişisel verilerin korunmasına yönelik yükümlülüklerin, anonim şirketlerin faaliyetlerini doğrudan etkilediği bir dönemde, standart sözleşmeler, yurt dışına veri aktarımını güvence altına almak için kritik bir mekanizma haline gelmiştir. Kişisel Verilerin Korunması Kanunu'nun 9. maddesinde yapılan düzenlemelerle birlikte, anonim şirketlerin veri aktarım süreçlerinde uyum sağlamak amacıyla kullanmaları gereken sözleşmesel araçlar daha belirginleşmiştir. Bu bölümde, anonim şirketlerin, yurt dışına veri aktarımı için hangi koşullar altında standart sözleşmeler uygulamak zorunda oldukları ve bu sözleşmelerin hukuki dayanakları ele alınacaktır.

### A. Standart Sözleşmelerin İçeriği ve Kapsamı

6698 sayılı Kişisel Verilerin Korunması Kanunu'nun 9. maddesinde yapılan son değişiklikler, kişisel verilerin yurt dışına aktarımına ilişkin hukuki altyapıyı köklü bir şekilde değiştirmiş ve "standart sözleşmeler" mekanizmasını merkezî bir konuma yerleştirmiştir. Bu düzenleme, özellikle anonim şirketlerin kişisel veri aktarım süreçlerini doğrudan etkileyerek hem hukuki hem idari hem de cezai sorumluluklar doğuran bir dizi yeni yükümlülük getirmiştir. KVKK'nın değişen 9. maddesi, yurt dışına veri aktarımında açık rızayı istisnai bir yöntem olarak belirlemiş; yeterlilik kararı ve uygun güvenceler çerçevesinde aktarımı esas hale getirmiştir[353]. Bu uygun güvenceler arasında standart sözleşmeler önemli bir yer tutmakta; bu sözleşmelere dayanarak yapılacak aktarımlarda KVK Kurulu'ndan önceden izin alınması gerekmemekte, yalnızca Kurul'a bildirimde bulunulması yeterli olmaktadır[354]. Anonim şirketlerin, yurt dışına veri aktarımı sürecinde KVKK'ya uygun hareket edebilmesi için standart sözleşmeler önemli ve işlevsel bir hukuki araç olarak öne çıkmaktadır. Bu sözleşmeler, veri alıcısına kişisel verilerin güvenliğine ilişkin açık yükümlülükler yüklemekte; veri sorumlusunun ise veri alıcısının bu yükümlülüklere uygun hareket edip etmediğini denetleyebilmesini mümkün

[353] Mehmet Bedi Kaya, "KVKK Reformu 2024 Değişiklikleri", Dijital Baskı v1.0- Mart 2024, s.75-76. https://mbkaya.com/hukuk/kvkk-reformu.pdf, (Erişim Tarihi:13.05.2025).
[354] Kişisel Verileri Koruma Kurumu, "6698 Sayılı Kişisel Verilerin Korunması Kanunu 9. Madde Değişiklikleri", Resmî Gazete, 12.03.2024.

kılmaktadır[355]. Standart sözleşmeler kapsamında; aktarılacak verilerin hangi amaçlarla ve hangi sınırlar dahilinde işleneceği açıkça belirlenmeli, verilerin korunması için alınacak teknik ve idari tedbirler detaylandırılmalı, veri sorumlusuna denetim yetkisi tanınmalı ve olası bir veri ihlali durumunda tarafların yükümlülükleri ile başvurulacak mekanizmalar önceden düzenlenmelidir. Bu uygulama, anonim şirketlerin süreklilik arz eden uluslararası ticari ilişkilerinde operasyonel esneklik sağlarken, beraberinde belirli sorumluluklar[356] da getirmektedir[357]. Standart sözleşmeler, veri aktarımının güvenliğini temin etmek için veri sorumlularının yasal sorumluluklarını yerine getirmeleri adına önemli bir araçtır. Standart sözleşmelerin kullanımının temel avantajı, kişisel verilerin korunmasına ilişkin temel ilkelerin hem veri sorumlusu hem de veri alıcısı tarafından önceden kabul edilmesini sağlamasıdır. Bu sözleşmeler, veri alıcılarının yurt dışındaki yasal yükümlülüklerini yerine getirmesini temin ederken, veri aktarım sürecinde güvenliğin sağlanmasına da katkı sunar. Yurt dışına veri aktarımı yapan anonim şirketler, veri alıcıları ile imzalanacak bu sözleşmeler aracılığıyla veri güvenliğini temin edebilir, veri sahibinin haklarını ihlal etmeden işlemi gerçekleştirebilirler[358]. Özellikle Avrupa Ekonomik Alanı (EEA) dışındaki ülkelere yapılan veri aktarımında, bu tür sözleşmelerin hukuki geçerliliği büyük bir öneme sahiptir[359]. Standart sözleşmelerin kullanımı, veri koruma ilkelerinin her iki tarafça kabul edilmesini sağlar ve özellikle veri alıcılarının yükümlülüklerini somutlaştırır. Yurt dışına kişisel veri aktarımı yapan anonim şirketlerin, bu tür standart sözleşmeleri kullanarak, sadece yasal yükümlülüklerini yerine getirmekle kalmaz, aynı zamanda veri sahiplerinin gizliliğini ve güvenliğini sağlamaya yönelik sorumluluklarını

[355] Kişisel Verileri Koruma Kurumu, "Yurt Dışına Kişisel Veri Aktarımında Standart Sözleşme Metni ve Taahhütname Uygulaması Hakkında Kamuoyu Duyurusu", E.T.: 10.07.2023, Erişim: https://www.kvkk.gov.tr/Icerik/7285/Yurt-Disina-Kisisel-Veri-Aktarimi.

[356] Bu sorumluluklar aşağıdaki gibidir;
Veri güvenliğine ilişkin önlemleri alma yükümlülüğü: Aktarılan verilerin güvenliğini sağlamak amacıyla teknik ve idari tedbirlerin standart sözleşmede açık şekilde yer alması gerekir.
Veri ihlali bildirim yükümlülüğü: Yurt dışındaki veri alıcısının bir ihlal durumunda derhal veri sorumlusunu haberdar etmesi ve gerekli müdahaleyi sağlaması beklenir.
Veri işleme faaliyetlerinin denetlenmesi: Veri sorumlusu, veri alıcısının işlemelerini belirli aralıklarla gözden geçirme ve denetleme hakkına sahiptir.
Amaçla sınırlılık ilkesine riayet: Verilerin sadece belirlenen amaçlarla işlenmesi; başka bir amaçla kullanılması veya üçüncü taraflarla paylaşılmasının yasaklanması gerekir.
Yükümlülüklerin sözleşmesel bağlayıcılığı: Taraflar, bu sözleşmesel yükümlülükleri ihlal ettiklerinde hukuki sorumlulukla karşı karşıya kalabilir.

[357] Kişisel Verileri Koruma Kurumu, "Yurt Dışına Kişisel Veri Aktarımında Standart Sözleşme Metni ve Taahhütname Uygulaması Hakkında Kamuoyu Duyurusu", 10 Temmuz 2023, https://www.kvkk.gov.tr/Icerik/7285/Yurt-Disina-Kisisel-Veri-Aktarimi, (E.T.: 16.05.2025).

[358] Kişisel Verileri Koruma Kurumu, "Yurt Dışına Kişisel Veri Aktarımında Standart Sözleşme Metni ve Taahhütname Uygulaması Hakkında Kamuoyu Duyurusu", 10 Temmuz 2023, https://www.kvkk.gov.tr/Icerik/7285/Yurt-Disina-Kisisel-Veri-Aktarimi, (E.T.: 16.05.2025).

[359] Kişisel Verilerin Korunması Kanunu, 6698 s., md. 9; Avrupa Birliği Genel Veri Koruma Tüzüğü (GDPR), 2016/679, md. 46.

yerine getirmiş olurlar. Bu bağlamda, anonim şirketlerin veri koruma mekanizmalarını güçlendirmeleri, yalnızca hukuki uyumu değil, aynı zamanda kurumsal itibarlarını da olumlu yönde etkileyebilir. Standart sözleşmeler aracılığıyla gerçekleştirilecek yurt dışı veri aktarımlarında, özellikle aktarılan verilerin işlenme amacı, aktarımın kapsamı ve süresi gibi hususlar açık ve net bir şekilde belirtilmelidir[360]. Veri aktarımının amacı, yalnızca anonim şirketlerin ticari faaliyetlerini sürdürmesi için gerekli olan bir işlem değil, aynı zamanda belirli bir hizmetin sağlanması veya yükümlülüklerin yerine getirilmesi amacıyla da gerekli olabilir[361]. İlgili kişilere, kişisel verilerinin hangi güvencelerle korunduğu hakkında bilgi verilmesi, açık rızaya dayanmayan aktarımlar açısından da önem arz etmektedir. Veri alıcısının yükümlülükleri, veri güvenliğini sağlama, verinin yalnızca belirlenen amaçlarla işlenmesi ve korunması adına gerekli teknik ve idari tedbirlerin alınmasını içerir[362]. Sözleşme, veri alıcısının ayrıca veri sahibinin haklarına saygı göstermesi, veri ihlali durumunda gereken bildirimleri yapması ve şeffaflık ilkesine uyması gerektiğini belirten hükümler de içermelidir. Verilerin güvenliği, yurt dışına veri aktarımını gerçekleştiren anonim şirketlerin en önemli sorumluluklarından biridir. Bu nedenle, sözleşmelerde veri güvenliğini sağlayacak tedbirler, verinin kaybolmasını, yetkisiz erişimini ve başka şekilde ihlal edilmesini engellemek amacıyla belirlenmelidir[363]. Ayrıca, veri ihlali durumunda yapılacak bildirimler ve düzeltici tedbirler de sözleşme hükümlerinde yer almalıdır[364]. Standart sözleşmelerde veri sahibinin haklarının korunması da önemlidir. Veri sahiplerine, erişim, düzeltme, silme, kısıtlama ve veri taşınabilirliği gibi haklar tanınır ve bu hakların nasıl kullanılacağı sözleşme çerçevesinde belirtilmelidir. Ayrıca, verilerin saklanma süresi de net bir şekilde sözleşmeye dahil edilmelidir[365]. Veri saklama süresi sona erdiğinde verilerin nasıl imha edileceği veya anonimleştirileceği de belirtilmelidir[366]. Veri ihlali durumunda yapılacak işlemler, sözleşme

---

[360] Kişisel Verileri Koruma Kurulu, *Yurt Dışına Veri Aktarımı Rehberi*, 09 Mayıs 2024, *https://www.kvkk.gov.tr/Icerik/6696/Yurt-Disina-Veri-Aktarimi-Rehberi*, (E.T.: 18 Mayıs 2025).

[361] Kişisel Verileri Koruma Kurulu, "Yurt Dışına Veri Aktarımı Süreçlerinde Standart Sözleşmelerin Kullanımı Hakkında Kamuoyu Duyurusu", 7.2.2024, Erişim: *https://www.kvkk.gov.tr/Icerik/8197/Standart-Sozlesmeler-Hakkinda-Kamuoyu-Duyurusu*, (E.T.: 18.05.2025).

[362] Kişisel Verileri Korumu Kurulu, "Kişisel Verilerin Korunması Kanunu ve Uygulaması", s. 48, *https://www.kvkk.gov.tr/yayinlar/K%C4%B0%C5%9E%C4%B0SEL%20VER%C4%B0LER%C4%B0N%20KORUNMASI%20KANUNU%20VE%20UYGULAMASI.pdf* , (E.T.: 18.05.2025), GDPR m.32.

[363] Kişisel Verileri Koruma Kurulu, Kişisel Veri Güvenliği Rehberi (Teknik ve İdari Tedbirler), Ankara, KVKK Yayınları, Ocak 2018, s. 39-40, *https://www.kvkk.gov.tr/yayinlar/veri_guvenligi_rehberi.pdf*, (E.T.: 18.05.2025).

[364]Kişisel Verileri Koruma Kurulu, Veri İhlali Bildirim Formu, *https://www.kvkk.gov.tr/SharedFolderServer/CMSFiles/8217d07e-5af7-43f0-ad02-a48cb1e23cd7.pdf*, (E.T.: 18.05.2025).

[365] Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi Hakkında Yönetmelik, madde 7/3, *https://www.mevzuat.gov.tr/mevzuat?MevzuatNo=24038&MevzuatTur=7&MevzuatTertip=5*, (E.T.: 18.05.2025).

[366] Kişisel Verileri Koruma Kurulu, Kişisel Verilerin Silinmesi, Yok Edilmesi

kapsamında açıkça düzenlenmeli, ihlal durumunda yapılacak bildirimler ve düzeltici işlemler belirlenmelidir[367].

Çift yönlü veri aktarımı, yurt dışına veri gönderilirken, aynı zamanda yurt dışından alınan verilerin de korunması için geçerli olacak standart sözleşmelerin oluşturulmasını gerektirir. Anonim şirketler, yurt dışındaki veri alıcılarının verilerini alırken de bu yükümlülükleri yerine getiren sözleşmeler imzalamalıdır. Ayrıca, uluslararası düzeyde uyum sağlamak adına, GDPR gibi düzenlemelere uygun sözleşmeler yapılmalıdır. Anonim şirketler, veri güvenliği ve kişisel veri koruma süreçlerinde karşılaştıkları zorlukları aşmak adına bu sözleşmelerin içeriğini doğru şekilde düzenlemeli, veri alıcılarının yükümlülüklerini belirlemeli ve veri güvenliği ile ilgili tedbirleri şeffaf bir şekilde açıklamalıdır. Aydınlatma metinleri, ilgili kişilerin kolayca anlayabileceği bir dilde ve formatta hazırlanmalıdır[368]. Özellikle yabancı dilde sözleşmeler imzalandığında, Türkçe metnin esas alınarak bilgilendirme yapılması gerekir[369]. Aydınlatma yükümlülüğünün eksik veya hiç yerine getirilmemesi, KVKK'ya aykırılık teşkil etmekte ve veri sorumlusu hakkında idari yaptırımlara sebebiyet verebilmektedir[370].

Bu bağlamda, KVKK'nın değişen 9. maddesi, veri aktarımına dair düzenlemeler açısından önemli bir evrim geçirmiştir ve bu değişiklik, Avrupa Birliği Genel Veri Koruma Tüzüğü'nün 5. Bölümü ile büyük ölçüde uyumlu hale getirilmiştir[371]. Özellikle GDPR'da yer alan "Standard

---

Veya Anonim Hale Getirilmesi Rehberi, *https://www.kvkk.gov.tr/SharedFolderServer/CMSFiles/bc1cb353-ef85-4e58-bb99-3bba31258508.pdf*, (E.T.: 18.05.2025).

[367] Bknz. Kişisel Verilerin Yurt Dışına Aktarılmasında Kullanılacak Standart Sözleşme – 2, (Veri Sorumlusundan Veri İşleyene) tarafların yükümlülükleri m.7, https://www.kvkk.gov.tr/Icerik/7931/Kisisel-Verilerin-Yurt-Disina-Aktarilmasinda-Kullanilacak-Standart-Sozlesme-2-Veri-Sorumlusundan-Veri-Isleyene- (E.T.: 18.05.2025).

[368] Aydınlatma Yükümlülüğünün Yerine Getirilmesinde Uyulacak Usul ve Esaslar Hakkında Tebliğ, Resmî Gazete, 10.03.2018, Sayı: 30356.

[369] KVK Kurulu, *"Yurt Dışına Veri Aktarımı ve Aydınlatma Yükümlülüğü Hakkında Duyuru"*, 2024.

[370] Kişisel Verileri Koruma Kurulu, "Veri sorumlusu ve veri işleyenin tespitinde göz önünde bulundurulması gereken hususlar ile aydınlatma yükümlülüğünün kim tarafından yerine getirileceği" ne ilişkin 30/01/2020 tarihli ve 2020/71 sayılı Karar Özeti, veri sorumlusu ve veri işleyenin tespiti ile aydınlatma yükümlülüğünün kim tarafından yerine getirileceği konularında önemli açıklamalar içermektedir. Bu karara göre:
Veri Sorumlusu: Kişisel verilerin işlenme amaç ve vasıtalarını belirleyen gerçek veya tüzel kişidir. Veri sorumlusu, veri işleme faaliyetlerinin planlanması ve yürütülmesinden sorumludur.
Veri İşleyen: Veri sorumlusunun verdiği yetkiye dayanarak onun adına kişisel verileri işleyen gerçek veya tüzel kişidir. Veri işleyen, veri sorumlusunun talimatları doğrultusunda hareket eder ve kendi başına veri işleme amacı belirleyemez.
6698 sayılı Kişisel Verilerin Korunması Kanunu'nun 10. maddesi uyarınca, aydınlatma yükümlülüğü veri sorumlusuna aittir. Veri işleyen, veri sorumlusunun talimatları doğrultusunda hareket ettiğinden, aydınlatma yükümlülüğü doğrudan veri işleyene ait değildir.
Bu karar, veri sorumlusu ve veri işleyenin rollerinin net bir şekilde belirlenmesi ve aydınlatma yükümlülüğünün doğru kişi tarafından yerine getirilmesi açısından rehber niteliğindedir. https://www.kvkk.gov.tr/Icerik/6783/Karar-Ozetleri-2020, (Erişim Tarihi: 19.05.2025).

[371] Mehmet Bedi Kaya, "KVKK Reformu 2024 Değişiklikleri", Dijital Baskı v1.0- Mart 2024, s.1-7. https://mbkaya.com/hukuk/kvkk-reformu.pdf

Contractual Clauses" (SCC) örnek alınarak Türkiye'deki standart sözleşmeler geliştirilmiştir. Ancak Türkiye'deki metinlerin AB'deki modal clauselara yeterince yakın olmaması, uygulamada bazı zorluklara neden olabilmektedir. Bu nedenle AB ile daha paralel bir yapı kurulması önem arz etmektedir. Amerika Birleşik Devletleri ile karşılaştırıldığında ise Türkiye'nin standart sözleşme yaklaşımı daha şekli ve katı kurallar içermektedir. Özellikle imza prosedürlerinin fiziki ortamda veya Kayıtlı Elektronik Posta (KEP) yoluyla gerçekleştirilmesi ile Kurul'a beş iş günü içinde bildirim zorunluluğu gibi düzenlemeler[372], Türkiye uygulamasını daha şekli ve katı bir yapıya kavuşturmakta; bu yönleriyle AB düzenlemelerinden ayrışmaktadır[373]. Sözleşmelerin çok farklılaşması hâlinde, 9. maddenin işlevselliği zayıflayabilir. Bu noktada, standart sözleşmelerin farklılaşmasının yaratabileceği hukuki belirsizlikler, özellikle çok uluslu şirketler açısından veri aktarımı süreçlerinde çeşitli ülkelerdeki farklı mevzuatlarla uyum sağlama zorunluluğu da getirmektedir. Bu bağlamda çok uluslu şirketlerin grup içi veri aktarımlarına yönelik uygulamaları, zaman içinde evrilmiş ve daha önce kullanılan detaylı sözleşme belgeleri, yeni düzenlemelerle birlikte daha basitleştirilmiş bir yapıya kavuşturulmuştur. Yeni sistemle birlikte, bu belgeler "grup içi standart sözleşme" formuna dönüştürülerek operasyonel kolaylık sağlanmıştır. Yeni sistemin getirdiği önemli bir değişiklik, KVKK kapsamında grup içi veri aktarımında yalnızca bildirim yükümlülüğü getirilmesi ve Kurul izni gerekliliğinin ortadan kaldırılmasıdır[374]. Bu gelişme, çok uluslu şirketlerin veri aktarım süreçlerini daha hızlı ve etkili bir şekilde yönetebilmelerine olanak sağlamıştır. Ancak, aynı zamanda bu tür veri aktarımlarının başka ülkelere yapılması durumunda, özellikle üçüncü ülkelerdeki veri koruma mevzuatları ve onward transfer (sonraki aktarımlar) ile ilgili denetim süreçlerinin henüz olgunlaşmadığı görülmektedir. Bu nedenle, Kurul'un denetim kapasitesinin sınırlı olması nedeniyle, sonraki aktarımlara ilişkin zaman zaman bildirim yapılmaması gibi uygulamalara rastlanabilmektedir. Grup içi veri aktarımları ve veri sorumlusu-veri işleyen ilişkileri açısından ise, veri işleyen sıfatıyla hareket eden şirketlerin hem yerel mevzuatlara hem de uluslararası düzenlemelere uyum sağlamak zorunda oldukları açıktır. Bu uyumun sağlanabilmesi için veri aktarımına ilişkin sözleşmelerde, özellikle veri alıcısı ve veri aktarıcısı arasında net bir sorumluluk paylaşımının yapılması

[372] Kişisel Verileri Koruma Kurulu, *"Standart Sözleşmelere İlişkin Usul ve Esaslar Hakkında Karar*", 15.02.2025 tarihli duyuru.
[373] Veri Koruma Derneği, "Data Privacy Türkiye KVKK Yurt Dışı Kişisel Veri Aktarımı Soru-Cevap Etkinliği", *YouTube*, 29 Eylül 2023, https://www.youtube.com/watch?v=k8KKAisrvgQ (Erişim: 17 Mayıs 2025).
[374] Bu konuyla ilgili görüşler için bknz. Mehmet Bedi Kaya, "KVKK Reformu 2024 Değişiklikleri", Dijital Baskı v1.0- Mart 2024, s.40-43. *https://mbkaya.com/hukuk/kvkk-reformu.pdf,* (Erişim Tarihi:13.05.2025).

gerekmektedir[375]. Yurt dışına veri aktarılan şirketlerin, yalnızca veri alıcısı olarak değil, aynı zamanda veri işleyen sıfatıyla da hareket edebileceği durumlar söz konusu olabilmektedir[376]. Bu nedenle, veri aktarımı sırasında dikkat edilmesi gereken en önemli husus, aktarılacak verinin hangi ülkede işleneceği ve o ülkedeki veri koruma yasalarına uygunluğunun sağlanmasıdır.

Grup şirketleri söz konusu olduğunda, genellikle iki önemli konu tartışılmaktadır. İlk olarak, yurt dışı ana şirketin veya yurt dışı kardeş şirketlerin Türkiye'deki iştirakleriyle veri paylaşması durumunda, bu ilişkide veri sorumluluğunun ve veri işleme sorumluluğunun nasıl tanımlanması gerektiği ortaya çıkmaktadır. Bu durumun daha iyi anlaşılabilmesi için, ilk olarak yurt dışındaki şirketin veri sorumlusu mu, yoksa veri işleyeni mi olarak hareket ettiğini tespit etmek gerekmektedir[377]. Yurt dışındaki şirketler genellikle ana şirketler veya altyapı sağlayıcıları, kendilerini veri sorumlusu olarak tanımlamazlar. Bunun yerine, GDPR gibi düzenlemelere uyarak, çoğu zaman veri işleyeni olarak konumlanmışlardır. Veri aktarılan yurt dışındaki ana şirket veya bağlı şirket, verileri veri sorumlusu olarak mı alıyor, yoksa veri işleyeni olarak mı alıyor, bu sorunun cevabının belirlenmesi kritik önem taşır.

Çok uluslu şirketlerin grup içindeki veri aktarımları açısından uygulamada görülen bir diğer önemli husus ise, yazılım sağlayıcıları ve altyapı hizmet sağlayıcıları ile yapılan sözleşmelerdir. Bu durumda, Türkiye'deki iştiraklerin, ana şirketin veya yurt dışındaki kardeş şirketlerin veri işleyeni sıfatıyla konumlandığı ve bu şirketlerin sunduğu altyapıların, Türkiye'deki iştirakler tarafından veri sorumlusu olarak kullanıldığı görülmektedir[378]. Bu tür yapıların, GDPR gibi uluslararası düzenlemelerle uyumlu olması, veri işleme ve aktarım süreçlerini şeffaf ve güvenli bir hale getirmektedir. Uygulamada, özellikle Türk iştirakleri için sıkça sorulan sorulardan biri, yurt dışındaki ana şirketin lisanslar alırken ve tedarikçilerle iş birliği yaparken, bu süreçte veri işleme faaliyetlerinin nasıl organize edileceğidir. Genellikle, ana şirket tarafından alınan lisanslar ve yurt dışındaki tedarikçilerle bağlantının olmaması gibi durumlar ortaya çıkmaktadır. Bu noktada, uygulamada karşılaşılan bazı çözüm önerileri mevcuttur. Örneğin,

---

[375] Mehmet Bedi Kaya, "KVKK Reformu 2024 Değişiklikleri", Dijital Baskı v1.0- Mart 2024, s.37. *https://mbkaya.com/hukuk/kvkk-reformu.pdf,* (Erişim Tarihi:15.05.2025).

[376]Kişisel Verileri Koruma Kurulu, "Veri Sorumlusu ve Veri İşleyen", s.4, https://www.kvkk.gov.tr/Icerik/4195/Veri-Sorumlusu-ve-Veri-Isleyen, (E.T. 21.05.2025).
Rehberde "Bir tüzel ya da gerçek kişinin aynı anda hem veri sorumlusu hem de veri işleyen olabileceği ifade edilmektedir. Örneğin, bir bulut bilişim hizmeti sunan şirket kendi çalışanlarının verileri bakımından "veri sorumlusu" iken, müşterilerinin verileri bakımından "veri işleyen" sıfatıyla hareket edebileceği ifade edilmiştir."

[377] Veri Koruma Derneği, "Data Privacy Türkiye KVKK Standart Sözleşme Atölyesi- Veri Koruma Derneği Platform Toplantısı Çıktıları", *YouTube*, 13 Şubat 2024, (Erişim: 17 Mayıs 2025), https://www.youtube.com/watch?v=K-zdTpx2l3E. (Konuşmacı: Av. Selen İbrahimoğlu Güreş, 45:00–60:00 dk.)

[378] *Ibid.*

Türkiye'deki grup şirketleri ve holding şirketleri, yurt dışındaki grup şirketlerine veya altyapı sağlayıcılarına veri işleme faaliyetlerinde kullanılacak teknik altyapıyı sağlamak üzere veri işleyeni olarak tanımlanabilir. Bu durumda, standart sözleşmeler çerçevesinde, veri işleyenler arasında sözleşmeler yapılır ve bu sözleşmelerde veri aktarımının kapsamı netleştirilir. Bir başka örnek de yurt dışında ana şirketi bulunan Türk iştirakinin veri işleme sorumluluğunu nasıl yerine getirdiğidir. Bu tür yapılarda, genellikle yurt dışındaki ana şirket veya seçilen kardeş şirket veri işleyeni olarak konumlanırken, Türkiye'deki iştirak veri sorumlusu olarak konumlandırılır. Bu durumda, veri aktarımı ve standart sözleşmeler üzerinden yapılan faaliyetlerde, yurt dışındaki veri işleyeni, veri aktarımını ve işleme faaliyetlerini düzenleyen sözleşmelere uyarak hizmet verir. Benzer bir uygulama, yazılım hizmetleri alanında faaliyet gösteren şirketlerde de görülmektedir. Bu çerçevede örnek olarak SAP Türkiye Yazılım Üretim ve Ticaret AŞ'nin uygulamasına değinmek mümkündür. SAP Türkiye, yurt dışındaki ana şirketi ile yaptığı sözleşme kapsamında, kendisini veri işleyen olarak konumlandırmış ve yurt dışındaki ana şirket ile sözleşme yaparak veri işleme faaliyetlerini yürütmüştür. Bu tür yazılım hizmetlerinde, verinin yurt dışına aktarılmasının takibi önemlidir, çünkü çoğu zaman, bu yazılımlar farklı modüller içerir ve her bir modülün veri işleme faaliyetleri farklı olabilir. Bu durumda, verinin yolculuğu ve sorumlulukları netleştirilmelidir.

Bir diğer önemli konu ise, grup içindeki veri aktarım sözleşmelerinde yer alan standart sözleşmelerin ek1'inin doldurulmasıdır. Sözleşmelerin eklerini doldururken dikkat edilmesi gereken önemli bir nokta da yurt dışına veri aktarılacak modüllerin ve yazılımların kapsamının doğru bir şekilde belirlenmesidir[379]. Sözleşme ekinde, veri işleme faaliyetlerinin amacı, kullanılan yazılımların modüllerinin nerelerde işlendiği, hangi tedarikçilerle iş birliği yapıldığı ve veri aktarımının detayları açıkça belirtilmelidir. Ancak burada dikkat edilmesi gereken bir diğer önemli konu ise, her yazılımın modüllerinin ilerleyen zamanlarda değişebileceği ve yeni modüllerle veri işleme faaliyetlerinin genişleyebileceğidir[380]. Bu nedenle, sözleşme eklerinde çok geniş bir detaylandırma yapmamak, sadece gerekli olan bilgilerin yer aldığı bir düzenleme yapmak daha sağlıklı olacaktır. Avrupa'daki uygulamalara baktığımızda, genellikle ana veri işleme sözleşmesinde, veri aktarımına ilişkin faaliyetlerin tüm detayları ve sorumluluklar yer almaktadır. Bu nedenle, Avrupa'daki veri sorumluları, bu sözleşmeye atıfta bulunarak veri

[379] Veri Koruma Derneği, "Data Privacy Türkiye KVKK Standart Sözleşme Atölyesi- Veri Koruma Derneği Platform Toplantısı Çıktıları", *YouTube*, 13 Şubat 2024, (Erişim: 17 Mayıs 2025), https://www.youtube.com/watch?v=K-zdTpx2l3E. (Konuşmacı: Av. Selen İbrahimoğlu Güreş, 50:00–57:00 dk.)

[380] Kişisel Verileri Koruma Kurumu, "Veri Sorumluları İçin Kişisel Veri İşleme Envanteri Hazırlama Rehberi", s. 9, https://www.kvkk.gov.tr/Icerik/6679/Kisisel-Veri-Isleme-Envanteri-Hazirlama-Rehberi (E.T. 21.05.2025).

aktarım faaliyetlerini düzenleyebilmektedir[381]. Ancak Türkiye'de bu durum biraz daha karmaşıktır, çünkü yurt dışına veri aktarımı ve veri işleyenler arasındaki sözleşmeler detaylandırılmadan önce her iki tarafın da yükümlülükleri açıkça belirtilmelidir. Bu kapsamda, özellikle çoklu sistemler kullanan grup şirketlerinde, her bir yazılım ve hizmetin ayrıntıları ile ilgili sözleşmeye ek yapılması gerektiği ortaya çıkmaktadır[382]. Bu, zaman zaman oldukça fazla detay ve ek belge gerektirebilir. Bu yüzden hem veri aktarılan tarafın hem de veri alıcısının yükümlülüklerinin açıkça belirlenmesi, ileride yaşanacak sorunları en aza indirecektir. Bu ekler, veri aktarımıyla ilgili faaliyetlerin amacını ve kapsamını belirleyerek, tarafların yükümlülüklerini net bir şekilde ortaya koymaktadır. Avrupa'daki uygulamalara bakıldığında, bu tür sözleşmelerin genellikle ana veri işleme sözleşmesine atıf yaparak, her iki tarafın da sorumluluklarını yerine getirmesini sağlayacak şekilde düzenlendiği görülmektedir[383]. Ancak Türkiye'deki uygulamalarda, bu sözleşmelerin detaylı bir şekilde doldurulması gerektiği, özellikle veri sorumlusu ve veri işleyeni arasındaki ilişkinin net bir şekilde tanımlanmasının önem taşıdığı vurgulanmaktadır[384].

Grup şirketleri ister yurt içi ister yurt dışı olsun, genellikle büyük hizmet sağlayıcılarıyla sözleşme yaparak bu hizmetlerden faydalanır. Bu hizmet sağlayıcıları arasında Microsoft gibi bulut bilişim servisleri de yer almaktadır. Grup şirketleri, bu hizmet sağlayıcılarıyla yaptıkları sözleşmelerle, hizmeti kullanırken kendi alt hesaplarını (sub accounts) oluşturabilirler. Bu durumda, verinin aktarımı ve takibi söz konusu olduğunda, grup şirketlerinin kullandığı bu hesaplar, sözleşme yapan ana şirketin altında yer alır. Teknik olarak holdingin alt hesaplara erişimi mevcut olduğundan, bu durum holdingin veri yönetimi ve gözetimi üzerinde doğrudan bir etkide bulunmaktadır. Bu tür organizasyonlarda, holding veri işleyen olarak tanımlanmaktadır; zira verilerin işlenmesi alt hesaplar aracılığıyla gerçekleştirilmekte ve holding, bu hesaplar üzerinde sahip olduğu erişim sayesinde işleme süreçlerinde aktif bir kontrol yetkisi kullanmaktadır. Dolayısıyla, holdingin hizmet aldığı firma, alt veri işleyen

[381] Avrupa Veri Koruma Kurulu (EDPB), *Guidelines 07/2020 on the concepts of controller and processor in the GDPR*, 2.0 versiyonu, 07.07.2021, s. 23-24, https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-072020-concepts-controller-and-processor_en, (E.T.:: 21.05.2025).
[382] Kişisel Verileri Koruma Kurumu, *Yurt Dışına Kişisel Veri Aktarımı Rehberi*, 2024, s. 14-15, https://www.kvkk.gov.tr/Icerik/8387/Yurt-Disina-Kisisel-Veri-Aktarimi-Rehberi, (E.T.: 21.05.2025).
[383] Avrupa Veri Koruma Kurulu (EDPB), *Guidelines 07/2020 on the concepts of controller and processor in the GDPR*, 2.0 versiyonu, 07.07.2021, s. 23-24, https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-072020-concepts-controller-and-processor_en, (E.T.: 21.05.2025).
[384] Veri Koruma Derneği, "Data Privacy Türkiye KVKK Standart Sözleşme Atölyesi- Veri Koruma Derneği Platform Toplantısı Çıktıları", *YouTube*, 13 Şubat 2024, (E.T.: 17 Mayıs 2025), https://www.youtube.com/watch?v=K-zdTpx2l3E. (Konuşmacı: Av. Selen İbrahimoğlu Güreş, 50:00–57:00 dk.)

olarak kabul edilir. Bu yaklaşım, özellikle grup şirketlerinin kullandığı yazılımlar ve sistemler için önemli bir düzenlemeyi işaret eder. Örneğin, Türkiye'deki bir grup şirketi, Microsoft ile yaptığı sözleşmede bu yapıyı kullanarak, veriyi ve sözleşme yükümlülüklerini takip etmiştir. Bu bağlamda, grup şirketlerinin özellikle alt hesap kullandığı durumlarda, veri işleme süreçlerinin daha şeffaf ve yönetilebilir hale gelmesi sağlanmaktadır. Bu tür yapılar, veri işleme sorumluluklarının daha net bir şekilde belirlenmesine olanak tanımaktadır[385]. Sonuç olarak, çok uluslu şirketler için kişisel veri aktarım süreçleri, yalnızca yurt dışına veri gönderimi değil, aynı zamanda veri koruma mevzuatları ile uyum sağlama zorunluluğu, denetim süreçlerinin geliştirilmesi ve grup içindeki veri aktarım sözleşmelerinin detaylı bir şekilde hazırlanması gerekliliği gibi çok yönlü bir karmaşaya işaret etmektedir. Bu noktada, standart sözleşmeler ve veri aktarım süreçlerinin şeffaf ve düzenli bir şekilde yönetilmesi, şirketlerin yerel ve uluslararası düzenlemelere uyum sağlamaları açısından kritik öneme sahiptir. Bu düzenlemelerle birlikte, kişisel verilerin korunması alanında uluslararası uyum ve denetim süreçlerinin daha etkin hale getirilmesi amaçlanmaktadır. Bu çerçevede, holdingin veri işleyen olarak konumlanmasıyla birlikte, grup içi veri aktarımlarında kullanılan standart sözleşmelerin imzalanma ve bildirim süreçleri de ayrı bir önem kazanmaktadır. Özellikle bu sözleşmelerin fiziki imza, KEP veya BTK onaylı elektronik imza ile imzalanması ve ardından imza sonrası beş iş günü içinde Kurul'a bildirimde bulunulması gibi şekli yükümlülükler, uygulamada dikkat edilmesi gereken kritik hususlar arasında yer almaktadır. Ayrıca, söz konusu sözleşmelerin Türkçe versiyonları bağlayıcı olup, İngilizce metinler yalnızca iç yazışma ve belge niteliğinde kabul edilmektedir[386]. Bu değişiklikler, çok uluslu şirketlerin ve grup içi veri aktarım süreçlerinin daha yönetilebilir ve uyumlu hale getirilmesine katkı sağlamaktadır. Bu bağlamda, kişisel verilerin aktarımıyla ilgili düzenlemeler, sektörel uygulamalara da yansımaktadır. Özellikle, uygulamada seyahat acenteleri yurt dışına veri aktarımının en görünür örneklerinden birini oluşturur. Örneğin, bir turizm şirketi her hafta düzenli olarak yurtdışına turlar düzenliyorsa bu aktarım süreklilik arz ettiğinden standart sözleşme akdedilmesi gerekir. Buna karşılık yalnızca özel bir çift için düzenlenen balayı turunda yapılan aktarım arızi ve istisnai nitelikte olduğundan, açık rıza ile aktarım mümkündür. Burada belirleyici unsur, aktarımın

[385] Veri Koruma Derneği, "Data Privacy Türkiye KVKK Standart Sözleşme Atölyesi- Veri Koruma Derneği Platform Toplantısı Çıktıları", *YouTube*, 13 Şubat 2024, (Erişim: 17 Mayıs 2025), https://www.youtube.com/watch?v=K-zdTpx2l3E. (Konuşmacı: Av. Bora Yazıcıoğlu, 57:00–60:00 dk.)

[386] Kişisel Verileri Koruma Kurumu, "Yurt Dışına Kişisel Veri Aktarımı Rehberi", s. 19-20, https://www.kvkk.gov.tr/Icerik/6789/Yurt-Disina-Kisisel-Veri-Aktarimi-Rehberi (E.T.:21.05.2025).
Rehberde, veri aktarımı amacıyla düzenlenen standart sözleşmelerin fiziki ortamda imzalanması, KEP üzerinden veya güvenli elektronik imza ile gönderilmesi ve imza tarihinden itibaren beş iş günü içerisinde Kurula bildirilmesi gerektiği; ayrıca Türkçe metinlerin esas alınacağı, yabancı dildeki versiyonların yalnızca bilgi amaçlı kullanılabileceği belirtilmiştir.

şirketin olağan faaliyet akışının bir parçası olup olmamasıdır[387]. Grup içi veri aktarımları ve standart sözleşmelere ilişkin düzenlemeler yanında, özellikle bulut bilişim sistemleri gibi modern veri işleme yöntemlerinde de veri aktarımı süreçleri farklı dinamiklere sahiptir. Bu kapsamda, Avrupa düzenlemelerine göre, bireylerin kişisel verilerini doğrudan bulut sistemlerine yüklemesi veri aktarımı olarak değerlendirilmemektedir. Ancak anonim şirketlerin çalışanlarına ait kişisel verileri yurt dışındaki sunuculara aktarması halinde, standart sözleşme yapılması zorunlu hale gelmektedir[388]. Özellikle birden fazla şirketin (örneğin A, B ve C) aynı bulut hizmetini kullanması durumunda, her bir veri sahibinden ayrı ayrı açık rıza alınması zorunluluğunu ortadan kaldıran pratik bir çözüm geliştirilmiştir. Bu yaklaşım, şirketlerin veri aktarım süreçlerini daha etkin ve verimli bir şekilde yürütmelerine olanak sağlaması açısından önemli bir adım olarak öne çıkmaktadır. Özellikle bulut hizmetleri gibi dış kaynaklı veri işleme faaliyetlerinde pratik çözümlere duyulan ihtiyaç, grup içi veri aktarımlarında da benzer bir yaklaşımı gündeme getirmektedir. Bu noktada, büyük ölçekli şirketlerin tercih edebileceği yöntemlerden biri olan Bağlayıcı Şirket Kuralları (Binding Corporate Rules- BCR) uzun vadede sürdürülebilir bir çözüm sunsa da Türkiye'de hazırlık ve onay süreçlerinin zorluğu nedeniyle pek tercih edilmemektedir. Bu bağlamda, daha pratik ve erişilebilir bir alternatif olarak standart sözleşmeler ön plana çıkmaktadır. Standart sözleşmeler, büyük şirketlerin veri aktarımlarını daha hızlı ve etkili bir şekilde yönetmelerine olanak tanırken, aynı zamanda çeşitli düzenlemelere de uyum sağlamak adına yeterli koruma sağlamaktadır. Bu yöntem, özellikle veri aktarımlarının süreklilik arz ettiği durumlar için uygun bir çözüm sunmaktadır.

Anonim şirketlerde yurt dışına kişisel veri aktarımı, genellikle sözleşmelerle düzenlenmekte olup, bu süreçte veri aktarımının güvenliğini temin etmek için özellikle standart sözleşmelerin kritik bir rol oynadığından daha önce bahsedilmiştir. Ancak, veri işleyenlerin durumu ve alt veri işleyenlerle gerçekleştirilen işlemler, bu sözleşmelerin uygulanmasını etkileyen önemli bir unsurdur. Şüphesiz, kişisel verilerin yurt dışına aktarımı söz konusu olduğunda, yalnızca veri sorumlusundan veri işleyene ya da veri işleyenden başka bir veri işleyene yapılan aktarımlar değil; bu aktarımların devamındaki alt veri işleyenlere yapılan aktarımları da aynı yasal düzenlemelere tabidir. Özellikle ilk mevzuatın çıktığı dönemde, uygulamada şu tür sorular gündeme gelmiştir: Veri sorumlusundan veri işleyene bir aktarım yapıldığında, eğer veri işleyenin alt veri işleyenleri de bulunuyorsa bu aktarımlar için ayrıca ayrı bir standart

[387] *Ibid.,* s.16.
[388] Avrupa Veri Koruma Kurulu, *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*, Version 2.0, 14 February 2023, s. 6-8.

sözleşmenin yapılması gerekecek mi? Bir başka deyişle, bir veri işleyenin alt veri işleyeni ile de ayrıca standart sözleşme imzalanmalı mı? Başlangıçta bu durum, özellikle Kurul'a bildirilecek sözleşme sayısının artması gibi pratik zorluklar yaratmıştır. Ancak hem KVKK'nın 8. maddesinin (b) bendi hem de buna paralel olarak GDPR'daki standart sözleşme düzenlemeleri çerçevesinde, bir alt veri işleyene yapılan aktarımda ayrıca bir standart sözleşme imzalanması zorunluluğu bulunmadığı açıklığa kavuşmuştur. Bu durumda, veri işleyenden veri işleyene yapılan sözleşme ile alt veri işleyenlere yapılan aktarımlarda da gerekli yükümlülüklerin yerine getirilmiş sayılacağı belirtilmiştir. Bu da sektörde oldukça rahatlatıcı bir yorum olarak kabul edilmektedir. Ancak, burada dikkat edilmesi gereken husus, söz konusu sözleşmenin asgari şartları içermesi ve yazılı olarak yapılmış olması gerektiğidir. Kanaatime göre, bunun için GDPR uyumlu dokümanlar yeterli olmayacaktır. Doktrindeki baskın kanaatte veri işleyenden veri işleyene sözleşmenin yapılması gerektiği yönündedir. Yine de veri işleyenden veri işleyene yapılan sözleşmelerde, yurt dışı aktarım kurallarına uyulması koşuluyla, alt veri işleyenlerle ayrıca bir standart sözleşme yapılmasına gerek bulunmamaktadır. Yurt dışına veri aktarımı ve sözleşme yükümlülükleri göze alındığında prensip olarak, yurt dışındaki bir veri sorumlusunun Türkiye'deki veri işleyenin yapacağı veri aktarımlarında, yurt içindeki veri sorumlusunun yükümlülükleriyle paralel bir şekilde hareket etmesi beklenir. Yani, Türkiye'deki veri sorumlusu nasıl ki sıfırdan veri aktarımı yapıyorsa, yurt dışındaki veri sorumlusunun da benzer şekilde hareket etmesi gerektiği kanaatindeyim. Ancak, yurt dışına veri aktarımı yaparken, KVKK'ya uyumlu şekilde hareket edilmediği takdirde, cezai sorumluluk öncelikle Türkiye'deki veri sorumlusuna yüklenmektedir. Bu bağlamda, AB Veri Koruma Kurumu tarafından verilen bir kararda, veri sorumlusunun yalnızca kendisinin değil, alt veri işleyenlerinin ve onların alt veri işleyenlerinin de tüm aktarımlarını denetlemekle yükümlü olduğu ifade edilmiştir. Uygulamada ise, bu yükümlülük çoğunlukla veri işleyene devredilmektedir; fakat bu, veri sorumlusunun cezai sorumluluğunu ortadan kaldırmaz. Eğer bir hata varsa, veri sorumlusu, veri işleyenden rücu hakkını kullanabilecektir. Şirketler, genellikle rücu maddelerini sözleşmelerine ekleyerek, bu tür sorumlulukları veri işleyenin üzerine bırakmayı tercih etmektedir. Bu, menfaat ve efor açısından makul bir çözüm gibi görünse de alt veri işleyenlere benzer şekilde veri işleyenin de bu yükümlülükleri yerine getirmesi gerekmektedir. Örneğin, bir veri sorumlusunun, yurt dışındaki veri işleyene veri aktarımı yaparken, alt veri işleyenlerle yapılan aktarımda herhangi bir standart sözleşme imzalamamış olması durumunda, bunun cezası yine veri sorumlusuna kesilebilir. Buna karşın, eğer veri işleyenin sözleşmede belirtilen yükümlülükleri yerine getirmediği anlaşılırsa, bu durumda veri sorumlusu, veri işleyene karşı rücu talep edebilir. Bu tür rücu düzenlemeleri,

şirketlerin yasal sorumluluklarını sınırlama adına önemli bir önlem olarak kabul edilmektedir. Kanaatimizce Türkiye içindeki veri aktarımlarında, özellikle veri sorumlusundan veri sorumlusuna yapılan aktarımda, standart sözleşme yapılması gerekmediği ve bunun doğru bir kanun yorumu olmadığı ifade edilebilir[389]. Eğer iki veri sorumlusu arasındaki ilişki, belirli bir amaca yönelik veri aktarımı sağlıyorsa, veri işleme sözleşmesi yeterli olacaktır. Bu sözleşmede, veri aktarımının amacı ve bu verilerin nasıl kullanılacağına dair hükümler yer almalı, ancak bunun dışında Türkiye'deki veri sorumlusunun diğer veri sorumlusunun faaliyetlerini sürekli izlemek gibi bir yükümlülüğü bulunmamaktadır. Veri işleyenin, bu aktarımlar sırasında standart sözleşme yapması gerekmez; yalnızca bu aktarımların güvenliğini sağlayacak bir sözleşme ile veri işleyene yükümlülükler aktarılabilir. Standart sözleşme yapılması yalnızca yurt dışına veri aktarımında gereklidir. Bu, verilerin güvenliğini temin etmek adına önemlidir. Örnek olarak, yurt içindeki bir veri aktarımı sırasında veri sorumlusu, veri işleyene, verilerin yalnızca belirli bir amaçla kullanılacağını belirten bir sözleşme imzaladığında, ek olarak standart sözleşme yapılmasına gerek kalmamaktadır. Bu tür durumlarda, Türkiye'deki veri sorumlusunun yurt dışına veri aktarımı yapmaması şartıyla, yalnızca işleme sözleşmesi ile ilgili yükümlülükler yerine getirilebilir.

Bununla birlikte, veri sorumlusu ile veri işleyen – veya veri işleyen ile alt veri işleyen – arasındaki yükümlülüklerin sözleşmesel düzeyde netleştirilmesi açısından, rücu hükümlerinin[390] sözleşmelere eklenmesi de büyük önem taşımaktadır. Özellikle veri sorumlusu

[389] Kişisel Verileri Koruma Kurulu'nun 02.08.2018 tarihli kararında, bir şirketler topluluğu bünyesinde yer alan birden çok veri sorumlusu şirket arasında kişisel veri aktarımının, üçüncü kişiye veri aktarımı olarak değerlendirildiği ve bu nedenle Kanun'un 8. maddesi kapsamında ilgili kişinin açık rızasının alınması gerektiği belirtilmiştir. Bu kararda, iş başvurusunda bulunan bir adayın kişisel verilerinin (örneğin adı, soyadı, e-posta adresi) ortak veri tabanı aracılığıyla grup şirketleriyle paylaşılabilmesi için açık rıza temin edilmesinin zorunlu olduğu vurgulanmıştır. Aksi takdirde, Kanun'un 18. maddesi gereği idari para cezası uygulanabileceği ifade edilmiştir. Bu karar, grup şirketleri arasında kişisel veri aktarımında, her bir şirketin ayrı bir tüzel kişilik ve dolayısıyla ayrı bir veri sorumlusu olduğu gerçeğini vurgulamaktadır. Bu nedenle, grup şirketleri arasında kişisel veri aktarımı yapılırken, ilgili kişilerin açık rızasının alınması veya Kanun'un 5. ve 6. maddelerinde belirtilen istisnai hallerin bulunması gerekmektedir. Detaylı bilgi için: https://www.kvkk.gov.tr/Icerik/5410/Is-Basvurusu-Surecinde-Islenen-Kisisel-Verilerin-Hukuka-Aykiri-Sekilde-Paylasilmasi. (E.T.: 20.05.2025).

[390] **Anonim Şirketler İçin Örnek Rücu ve Sorumluluk Hükmü**

Taraflar, işbu sözleşme kapsamında yurt dışına kişisel veri aktarımında, KVKK, ikincil mevzuat, Kişisel Verileri Koruma Kurulu kararları ile uluslararası düzenlemelerden doğan tüm yükümlülüklere uyacaklarını karşılıklı olarak taahhüt ederler. Veri aktarımı gerçekleştiren anonim şirket, aktarıma konu verilerin kendi sorumluluk alanında kalmaya devam ettiğini ve üçüncü kişiler nezdinde doğabilecek her türlü zarardan ve idari yaptırımdan ötürü sorumlu tutulabileceğini kabul eder.

Ancak, söz konusu yükümlülüklerin ihlali, veri alıcısı, veri işleyen ya da alt veri işleyen tarafından gerçekleştirilmişse, anonim şirket bu zararın tazminini ilgili taraftan talep edebilir. Bu doğrultuda, veri alıcısı ve/veya veri işleyen, doğrudan veya dolaylı olarak sebep olduğu her türlü zarar, idari yaptırım, dava masrafı, tazminat talebi veya cezai yükümlülük dolayısıyla anonim şirketin uğrayacağı zararları derhal ve eksiksiz şekilde tazmin etmeyi kabul ve taahhüt eder.

Veri alıcısı ayrıca, kendi alt yüklenicileri, grup şirketleri veya hizmet sağlayıcıları ile gerçekleştireceği veri aktarımlarında da işbu sözleşme hükümlerine ve KVKK kapsamında düzenlenen yükümlülüklere uygun hareket

adına hareket eden veri işleyenlerin ve onların alt yüklenicilerinin, olası bir ihlal durumunda hangi koşullarda ve ne ölçüde sorumluluk üstlenecekleri, taraflar arasında çıkabilecek uyuşmazlıkların önüne geçmek açısından açıkça düzenlenmelidir. Bu durumlarda yurt dışına veri aktarımında, bir sonraki aktarımların takibini yapmak her zaman mümkün olmayabilir. Bu nedenle, rücu maddeleri ile sorumluluğun, veri işleyen üzerine bırakılması makul bir çözüm olarak değerlendirilebilir. Bu yaklaşımda, herhangi bir veri ihlali durumunda rücu hakkı kullanılabilir. Ancak, bu tür rücu maddelerinin yazılı bir şekilde ve anlaşılır biçimde sözleşmeye dahil edilmesi önemlidir. Aksi halde, veri sorumlusu sözleşmesel yükümlülüklerini yerine getirmediği gerekçesiyle bizzat sorumlu tutulması söz konusu olabilir.

Bu kapsamda, veri aktarımına ilişkin sözleşmelerin yalnızca içeriği değil, aynı zamanda şekli unsurları da hukuki sorumluluklar açısından kritik öneme sahiptir. Özellikle sözleşmelerde yer alan hükümlerin açık, anlaşılır ve taraflar arasında ihtilafa yer bırakmayacak şekilde kaleme alınması gerekmektedir. Bu noktada, veri aktarımıyla ilgili sözleşmelerin düzenlenmesinde dil seçimi de tartışmalı bir alan olarak öne çıkmaktadır. Yargıtay'ın konuya dair çelişkili kararları, sözleşmelerin hukuki geçerliliği ve dil seçimi konusunda çeşitli belirsizlikler yaratmaktadır[391]. Özellikle anonim şirketlerde, kişisel verilerin yurt dışına aktarımı ile ilgili düzenlemelerde, farklı dilde hazırlanmış sözleşmelerin geçerliliği ve uygulanabilirliği konusunda bazı karışıklıklar bulunmaktadır. Bu noktada, Türkçe ve İngilizce olarak hazırlanan "kolon sözleşmeler" pratikte yaygın bir uygulama biçimi olarak ortaya çıkmaktadır. Ancak bu durum, bazı hukuki belirsizlikleri beraberinde getirmektedir. Özellikle Türk Mahkemelerinin yetkili

edeceğini, aksi halde ilgili yüklenicilerin fiillerinden de doğrudan sorumlu olacağını kabul eder. Bu kapsamda, anonim şirketin gerekli gördüğü hallerde rücu hakkını kullanma, zararların giderimi için yasal yollara başvurma ve veri akış zincirinin bütününde denetim yetkisi saklıdır.

[391] Bknz. Yargıtay 11. Hukuk Dairesi'nin 04.05.2009 tarihli, 2009/2051 E. – 2009/5292 K. sayılı kararı: "…dava dilekçesinde belirtilen hususlar ve sözleşmenin yabancı dilde düzenlenmiş olması sebebiyle davalı tarafın 805 sayılı Kanun'a aykırı olarak yabancı dilde düzenlenen sözleşme hükümlerine dayanarak kendi lehine bir hak elde etmesi mümkün değildir." (Bu karar, yabancı dildeki sözleşmenin doğrudan geçersiz olduğunu değil, Türk tarafı lehine hüküm ifade etmeyeceğini belirtir.) Yargıtay 11. Hukuk Dairesi'nin 05.02.2019 tarihli, 2017/5003 E. – 2019/842 K. sayılı kararı: "...Somut olayda taraflar arasındaki tahkim şartını içeren acentalık sözleşmesi yabancı dilde düzenlenmiş olmakla yukarıda sözü edilen yasa gereğince geçersizdir." (Bu karar ilk bakışta çelişkili gibi görünse de bazı eski kararların tahkim şartını da Kanun kapsamına aldığını gösterir. Ancak güncel eğilim tahkim anlaşmalarının istisna olduğu yönündedir.) İstanbul BAM 43. Hukuk Dairesi'nin 04.03.2021 Tarihli 2020/201 E. – 2021/249 K. Sayılı Kararı: "...kanunun 2. Maddesi uyarınca sözleşmenin taraflarından birinin yabancı olması halinde Türk şirketleriyle yapacakları sözleşmelerde Türkçe kullanılması zorunluluğu bulunmamaktadır." (Bu karar, yabancı tarafın olması halinde 805 sayılı Kanun'un 2. maddesi kapsamında Türkçe zorunluluğunun olmadığını açıkça belirtir ve tahkim anlaşmalarının da bu kapsamda değerlendirilebileceğine işaret eder.) Yargıtay 11. Hukuk Dairesi'nin 2020 tarihli, 2018/3182 E. – 2020/2652 K. sayılı kararı: "Milletlerarası Tahkim Kanunu'nun 15. maddesinde yer alan iptal sebepleri ile sınırlı yapılan incelemede; dava şartları ve hukukun uygulanması bakımından da hükmün bozulmasını gerektirir bir neden bulunmamasına ve özellikle tahkim yargılamasına konu uyuşmazlıkta 4686 sayılı Kanun'un 2. maddesi ve 805 sayılı Kanun'un 4. maddesinin uygulama yeri bulunmadığından, yabancılık unsuru bulunan tahkim sözleşmelerinin geçerliliğini koruduğu kabul edilmiştir." (Bu karar, tahkim anlaşmalarının 805 sayılı Kanun kapsamı dışında olduğunu açıkça teyit etmektedir.)

kılındığı durumlarda, 805 sayılı Kanun gereğince, sözleşmenin Türkçe metni geçerli kabul edilmektedir. Ancak, KVKK kapsamında, farklı dillerde imzalanmış bir sözleşmenin yine de Türkçe metninin geçerli olacağı belirtilmiştir. Bu konuda uygulamada ise KVKK Danışma Hattı'nın yanlış bir anlayışa yol açması, Türkçe sözleşme imzalanmasının zorunlu olduğu yönünde yanlış bir algı oluşturmuştur. Ancak sonrasında yapılan görüşmeler ve düzeltmelerle, çift kolonlu sözleşme uygulamasının kabul edilebilir olduğu anlaşılmıştır[392]. Çift dilde hazırlanan sözleşmelerde imzalanacak metnin hangisi olması gerektiği ise bir başka tartışma konusudur. Türk Mahkemeleri söz konusu olduğunda, kanunun açık bir şekilde Türkçe metnin geçerli olacağı yönünde hüküm verdiği göz önüne alındığında, imzanın Türkçe metne atılması pratikte en güvenli yaklaşım gibi gözükmektedir. Ancak, yabancı kişilerle yapılan sözleşmelerde, İngilizce metnin geçerliliği konusunda şüpheler oluşabileceği için, uygulamada çoğu zaman hem Türkçe hem de İngilizce metinler aynı anda düzenlenip, her iki metnin de ad, soyad, name, sur name gibi unsurlarının paralel şekilde yazılması sağlanmaktadır. Bu tür bir uygulama, özellikle çok uluslu şirketlerle yapılan sözleşmelerde pratik bir çözüm sunmaktadır. Türkçe ve İngilizce metinlerin eş zamanlı olarak hazırlanması, uygulamada pratik bir çözüm olarak kabul edilmektedir. Burada önemli olan, sözleşmenin taraflarca imzalanmasının ardından geçerli olacak dilin net bir şekilde belirlenmesidir. Pratikte ise, genellikle Türkçe ve İngilizce metinlerin aynı anda imzalanması en uygun çözüm olarak uygulanmaktadır. Bu konuda, sözleşmelerin taraflarca kabul edilen dilinde imzalanması gerektiği ifade edilmektedir. Sözleşmenin imza tarihi, yasal açıdan oldukça önemli bir husus olup, bazı durumlarda bu tarih, sözleşmenin geçerliliğini etkileyebilir. İmza tarihi ile ilgili de ciddi bir belirsizlik bulunmaktadır. Özellikle kanun değişiklikleri ve geçiş dönemlerinin sona erdiği tarihler bu konuda çeşitli kaygılara yol açmaktadır. Örneğin, 1 Eylül 2024 tarihinden itibaren geçiş dönemi sona erdiği için, o tarihten sonraki dönemde devam eden veri işleme faaliyetlerinin ne zaman başlayacağı konusunda bir belirsizlik oluşmuştur. Eğer müzakereler devam ederken, sözleşme imzalanamamışsa, bu durumun ihbar olarak değerlendirilip değerlendirilemeyeceği konusunda endişeler bulunmaktadır. Örneğin, Amazon Türkiye kararında, veri sorumlusunun taahhüdü sunulurken, taahhütname verildiği takdirde ceza uygulanması durumu ortaya çıkmıştır[393]. Burada, taahhütnamenin sunulmasının kendini ihbar etme anlamına gelip gelmeyeceği

[392] Veri Koruma Derneği, "Data Privacy Türkiye KVKK Standart Sözleşme Atölyesi- Veri Koruma Derneği Platform Toplantısı Çıktıları", *op.cit.*

[393] Kişisel Verileri Koruma Kurulu'nun Amazon Turkey Perakende Hizmetleri Limited Şirketi hakkındaki 27/02/2020 Tarihli ve 2020/173 Sayılı Kararı, https://www.kvkk.gov.tr/Icerik/6739/2020-173. KVKK'nın Amazon Türkiye hakkında aldığı bu kararda, temel olarak üç ana ihlal tespit edilmiştir: Mevzuata Uygun Açık Rıza Alınmaması, Kişisel Verilerin Hukuka Aykırı Olarak Yurt Dışına Aktarılması, Aydınlatma Yükümlülüğünün İhlali

konusunda kaygılar bulunmaktaydı. Bu tür durumlar, pratikte, imza tarihinin etkisiyle ilgili hukuki belirsizliklere yol açmaktadır. Ancak, bu tür bir durumda, tarafların iradesi önemlidir. Eğer taraflar, sözleşmenin geçmişe etkili olmasını kabul etmişse, bu geçerli olacaktır. Sözleşme serbestisi kapsamında, sözleşmenin geriye etkili olması, tarafların mutabakatı ile mümkün olabilmektedir. Bu bağlamda, uygulamada bazı avukatlar, sözleşmeye "1 Eylül 2024 tarihinden itibaren geçerli olmak üzere" şeklinde bir ibare eklemeyi tercih etmektedir. Ancak, bu düzenlemenin kurum tarafından kabul edilip edilmeyeceği belirsizdir. Makul olan bu uygulamanın kabul edilmesi olduğu kanaatindeyim. Sonuç olarak sözleşme geçerliliği ve imza tarihinin etkisi konusunda doktrinde iki farklı görüş bulunmaktadır: Bazı hukukçular, bu tür sözleşme düzenlemelerinin geçerli olacağını savunurken, diğerleri, geçersiz olacağı yönünde görüş bildirmektedir. Objektif hukuk anlayışı ve sözleşme serbestisi göz önüne alındığında, bu tür düzenlemelerin geçerli olacağı kanaatindeyim. Ancak, sözleşmenin geçerlilik tarihine dayanarak yapılacak bir yaptırımın, çok ağır ve adil olmayan sonuçlara yol açabileceği düşünülmektedir. Bu nedenle, sözleşme taraflarının bu tür konularda daha esnek ve makul çözümler üretmesi gerektiği kanaatindeyim.

Uygulamada en çok merak edilen bir diğer husus sözleşmelerin tüm sayfalarının taraflar tarafından imzalanması gerekip gerekmediği yönündedir. Hukukumuzda yazılı şekil şartı bulunmamakla birlikte, sözleşmelerin tüm sayfalarının taraflarca imzalanması gerekmemektedir. Yargıtay kararları da bu hususu desteklemektedir[394]. Önemli olan, imzanın o dokümana ait olduğunun tespit edilebilmesidir ve belgenin bir bütünlük içinde sunulmasıdır. Eğer bir sözleşme tüm sayfalarda imza veya paraf ile tamamlanmışsa, bu yalnızca ispatı güçlendiren bir önlem olarak kabul edilebilir. Ancak, her sayfanın imzalanması, hukuki bir yükümlülük değildir. Uygulamada, taraflarca sayfalara paraf atılması sıklıkla görülse de bu işlem yasal bir zorunluluk olmamakla birlikte, belgelerin geçerliliğini ve taraflar arasında anlaşmazlık durumunda ispatı kolaylaştıran bir önlem olarak değerlendirilebilir. Resmi bir

[394] Yargıtay 3. Hukuk Dairesi'nin 07.12.2021 tarihli, 2021/12613 sayılı kararında imzanın geçerliliğiyle ilgili tartışmalar önemli bir yer tutmaktadır. Özetle, Davacı tarafından sunulan 25.08.2008 tarihli sözleşme iki sayfadan oluşmaktadır. Sözleşmenin ilk sayfasında davalının imzası bulunmamaktadır. Ancak ikinci sayfanın sonunda, "iş bu 2 sayfadan ve 8 maddeden ibaret sözleşme metnini okuduk, mahiyetini anladık ve taraflar adına serbest irademizle imzaladık" şeklindeki ifade yer almakta ve bu sayfa taraflarca imzalanmıştır. Yargıtay'a göre, çok sayfalı sözleşmelerde her sayfanın ayrı ayrı imzalanması zorunlu değildir. Yeter ki metin, içerik olarak bir bütünlük ve mantıksal devamlılık arz etsin. İkinci sayfadaki açıklama, iki sayfanın tek bir sözleşmenin parçası olduğunu göstermektedir. Davalının, ilk sayfanın farklı içerikte olduğuna veya sonradan eklendiğine dair delil sunmadığı belirtilmiştir.https://www.lexpera.com.tr/ictihat/yargitay/3-hukuk-dairesi-e-2021-273-k-2021-12613-t-7-12-2021. Benzer bir şekilde Yargıtay 6. Hukuk Dairesi'nin 30.09.2015 tarihli kararı hakkında detaylı bilgi için: https://eshukuk.com/Icerik/davali-davada-dayanilan-kira-sozlesmesindeki-imzasini-inkar-etmemektedir-kira-s. (Erişim Tarihi:15/05/2025).

rehber olmamakla birlikte, Kurul'un açıklamaları da bu doğrultudadır[395]. Bu durumda, sözleşmelerin geçerliliği, her sayfanın imzalanmasından ziyade, sözleşme metninin bütünlük arz etmesi ve tarafların iradelerinin açıkça belirlenmesi ile sağlanmaktadır[396]. Sözleşmelerin imzalanması sırasında vekâletname veya yetki belgesi sunulması uygulamada sıklıkla tartışma konusu olmaktadır. Yargı kararları incelendiğinde, bu konuda açık bir mutabakat bulunmadığı, ancak temsil yetkisinin yazılı belgeyle tevsik edilmesinin hukuki güvenlik açısından önemli olduğu görülmektedir. Özellikle Yargıtay Hukuk Genel Kurulu'nun 2023/618 K. sayılı kararında, vekâletnameye ilişkin bilgilerin (vekâlet veren, dayanak vekâletname, noter tarih ve yevmiye no) eksik olması nedeniyle sunulan yetki belgesinin geçersiz olduğuna hükmedilmiştir[397]. Benzer şekilde, Yargıtay 3. Hukuk Dairesi'nin 2002/1200 K. sayılı kararında da genel vekâletnamenin sadece olağan işleri kapsadığı, özel işlemler için açıkça yetki verilmiş olması gerektiği vurgulanmıştır[398]. Kişisel Verileri Koruma Kurulu da bu konuda çeşitli kararlarında temsil yetkisine ilişkin belgelere atıfta bulunmaktadır. Kurulun 2021/1262 sayılı kararında, ilgili kişinin banka nezdindeki kişisel verilerinin işlenmesine ilişkin başvurusunda sunulan vekâletnamenin geçerliliği incelenmiş; temsil ilişkisinin yazılı belge ile ispatı gerektiği değerlendirilmiştir[399]. Yine 2022/489 sayılı Kurul kararında, kamu kurumu nezdinde yapılan başvuruda sunulan yetki belgesinin, vekâletname ile aynı işlevi yerine getirebileceği ifade edilmiştir[400]. Bu nedenle, sözleşme tarafının bir temsilci aracılığıyla işlem yapması durumunda, temsil yetkisinin dayanağı olan vekâletname veya yetki belgesinin, özellikle ileriye dönük ihtilafların önüne geçilmesi açısından, sözleşmeye eklenmesi yerinde olacaktır. Aynı durum, KEP (Kayıtlı Elektronik Posta) yoluyla yapılan bildirimlerde de geçerlidir. Bu tür işlemlerde de yetkilendirmeyi gösteren belge eklenmesi, uygulamada hukuki güvenliğin sağlanması bakımından önem taşımaktadır.

Sözleşmelerin hangi taraflar arasında ve hangi yetkiler kapsamında imzalandığı kadar, tarafların 6698 sayılı Kişisel Verilerin Korunması Kanunu kapsamında veri sorumlusu ya da veri işleyen olarak sıfatlandırılmaları da son derece önemlidir. Zira veri koruma rejiminde

[395] Kişisel Verileri Koruma Kurumu tarafından, sözleşmelerin tüm sayfalarının imzalanması gerekliliği konusunda özel bir karar bulunmamaktadır. KVKK'nın kararları genellikle kişisel verilerin işlenmesi, aktarılması ve korunması gibi konulara odaklanmaktadır.
[396] Yargıtay 3. Hukuk Dairesi'nin 07.12.2021 tarihli, 2021/12613 sayılı kararı.
[397] Yargıtay Hukuk Genel Kurulu, E. 2023/618, K. 2023/..., www.karamercanhukuk.com/yetki-belgesi-gecersiz-karar. (Erişim Tarihi:15/05/2025).
[398] Yargıtay 3. Hukuk Dairesi, E. 2002/414, K. 2002/1200, "Vekilin özel yetkisi olmadan yaptığı işlemler", Dergipark, https://dergipark.org.tr/tr/download/article-file/1878517. (Erişim Tarihi:15/05/2025).
[399] Kişisel Verileri Koruma Kurulu, Karar No: 2021/1262, www.kvkk.gov.tr. (Erişim Tarihi:15/05/2025).
[400] Kişisel Verileri Koruma Kurulu, Karar No: 2022/489, www.kvkk.gov.tr. (Erişim Tarihi:15/05/2025).

tarafların yükümlülükleri, sahip oldukları sıfatlara göre değişmektedir. Bu çerçevede, uygulamada sıklıkla karşılaşılan bir diğer durum ise veri işleyenlerin, belirli faaliyetler kapsamında veri sorumlusu olarak da hareket edebilmeleridir. Örneğin, bir veri işleyen, bir müşterinin verilerini alarak iletişim amacıyla kullanıyorsa, bu faaliyet kapsamında veri sorumlusu yine veri işleyeni olabilir[401]. Örneğin, bir firma çalışanlarının verilerini işleyen bir şirket, bu faaliyetle ilgili veri işleyeni kabul edilebilir[402]. Bir başka örnek olarak, admin hesapları üzerinden yapılan veri işlemleri de bu kapsama girebilir. Örneğin, bir veri sorumlusu şirketin müşteri verilerini işlemek üzere hizmet aldığı bir veri işleyenin "helpdesk" departmanında meydana gelen bir veri ihlali durumunda, sorumluluğun hangi tarafa ait olduğunun tespiti önem arz etmektedir. Bu tür durumlarda veri sorumlusu şirket, söz konusu ihlalin kendi kontrolü dışında, veri işleyenin kendi organizasyonel yapısı ve sorumluluğu çerçevesinde gerçekleştiğini ileri sürebilir. Özellikle, veri işleyenin helpdesk veya yönetici (admin) hesapları üzerinden gerçekleştirdiği işlemlerin, doğrudan veri sorumlusunun talimatlarıyla sınırlı olmayan, kendi faaliyet alanı içerisinde değerlendirilebilecek nitelikte olduğu durumlarda, bu bölümde gerçekleşen ihlalin veri işleyenin bağımsız sorumluluğu altında gerçekleştiği savunulabilir[403]. Bu çerçevede, veri sorumlusu ve veri işleyen arasındaki ilişkinin sınırlarının açık şekilde tanımlanması ve tarafların sorumluluklarının sözleşmesel düzenlemelerle netleştirilmesi, olası veri ihlallerinde sorumluluğun doğru belirlenebilmesi açısından kritik bir öneme sahiptir[404]. Ayrıca, Avrupa Birliği Genel Veri Koruma Tüzüğü kapsamında da benzer bir yaklaşım benimsenmiştir. GDPR'ın 33. maddesi uyarınca, veri işleyen, bir kişisel veri ihlali meydana geldiğinde, bu durumu derhal veri sorumlusuna bildirmekle yükümlüdür. Sonuç olarak, veri sorumlusu ve veri işleyen arasındaki ilişkinin ve sorumlulukların açıkça tanımlanması, özellikle veri ihlali gibi hassas durumlarda, tarafların

[401] Kişisel Verileri Koruma Kurulu'nun 2020/225 sayılı kararında, bir veri işleyenin müşterilere yönelik doğrudan pazarlama faaliyetleri yürütmesi durumunda, bu faaliyet özelinde veri sorumlusu sayılabileceği belirtilmiştir. Bknz. Kişisel Verileri Koruma Kurulu, Karar No: 2020/225, "Veri işleyenin pazarlama faaliyeti yürütmesi halinde veri sorumluluğu değerlendirmesi", www.kvkk.gov.tr. (Erişim Tarihi:15/05/2025).

[402] Bir hizmet sağlayıcısının, yalnızca işveren adına değil, kendi inisiyatifiyle çalışan verilerini kullanması hâlinde, Kurulun 2019/10 sayılı kararında açıklandığı üzere, ilgili faaliyet özelinde veri sorumlusu olarak değerlendirilebileceği ifade edilmiştir. Kişisel Verileri Koruma Kurulu, Karar No: 2019/10, "Çalışan verilerinin işlenmesinde veri sorumlusu ve veri işleyen ayrımı", www.kvkk.gov.tr. (Erişim Tarihi:15/05/2025).

[403] Kurulun 2022/987 sayılı kararında, sistem yöneticileri (admin hesapları) tarafından yapılan veri işleme faaliyetleri için yapılmıştır. Kurul, bu tür işlemlerde kişisel verilere erişen kişinin yalnızca teknik destek sağlayıcısı olması durumunda veri işleyen sıfatında kalacağını, ancak erişimin ötesinde bağımsız bir karar alma ve işleme faaliyetinin yürütülmesi halinde veri sorumluluğunun söz konusu olabileceğini vurgulamıştır. Kişisel Verileri Koruma Kurulu, Karar No: 2022/987, "Admin hesapları üzerinden gerçekleştirilen veri işlemelerinde sıfat değerlendirmesi", www.kvkk.gov.tr. (Erişim Tarihi:15/05/2025).

[404] Nitekim, Kişisel Verileri Koruma Kurumu'nun 24.01.2019 tarihli ve 2019/10 sayılı kararında, veri işleyenin nezdinde gerçekleşen bir kişisel veri ihlali durumunda, veri işleyenin bu durumu derhal veri sorumlusuna bildirmesi gerektiği belirtilmiştir.

yükümlülüklerinin belirlenmesi ve hukuki sorumluluğun doğru şekilde tespiti açısından büyük önem taşımaktadır.

Tüm bu sorumluluk ve ilişki tanımlamalarının yanı sıra, veri aktarım süreçlerinde aktarılan verinin niteliği de hukuki değerlendirmeyi doğrudan etkilemektedir. Özellikle, özel nitelikli kişisel verilerin aktarımı söz konusu olduğunda hem veri sorumluları hem de veri işleyenler açısından çok daha sıkı ve ayrıntılı düzenlemelere uyum sağlanması zorunluluğu doğmaktadır. Örneğin, bir hizmet alımı kapsamında kişisel verinin aktarılması, genellikle kanunun m. 5/2-f hükmü uyarınca "veri sorumlusunun meşru menfaati" gibi hukuki sebeplerle örtüşebilir, ancak özel nitelikli veriler söz konusu olduğunda, bu verilerin paylaşılmasını istemeyen veri sorumluları için belirli önlemler almak gereklidir[405]. Veri sorumlusunun kontrolü haricinde, örneğin bir e-posta servisi (Outlook, Gmail) üzerinden paylaşılan özel nitelikli verilerin, veri sorumlusunun istediği şekilde işlenip işlenmediğini denetlemek, genellikle zordur[406]. Ancak, bu tür verilerin paylaşılması durumunda, herhangi bir hukuki düzenleme getirilmeden, yalnızca veri sorumlusunun özel nitelikli verileri denetlemesi gerekir. Eğer veri sorumlusunun faaliyetlerinin bir parçası olarak özel nitelikli veriler işleniyorsa, bu verilerin aktarımı konusunda açık bir hukuka uygunluk sebebi bulunmamakla birlikte, aktarımlar için meşru menfaat gibi hukuki sebeplerin de kullanılabileceği belirtilmelidir[407].

Bir diğer önemli tartışma, veri aktarımının Avrupa düzenlemeleriyle kıyaslandığında Türkiye'deki farklılıklarıdır. Avrupa'da, verilerin aktarılması için belirli bir hukuki sebebin bulunması gerektiği açıkça ifade edilmiştir. Ancak, Türkiye'deki mevzuat, bu durumu biraz daha esnek şekilde ele almakta, 5. ve 6. maddelerde belirtilen hukuka uygunluk sebeplerine dayalı olarak verilerin aktarılmasına olanak tanımaktadır. Bu durum, özellikle yurt dışına veri aktarımı söz konusu olduğunda önemli bir fark yaratmaktadır. Yine de 9. madde çerçevesinde, veri aktarımının hukuka uygunluk sebeplerine dayanması gerektiği, özellikle özel nitelikli

[405] Zira özel nitelikli verilerin işlenmesi ve aktarılması, KVKK m. 6'da düzenlenen özel koşullara tabidir ve açık rıza dışındaki hukuka uygunluk sebepleri sınırlıdır.

[406] Kişisel Verileri Koruma Kurulu'nun 2018/10 sayılı ilke kararı, özel nitelikli verilerin işlenmesinde veri güvenliğine ilişkin teknik ve idari tedbirlerin alınmasını zorunlu kılmakta; özellikle bu verilerin aktarımı sırasında kriptolama, erişim kısıtı ve aktarımın sınırlandırılması gibi önlemlerin alınmasını tavsiye etmektedir.
Kişisel Verileri Koruma Kurulu, İlke Karar No: 2018/10, "Özel Nitelikli Kişisel Verilerin İşlenmesinde Alınması Gereken Teknik ve İdari Tedbirler", www.kvkk.gov.tr. (Erişim Tarihi:15/05/2025).

[407] Bu bağlamda, hizmet sağlayıcı aracılığıyla yapılan özel nitelikli veri aktarımı söz konusuysa, yalnızca meşru menfaat hukuki sebebine dayanmak yeterli görülmemelidir. Kurulun 2020/966 sayılı kararında da belirtildiği üzere, bu tür verilerin aktarımı sırasında veri sorumlusunun açık rıza alınmaksızın gerçekleştireceği işlemlerde hukuka uygunluk sebebi olarak yalnızca m. 5/2-f'ye (meşru menfaat) dayanılması yeterli olmayabilir ve bu durum açık rıza gerekliliğini doğurabilir.
Kişisel Verileri Koruma Kurulu, Karar No: 2020/966, "Özel nitelikli kişisel verilerin hizmet sağlayıcı yoluyla aktarımı ve açık rıza değerlendirmesi", www.kvkk.gov.tr. (Erişim Tarihi:15/05/2025).

veriler açısından büyük önem taşımaktadır. Bu noktada, Türkiye'deki mevzuat ile Avrupa'daki uygulamalar arasındaki farklar da dikkatle incelenmelidir. Bu bağlamda, standart sözleşmelerin imzalanması, yurt dışına kişisel veri aktarımında veri güvenliğini sağlamak için kullanılan araçlardan biridir. Ancak hem KVKK'da hem de GDPR'da olduğu gibi, veri aktarımının hukuka uygun kabul edilebilmesi için, öncelikle kişisel verilerin işlenmesine ilişkin geçerli bir hukuki sebebin (örneğin GDPR m.6 veya m.9 kapsamında) mevcut olması ve temel ilkelere (GDPR m.5) uygunluğun sağlanması gerekmektedir. Nitekim GDPR m.44 de açıkça, aktarımın tüzüğün diğer hükümlerine tabi olduğunu belirtmek suretiyle, yalnızca aktarım aracının varlığının yeterli olmadığını ortaya koymaktadır. Ancak, veri işleyene yapılan aktarım ile veri sorumlusundan veri sorumlusuna yapılan aktarım arasında bir fark bulunmaktadır. Bu fark, hukuki uygunluk sebeplerinin belirlenmesinde önemli bir rol oynamaktadır. Veri işleyenlerin, aktarılan verilerin kontrolünü sağlama noktasında daha fazla esneklik sağlayan bir düzenleme ile veri aktarımı yapılabilirken, veri sorumlusundan veri sorumlusuna yapılan aktarımlarda hukuka uygunluk sebebinin mutlaka belirlenmesi gerektiği anlaşılmaktadır. Sonuç olarak, özel nitelikli verilerin aktarılması ve genel veri aktarımı için farklı hukuki dayanakların bulunması gerektiği, aynı zamanda mevzuatın esnekliğine göre uygulanabilecek farklı yorumların var olduğu ortaya çıkmaktadır. Bu nedenle, özellikle veri aktarımının hukuka uygunluk sebeplerinin belirlenmesi, her iki tarafın da yasal yükümlülüklerini yerine getirebileceği bir denetim mekanizmasının kurulmasına olanak tanıyacaktır. Bu bağlamda, özel nitelikli kişisel verilerin aktarımında hangi hukuki zeminin tercih edileceği, yalnızca verinin niteliğine değil, aynı zamanda aktarım sürecinde kullanılan araçlara da bağlıdır. Özellikle standart sözleşmelerin yurt dışına veri aktarımında sıklıkla tercih edilen yöntemlerden biri olması, bu sözleşmelerin açık rıza ile ilişkisini tartışmalı hale getirmiştir. Standart sözleşmelerin kişisel verilerin yurt dışına aktarılmasında hukuki bir dayanak olarak kullanılmasında temel fark, veri aktarımının "açık rıza"ya dayalı mı yoksa "uygun güvenceye" mi dayalı olarak yapılacağı meselesidir. Kişisel Verileri Koruma Kurumu, 2 Ocak 2025 tarihinde yayımladığı "Kişisel Verilerin Yurt Dışına Aktarılması Rehberi"nde, standart sözleşmelerin, kişisel verilerin yurt dışına aktarımında uygun güvence sağladığını ve bu durumda ayrıca açık rıza alınmasının gerekmediğini belirtmiştir[408]. Rehberde, standart sözleşmelerin, veri aktarımında açık rızaya alternatif bir hukuki dayanak olduğu vurgulanmıştır. Ayrıca, 10 Temmuz 2024 tarihinde yayımlanan "Kişisel Verilerin Yurt Dışına Aktarılmasına İlişkin Usul ve Esaslar Hakkında Yönetmelik"te de yeterlilik kararı bulunmayan ülkelere veri aktarımında, standart

[408] Ayrıca değişen kanun ile açık rızaya sadece arızi sebeplerle dayanılacağı unutulmamalıdır.

sözleşmelerin uygun güvence sağladığı ve bu durumda açık rıza alınmasının zorunlu olmadığı düzenlenmiştir. Buna karşın, açık rızanın her durumda geçerli olabileceği, özellikle ortak faaliyetlerde veri sorumlularının ve veri işleyenlerinin bu hukuki zeminde anlaşmaları gerektiği konusu da tartışılabilir. Bu noktada, iki farklı hukuki sebep söz konusu olabilir: Meşru menfaat ve açık rıza. Veri sorumluları, özellikle kişiselleştirilmiş pazarlama gibi faaliyetlerde açık rızayı esas alırken, meşru menfaat gibi hukuki sebeplerle de veri işleyebilmektedir[409]. Bununla birlikte, özel nitelikli verilerin işlenmesi söz konusu olduğunda, bu işlemler için istihdam ilişkisi gibi belirli bağlamlar altında açık rıza alınması gerekmektedir. Ancak bu durumda, verilerin aktarımı için yine standart sözleşme imzalanmalı ve açık rıza alınmalıdır[410]. Bu yorum farkı, özellikle uygulamada önemli sonuçlar doğurmaktadır[411]. Standardın bir şekilde uygulanması, yalnızca teorik olarak değil, pratikte de hukuki zeminin doğru belirlenmesi gerekliliğini ortaya koymaktadır. Verilerin yurt dışına aktarılmasında da benzer şekilde hukuki sebepler devreye girmektedir. Özellikle, standart sözleşmenin yerine getirilmesi sırasında aktarılan verilerin hukuka uygun bir şekilde işlenmesi gerektiği unutulmamalıdır. Bu bağlamda, ilgili kişilere yönelik yapılan aydınlatma metinleri büyük bir önem taşımaktadır. Aktarımın hukuki dayanağının ne olduğunu belirlemek ve buna uygun hareket etmek gereklidir. Ancak, uygulamada, kimi zaman veri işleme faaliyetlerinin yalnızca operasyonel gerekçelere dayandırıldığı ve aktarımın hukuki temelinin yeterince açıklanmadığı görülmektedir. Bu durum bazı veri aktarım süreçlerinde hukuki belirsizliklere neden olabilmektedir. Yurt dışına veri aktarımı sürecinde veri sorumlusu ve veri işleyen arasındaki ilişki, farklı hukuki gerekçelerle yönetilebilmektedir. Özellikle, bir veri işleyen aracılığıyla verilerin yurt dışına aktarılmasında, bu aktarımın yalnızca veri sorumlusunun rızasıyla yapılması gerektiği düşünülmektedir. Uygulamada, veri sorumlusundan veri işleyene yapılacak aktarımın, her durumda ayrı bir hukuki sebep gerektirip gerektirmediği konusunda uygulayıcılar arasında farklı yaklaşımlar gözlemlenmektedir[412]. Ancak, aktarım işlemlerinde yasal uygunluk sebeplerinin açıkça

[409] KVKK'nın 02/09/2022 tarihli ve 2022/902 sayılı kararında, ilgili kişinin açık rızası alınmadan pazarlama amacıyla kısa mesaj gönderilmesi suretiyle kişisel verilerinin işlenmesi konusu ele alınmıştır. Kararda, kişisel verilerin işlenmesinde açık rızanın temel şart olduğu, ancak Kanun'un 5. maddesinin 2. fıkrasında belirtilen şartların varlığı halinde açık rıza olmaksızın da veri işlenmesinin mümkün olabileceği belirtilmiştir. Ancak, pazarlama faaliyetleri gibi durumlarda, ilgili kişinin temel hak ve özgürlüklerine zarar vermemek kaydıyla veri sorumlusunun meşru menfaatleri için veri işlenmesinin zorunlu olması şartının dikkatle değerlendirilmesi gerektiği vurgulanmıştır. https://www.kvkk.gov.tr/Icerik/7585/2022-902.

[410] Standart sözleşme süreçleriyle ilgili henüz kurul kararı olmadığı için açık rıza alınması ile ilgili Bknz. https://www.kvkk.gov.tr/Icerik/5410/Is-Basvurusu-Surecinde-Islenen-Kisisel-Verilerin-Hukuka-Aykiri-Sekilde-Paylasilmasi, (E.T.: 15/05/2025).

[411] Veri Koruma Derneği, "Data Privacy Türkiye KVKK Standart Sözleşme Atölyesi- Veri Koruma Derneği Platform Toplantısı Çıktıları", *YouTube*, 13 Şubat 2024, https://www.youtube.com/watch?v=K-zdTpx2l3E, (Erişim Tarihi: 17 Mayıs 2025).

[412] *Ibid.*

belirlenmesi ve bu aktarımın KVKK çerçevesinde temellendirilmesi, şirketlerin hukuki yükümlülüklerini yerine getirmesi açısından önem arz etmektedir. Tüm bu hukuki dayanakların belirlenmesi kadar, veri aktarımına eşlik eden süreçlerin içeriği de dikkatle değerlendirilmelidir. Özellikle, verilerin aktarılmasından sonraki dönemde nasıl saklandığı ve ne kadar süreyle muhafaza edildiği, veri sorumlusu ile veri alıcısı arasındaki iş birliğinin sınırlarını ve sorumluluk paylaşımını doğrudan etkilemektedir[413]. Yurt dışına veri aktarımı yapıldığında, verilerin saklanma süreleri konusunda da önemli bir tartışma bulunmaktadır. Özellikle Verbis 'in belirlediği saklama sürelerinin, veri aktarıcısının ve veri alıcısının süreçlerine paralel olup olmadığı sorgulanmaktadır. Bu konuda, veri aktarıcıları ve veri alıcıları arasında fikir birliği sağlanması önemlidir. Veri alıcısının verileri ne kadar süreyle saklayacağı ve hangi güvenlik tedbirlerini alacağı da belirleyici unsurlar arasında yer almaktadır. Veri sorumluları, kendi sistemlerinde verinin ne kadar süreyle saklanacağını belirleyebilse de dış kaynaklardan alınan hizmetlerde bu süre, veri işleyenin ya da hizmet sağlayıcının belirlediği şartlara göre değişebilmektedir. Bu nedenle hem veri işleyici hem de veri alıcıları ile yapılan sözleşmelerde, verilerin saklama süreleri ve güvenlik tedbirleri açıkça belirtilmelidir. Saklama sürelerine ilişkin belirsizliklerin ardından, veri aktarım zincirinde yer alan tarafların rollerinin netleştirilmesi de bir diğer önemli husus olarak karşımıza çıkmaktadır. Özellikle veri işleme faaliyetinin karmaşıklaştığı durumlarda, yalnızca veri sorumlusu ve veri işleyen arasında değil, bu ilişkilerin bir uzantısı olarak ortaya çıkan "alt veri işleyen" kavramı da gündeme gelmektedir[414]. GDPR 'de yer almayan ve Türk hukuku açısından önemli bir konu olan bu kavram, verilerin sadece sözleşme tarafları tarafından değil, aynı zamanda dış kaynaklardan gelen üçüncü taraflarca da alınabileceği durumları ifade etmektedir[415]. Bu noktada, veri sorumluları ve veri işleyenlerinin, sözleşmelerde "alt veri işleyenler" ve "alıcılar" gibi tanımlamalar yaparak, verinin aktarılacağı tüm paydaşları net bir şekilde belirtmeleri gerekmektedir[416]. Alt veri işleyen kavramı ile birlikte, yurt dışına yapılan veri aktarımlarında dikkat edilmesi gereken bir diğer önemli husus ise, onward transfer yani sonraki aktarım

[413] İkiler, Bora ve Y. Sertaç Serter. *Şirketler İçin Kişisel Verilerin Korunması Hukuku Rehberi*, On İki Levha Yayıncılık, İstanbul 2023, s.100-102.
[414] Ömer Ekmekçi, Nafiye Yücedağ, Elif Beyza Akkanat-Öztürk, Şehriban İpek Aşıkoğlu, Kişisel Verilerin Korunması Hukuku, On İki Levha Yayıncılık, 1.bs., İstanbul 2024, s.82.
[415] Miray Özer Deniz, "Kişisel Verilerin İşlenmesinin Türleri ve Hukuki Nitelikleri" *Necmettin Erbakan Üniversitesi Hukuk Fakültesi Dergisi*, cilt:6, S. 1, 2023, s. 104.
[416] Kişisel Verileri Koruma Kurulu, Veri Sorumlusu ve Veri İşleyen Rehberi'nde veri sorumlusu ile veri işleyen arasında akdedilecek veri işleme sözleşmesinde veri işleyene bazı yetkilerin bırakılabileceği örneklendirilmiştir; Kişisel Verileri Koruma Kurumu, "Veri Sorumlusu ve Veri İşleyen Rehberi", s.3, (https://www.kvkk.gov.tr/Icerik/4195/Veri-Sorumlusu-ve-Veri-Isleyen, (E.T.: 15.05.2025).

meselesidir[417]. Bu, veri işleyen tarafından aktarılan verilerin, başka bir üçüncü tarafa aktarılması anlamına gelir. Ancak, bu tür bir aktarımda, veri alıcılarının kimler olacağı ve bu kişilerin hangi hukuki dayanaklarla veri aldıkları da sözleşmelerde açıkça yer almalıdır. Onward transfer gibi veri zincirinin sonraki halkalarını düzenlemek, yalnızca aktarımın güvenliğini değil, aynı zamanda veri sorumluluğu çerçevesinde yükümlülüklerin doğru dağılımını da gerektirir. Bu noktada, standart sözleşmelerin yurt dışına kişisel veri aktarımındaki temel işlevlerinden biri, veri alıcısının yükümlülüklerini açık ve bağlayıcı şekilde tanımlamak suretiyle, veri aktarımının her aşamasında hukuka uygunluğu sağlamaktır[418]. Özellikle büyük teknoloji sağlayıcıları, örneğin Microsoft[419] ve AWS[420] gibi şirketler, bu yükümlülükleri sözleşmelerine dahil ederek, veri güvenliğini sağlamak adına hangi teknik ve idari tedbirleri alacaklarını taahhüt etmektedirler. Ancak, veri aktarım sürecinde veri aktaranın da kendi sorumluluğu bulunmaktadır; yani veri aktarırken uygun güvenlik önlemleri alması gerekmektedir[421]. Bu nedenle, veri aktarımında hem veri aktaranın hem de veri alıcısının sorumlulukları net bir şekilde tanımlanmalı ve sözleşmeye yansıtılmalıdır. Bununla birlikte, veri aktarımlarında veri aktaranın teknik ve idari tedbirlerle ilgili sorumluluğu, genel görüşe göre veri işleyenlere yapılan aktarımlarda daha çok devreye girmektedir[422]. Bu, aktarılan verilerin işlenme sürecindeki güvenlik önlemlerinin, veri alıcısının işleme faaliyetleri sırasında uyguladığı tedbirlerle uyumlu olması gerektiğini ifade eder. Ancak, bu konu özellikle Ek-2 ve Ek-3 gibi belgelerde daha fazla belirsizlik yaratmaktadır[423]. Bu belgelerin nasıl doldurulacağına dair açık bir rehberin bulunmaması, uygulama açısından zorluklar yaratabilmektedir. Bu noktada, kişisel verilerin korunmasına dair kurumsal rehberlerin ve örneklerin yayımlanması,

---

[417] Kişisel Verileri Koruma Kurumu, Kişisel Verilerin Yurt Dışına Aktarılmasında Kullanılacak Standart Sözleşme–1 (Veri Sorumlusundan Veri Sorumlusuna), m. 7/7-b, https://www.kvkk.gov.tr/Icerik/8000/Standart-Sozlesmeler, (Erişim: 19.05.2025).

[418] Kişisel Verileri Koruma Kurumu, Kişisel Verilerin Yurt Dışına Aktarılmasında Kullanılacak Standart Sözleşme–1 (Veri Sorumlusundan Veri Sorumlusuna), m. 7/7, https://www.kvkk.gov.tr/Icerik/8000/Standart-Sozlesmeler, (Erişim: 19.05.2025).

[419] Microsoft, "Veri Güvenliği ve Gizlilik Politikası," 2023, https://www.microsoft.com/en-us/trust-center. (E.T:25.04.2025)

[420] AWS, "Veri Güvenliği ve Gizlilik," 2023, https://aws.amazon.com/compliance/data-privacy/, (E.T:25.04.2025).

[421] Bu husus kurulun yayınladığı standart sözleşmelerde açıkça gözükmektedir. Örneğin bknz. Kişisel Verileri Koruma Kurumu, Kişisel Verilerin Yurt Dışına Aktarılmasında Kullanılacak Standart Sözleşme–1 (Veri Sorumlusundan Veri Sorumlusuna), m. 7/5, https://www.kvkk.gov.tr/Icerik/8000/Standart-Sozlesmeler, (E. T: 19.05.2025).

[422] Kişisel Verileri Koruma Kurumu, Kişisel Verilerin Yurt Dışına Aktarılmasında Kullanılacak Standart Sözleşme–1 (Veri Sorumlusundan Veri İşleyene), m. 7/6 veri güvenliği, https://www.kvkk.gov.tr/Icerik/7931/Kisisel-Verilerin-Yurt-Disina-Aktarilmasinda-Kullanilacak-Standart-Sozlesme-2-Veri-Sorumlusundan-Veri-Isleyene-, (Erişim Tarihi: 19.05.2025).

[423] Veri Koruma Derneği, "Data Privacy Türkiye KVKK Standart Sözleşme Atölyesi- Veri Koruma Derneği Platform Toplantısı Çıktıları", *YouTube*, 13 Şubat 2024, https://www.youtube.com/watch?v=K-zdTpx2l3E, (E.T.: 17 Mayıs 2025).

bu belirsizliklerin ortadan kaldırılmasına katkı sağlayacaktır. Standart sözleşmeler aracılığıyla veri alıcısının yükümlülükleri netleştirilmiş olsa da kişisel verilerin yurt dışına aktarımına ilişkin düzenlemeler yalnızca KVKK ile sınırlı değildir. Zira, bazı durumlarda aktarımın hukuka uygunluğu, genel veri koruma mevzuatının yanı sıra sektörel veya konuya özgü düzenlemelerin hükümlerine de bağlıdır. Bu bağlamda, kişisel verilerin yurt dışına aktarılmasına dair uygulamalarda, özel kanunların hükümleri de dikkate alınmalıdır. Nitekim, 6698 sayılı Kanun'un 9. maddesi de yurt dışına veri aktarımında özel kanun hükümlerinin saklı olduğunu açıkça ifade etmektedir. Bu hüküm, özellikle bankacılık sektöründe, önceki dönemde bankacılık faaliyetlerine ilişkin düzenlemelerde açıkça yer almıştır. Bankacılık sektöründe, bankaların müşterilerinin kişisel verilerini yurt dışına aktarmaları durumunda, özel bir kanun hükmü bulunuyorsa, KVKK'nın genel hükümleri yerine o özel hükmün uygulanacağı belirtilmiştir[424]. Bu durum, bankacılık sektörüne yönelik düzenlemelerle uyumlu hale getirilmiş ve özellikle Swift işlemleri gibi uluslararası finansal işlemler için rahatlatıcı hükümler getirilmiştir[425]. Benzer bir yaklaşım, diğer regüle edilmiş sektörlerde de gündeme gelebilir. Örneğin, sigorta sektöründe veya sermaye piyasalarına tabi kurumlarda, özel bir kanun hükmü bulunması durumunda, kişisel verilerin yurt dışına aktarılması için standart sözleşme yapmadan veya arızi aktarıma gitmeden de bir çözüm yolu bulunabilir. Bu tür düzenlemeler, sektörel kararlar ve yetkili kurumlarla yapılacak görüşmelerle netlik kazanabilir.

Öte yandan, kişisel verilerin yurt dışına aktarımı yalnızca ulusal mevzuat çerçevesinde değil, aynı zamanda uluslararası düzenlemelerle karşılaştırmalı olarak da ele alınmalıdır. Bu bağlamda, veri aktarımlarının hukuki dayanağı açısından Türkiye'deki düzenlemelere paralel olarak, Avrupa Birliği Genel Veri Koruma Tüzüğü ile 6698 sayılı KVKK arasındaki farklılıklar da dikkatle değerlendirilmelidir. Bu farklar, uygulamada veri sorumlularının yükümlülüklerini yerine getirirken karşılaştıkları zorlukları ve uyum süreçlerindeki öncelikleri doğrudan etkilemektedir. KVKK'da, veri aktarılan üçüncü kişilerin veri işleyen olarak tanımlanmadığı durumlar mevcuttur[426]. GDPR' de ise, üçüncü kişiler, yani veri işleyenler ve veri sorumluları arasında belirgin bir ayrım bulunmaktadır. GDPR, yurt dışına yapılan veri aktarımına ilişkin hükümleri açıkça 44 ila 49. maddelerinde düzenlemektedir, ancak burada "üçüncü kişi"

[424] 5411 sayılı Bankacılık Kanunu, Kabul Tarihi: 19.10.2005, RG: 01.11.2005, Sayı: 25983 (m. 73/3).
[425] Kişisel Verilerin Korunmasına İlişkin Bankacılık Sektörü İyi Uygulamalar Rehberi, Kişisel Verileri Koruma Kurumu, Mart 2020, https://kvkk.gov.tr/SharedFolderServer/CMSFiles/12236bad-8de1-4c94-aad6-bb93f53271fb.pdf, (E.T. 20 Mayıs 2025).
[426] Daha fazla bilgi için bknz. Miray Özer Deniz, "Kişisel Verilerin İşlenmesinin Türleri ve Hukuki Nitelikleri" *Necmettin Erbakan Üniversitesi Hukuk Fakültesi Dergisi*, cilt:6, S. 1, 2023, s. 104-105.

kavramına yer verilmemektedir[427]. Bu nedenle, yurt dışına veri aktarımı sırasında, verinin aktarıldığı ülkenin veya uluslararası kuruluşların güvenliğini sağlamak için ayrı bir hukuki uygunluk sebebi aranmalıdır. Türkiye'de ise, özellikle veri işleyenler açısından, veri aktarımı sırasında veri sorumlusunun hukuki uygunluk sorumluluğu devam etmektedir.

Sonuç olarak, kişisel verilerin yurt dışına aktarımı hem hukuki hem de pratik boyutlarıyla kapsamlı ve çok katmanlı bir alan olarak karşımıza çıkmaktadır. Bu süreçte, standart sözleşmeler gibi araçlar, aktarımın hukuki zeminini oluştursa da bu araçların içeriği, uygulanışı ve özellikle sonraki aktarımlar, alt veri işleyen ilişkileri ve rücu hükümleri gibi konular uygulamada ciddi tartışmalara neden olmaktadır. Bunun yanı sıra, sözleşmelerin dili, imza prosedürleri, veri sorumlusu-veri işleyen ayrımı gibi teknik detaylar da aktarım süreçlerinin hukukiliğini doğrudan etkilemektedir. Özel nitelikli veriler, saklama süreleri ve sözleşmelerin açık rıza gerektirip gerektirmediği gibi konular da farklı yorumlara açık alanlar arasında yer almaktadır. KVKK ile GDPR arasında var olan yapısal farklılıklar ise, çok uluslu şirketlerin ve anonim ortaklıkların farklı yargı alanlarında uyum sağlama zorluklarını artırmaktadır. Bu noktada, yurt dışına kişisel veri aktarımına ilişkin hukuki düzenlemelerin ve uygulamaların netleştirilmesi, özellikle sektörel farklılıkların ve özel hükümlerin doğru bir şekilde ele alınması açısından büyük önem taşımaktadır. Bu alanda yapılan yorum farklılıkları, uygulamada büyük farklar yaratabilmekte; bu nedenle, kişisel verilerin korunması alanındaki düzenlemeler ve rehberlerin daha açık ve kapsamlı bir şekilde yayımlanması gerekmektedir. Gelecekte, özellikle bankacılık ve diğer regüle edilmiş sektörlerde, yurt dışına veri aktarımı konusunda daha esnek ve net düzenlemeler beklenmektedir. Böylece hem veri güvenliği sağlanacak hem de şirketlerin yasal uyum süreçleri daha etkin ve öngörülebilir hale gelecektir.

### B. Anonim Şirketlerde Standart Sözleşme Hazırlama ve Onay Süreci

Kurul tarafından 4 Haziran 2024 tarihinde kabul edilen standart sözleşmeler, yeterli korumanın bulunmadığı ülkelere veri aktarımı yapılabilmesi için veri sorumlularına uygun güvence sağlama imkânı tanımaktadır[428]. Anonim şirketler, ticari faaliyetleri kapsamında elde ettikleri kişisel verilerin yurt dışına aktarılması sürecinde, veri sorumlusu sıfatıyla hareket ettiklerinden, kanunun belirlediği yükümlülüklere eksiksiz şekilde riayet etmekle mükelleftirler. Kanunun 9. maddesi uyarınca kişisel veriler, yalnızca yeterlilik kararı bulunan ülkelere ya da uygun

[427]GDPR Resmi Metni (EU Regulation 2016/679), https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016R0679.
[428] Kişisel Verileri Koruma Kurulu, *"Yurt Dışına Veri Aktarımında Kullanılacak Standart Sözleşmelere İlişkin Duyuru",* 4 Haziran 2024, https://www.kvkk.gov.tr/Icerik/7929/Standart-Sozlesmeler. (E.T: 27.04.2025)

güvencelerin sağlandığı hâllerde ve Kişisel Verileri Koruma Kurulu'nun izniyle aktarılabilecektir. Kurul, 4 Haziran 2024 tarihinde kabul ettiği 2024/959 sayılı kararı ile standart sözleşmeler düzenleyerek, yeterli korumanın bulunmadığı ülkelere veri aktarımı sürecinde veri sorumlularına uygun güvence sağlama imkânı sunmuştur. Böylece, anonim şirketler bakımından, açık rıza alma veya bireysel izin prosedürüne başvurmaksızın yurt dışı veri aktarımı yapılmasının yolu açılmıştır.

Kurul tarafından yayımlanan standart sözleşmeler, aktarım ilişkisinin taraflarına göre *"veri sorumlusundan veri sorumlusuna", "veri sorumlusundan veri işleyene", "veri işleyenden veri işleyene"* ve *"veri işleyenden veri sorumlusuna"* olmak üzere dört temel kategoriye ayrılmıştır[429]. Anonim şirketlerin, yurt dışına veri aktarımında bulunacakları tarafın hukuki statüsüne uygun olarak bu modellerden birini seçmeleri ve ilgili standart sözleşmeyi düzenlemeleri gerekmektedir[430]. Sözleşmelerde aktarılacak kişisel veri kategorileri, aktarımın amaçları, veri alıcısının yükümlülükleri ile alınacak teknik ve idari tedbirler ayrıntılı biçimde belirtilmelidir. Standart sözleşmenin hazırlanması sürecinde, aktarılacak verilerin niteliği, tarafların kimlik bilgileri ve veri güvenliğine ilişkin önlemler açıkça tanımlanmalıdır. Bu aşamada, KVKK'nın 12. maddesinde öngörülen teknik ve idari tedbirlerin sözleşmede somut şekilde düzenlenmesi büyük önem taşımaktadır. Zira, veri sorumluları kişisel verilerin hukuka aykırı işlenmesini ve erişilmesini önlemek, verilerin güvenliğini sağlamak amacıyla gerekli her türlü teknik ve idari tedbiri almakla yükümlüdür. Bu kapsamda, şifreleme yöntemlerinin kullanılması, erişim kontrollerinin sağlanması, sistem güvenliğinin temin edilmesi gibi teknik tedbirler ile veri güvenliği politikalarının oluşturulması, çalışanların eğitilmesi gibi idari tedbirlerin alınması gerekmektedir[431].

Sözleşmenin imzalanmasını müteakip, veri sorumlusu anonim şirketin, standart sözleşmeyi Kurul'a en geç beş iş günü içinde bildirmesi zorunludur[432]. Bildirimin eksiksiz ve doğru şekilde yapılması, aktarım sürecinin hukuka uygun yürütülmesi açısından kritik bir öneme sahiptir. Aksi hâlde, kişisel verilerin yurt dışına aktarılması hukuka aykırı hâle gelecek ve KVKK'nın

---

[429] Kişisel Verileri Koruma Kurulu, "Kişisel Verilerin Yurt Dışına Aktarılması Rehberi", Mart 2024, https://www.kvkk.gov.tr/Icerik/8142/Kisisel-Verilerin-Yurt-Disina-Aktarilmasi-Rehberi, (Erişim Tarihi: 27 Nisan 2025).

[430] Arzu Galandarlı, "KVKK ve GDPR: Standart Sözleşme Maddeleri Arasındaki Farklar", Hukuk ve Bilişim Dergisi, 21. Sayı, 2 Ocak 2025, https://www.hukukvebilisimdergisi.com/kvkk-ve-gdpr-standart-sozlesme-maddeleri-arasindaki-farklar/, (E.T.: 21.05.2025)

[431] Kişisel Verileri Koruma Kurumu, *Kişisel Veri Güvenliği Rehberi (Teknik ve İdari Tedbirler)*, 2018, s. 5-7, https://www.kvkk.gov.tr/SharedFolderServer/CMSFiles/7512d0d4-f345-41cb-bc5b-8d5cf125e3a1.pdf, (Erişim Tarihi: 20 Mayıs 2025).

[432] Kişisel Verileri Koruma Kurulu, "Bildirim Usul ve Esasları", https://www.kvkk.gov.tr/Icerik/8355/Standart-Sozlesme-Bildirim-Usul-ve-Esaslari, (Erişim Tarihi: 27 Nisan 2025).

18. maddesinde düzenlenen idari para cezaları ile karşılaşılabilecektir. Bunun yanı sıra, teknik ve idari tedbirlerin eksik veya yetersiz alınması da veri sorumlusunun doğrudan sorumluluğunu doğurmaktadır. Bu tür ihlaller sonucunda, yalnızca idari para cezası verilmekle kalınmayacak, aynı zamanda ilgili kişilerin uğradığı zararların tazmini yoluyla hukuki sorumluluk[433] da gündeme gelecektir[434]. Türk Borçlar Kanunu'nun 49. maddesi uyarınca, kişisel veri ihlallerinden kaynaklanan zararlar sebebiyle anonim şirket aleyhine maddi ve manevi tazminat davalarının açılması mümkündür[435]. Kurul da re' sen harekete geçerek veri aktarımını durdurabilir veya diğer idari tedbirleri uygulayabilir[436].

Sonuç olarak, anonim şirketler yurt dışına veri aktarımı sürecinde yalnızca standart sözleşmeleri düzenlemekle yetinmemeli; aynı zamanda, teknik ve idari güvenlik tedbirlerini etkin şekilde uygulayarak veri koruma yükümlülüklerini bütüncül bir şekilde yerine getirmelidirler. (Teknik ve idari tedbirler ile veri güvenliğinin sağlanmasına ilişkin detaylı açıklamalara üçüncü başlıkta ayrıca yer verilecektir). Bu hususlar, yalnızca hukuki sorumluluğun sınırlandırılması açısından değil, aynı zamanda şirketin itibarının korunması ve veri sahiplerinin temel hak ve özgürlüklerinin güvence altına alınması bakımından da hayati önem taşımaktadır. Anonim şirketlerin standart sözleşme hazırlarken, veri aktarımının niteliğine ve karşı tarafın konumuna (veri sorumlusu veya veri işleyen) göre bu modellerden uygun olanını tercih etmeleri gerekmektedir. Özellikle uluslararası ticari ilişkiler, yurtdışı merkezli grup şirketleriyle veri paylaşımı veya bulut bilişim hizmetlerinin kullanımı gibi durumlarda, aktarım modeli büyük önem arz etmektedir.

### C. Anonim Şirketlerce Yurt Dışına Veri Aktarımında Alınması Gereken İdari ve Teknik Tedbirler

6698 sayılı Kişisel Verilerin Korunması Kanunu'nun 9. maddesi uyarınca kişisel verilerin yurt dışına aktarımı, veri güvenliğinin sağlanması amacıyla belirli hukuki mekanizmalara bağlanmıştır. Bu kapsamda, özellikle anonim şirketlerin veri aktarım süreçlerinde standart sözleşmeler önemli bir araç olarak öne çıkmaktadır. Standart sözleşmeler ve açık rıza gibi

[433] Yargıtay 4. HD, 13.12.2017, E. 2016/2970, K. 2017/8273. Yargıtay, bu kararında, kişisel verilere izinsiz erişimin Türk Borçlar Kanunu'nun 58. maddesi kapsamında kişilik haklarının ihlali olduğunu ve manevi tazminat gerektirdiğini vurgulamıştır. Bu karar, kişisel verilerin korunması ve özel hayatın gizliliği ilkelerinin ihlali durumunda manevi tazminat talebinin mümkün olduğunu göstermektedir.
[434] KVKK Madde 14/3: "Kişilik hakları ihlal edilenlerin, genel hükümlere göre tazminat hakları saklıdır."
[435] Türk Borçlar Kanunu, 6098, Resmî Gazete: 4 Şubat 2011/27836, m. 49.
[436] Kişisel Verileri Koruma Kurulu, 6698 sayılı Kişisel Verilerin Korunması Kanunu'nun 15. maddesi uyarınca, telafisi güç veya imkânsız zararların doğma ihtimali ve açıkça hukuka aykırılık durumlarında re' sen harekete geçerek veri işlenmesini veya yurt dışına veri aktarımını durdurma yetkisine sahiptir.

hukuki dayanaklar, veri aktarımının güvenli ve yasal bir şekilde yapılabilmesi için kritik öneme sahiptir[437]. Kişisel veri aktarım süreçlerinde yalnızca açık rızaya dayanmaksızın, uygun güvenceler sağlamakla yükümlü tutulan anonim şirketler bu sözleşmelerin içeriğinde veri aktarımının amacı, işleme çerçevesi, saklama süreleri, sonraki aktarımlar ve güvenlik önlemleri gibi hükümlere yer vermek zorundadır[438].

Veri sorumlusu anonim şirket hem kendi faaliyetlerinde hem de veri alıcısının faaliyetlerinde, KVKK'nın 12. maddesi uyarınca gerekli idari ve teknik tedbirleri almakla mükelleftir. Kişisel Verileri Koruma Kurulu'nun 2020/966 sayılı kararında vurgulandığı üzere, yalnızca sözleşmesel taahhütler yeterli görülmemekte; şifreleme, erişim kontrolü, sızma testleri gibi teknik uygulamaların fiilen hayata geçirilmesi beklenmektedir[439]. Ayrıca, veri aktarımı yapılan ülkenin veri koruma seviyesinin de dikkate alınması beklenmektedir.

Avrupa Birliği Genel Veri Koruma Tüzüğü'nde öngörülen "Transfer Impact Assessment" (TIA) benzeri bir değerlendirme yaklaşımı, Kurul tarafından 2022/924 sayılı kararında dolaylı biçimde vurgulanmış, yurt dışı aktarım süreçlerinde risk değerlendirmesi yapılmasının gerekli olduğu belirtilmiştir[440] Standart sözleşmeye dayalı veri aktarımlarında, veri sahiplerinin bilgilendirilmesi de ayrı bir yükümlülük olup, KVKK'nın 10. maddesi uyarınca, ilgili kişilere verilerin hangi ülkeye, kimlere ve hangi hukuki sebeple aktarılacağı konusunda açık bir aydınlatmanın yapılması zorunludur. Kurul'un 2023/924 sayılı kararında, veri sorumlusu otopark işletmecesinin aydınlatma yükümlülüğünün yerine getirilmemesi nedeniyle veri sorumlusuna 75.000 lira idari para cezası uygulanmıştır[441]. Anonim şirketler açısından, standart sözleşmelere dayalı veri aktarımı sürecinde hukuki, idari ve cezai sorumluluklar doğmaktadır. Veri sorumlusu şirket, kişisel verilerin hukuka aykırı işlenmesi veya aktarılması halinde ilgili kişilere karşı tazminat sorumluluğu ile karşılaşabileceği gibi, aynı zamanda Türk Ceza Kanunu'nun 136. maddesi uyarınca cezai sorumluluk da üstlenebilir. Kemal Gözler 'in de

[437] Kişisel Verileri Koruma Kurulu, "Kişisel Verilerin Yurt Dışına Aktarılmasında Kullanılacak Standart Sözleşme- 2 (Veri Sorumlusundan Veri İşleyene)".
[438] 6698 sayılı Kişisel Verilerin Korunması Kanunu, m. 9.
[439]Kişisel Verileri Koruma Kurulu, 22.12.2020 tarih ve 2020/966 sayılı Kararı, https://www.kvkk.gov.tr/Icerik/6858/2020-966, (E.T:27.04.2025).
[440] Kişisel Verileri Koruma Kurulu, 08.09.2022 tarih ve 2022/924 Sayılı Kararı, (E.T:27.04.2025).
Özet: Kurul, küresel bir otel zincirinin Türkiye'deki kullanıcılarının verilerini yurt dışına hukuka aykırı bir şekilde aktarması nedeniyle 1.800.000 TL idari para cezası uygulamıştır. Bu karar, yurt dışına veri aktarımında idarenin ortaya çıkardığı belirsizliği ve Kurul'un zorunlu açık rıza yaklaşımını anlamak bakımından önemli bir örnektir. https://dergipark.org.tr/tr/download/article-file/3019992#:~:text=Kişisel%20Verileri%20Koruma%20Kurulu%2C%20incelememize,TL%20idari%20para%20cezası%20uygulamıştır, (E.T:27.04.2025).
[441]Kişisel Verileri Koruma Kurulu, 01.06.2023 tarih ve 2023/924 Sayılı Kararı, (E.T:27.04.2025). https://kvkk.gov.tr/Icerik/7763/2023-924, (E.T:27.04.2025).

belirttiği gibi, *"idare veya özel hukuk kişileri hukukla bağlı oldukları sürece, özgürlük alanları genişler; aksi takdirde sorumluluk kaçınılmaz olur*[442]*"*. Bu kapsamda, şirketlerin standart sözleşmelerin içeriğini belirlerken sadece formal unsurları değil, gerçek koruma mekanizmalarını da tesis etmeleri hukuki bir zorunluluktur. Özellikle çok uluslu şirketlerde, grup içi veri aktarımlarında farklı ülke mevzuatlarına uyum gerekliliği nedeniyle standart sözleşmelerin basitleştirilmiş ve uyumlaştırılmış yapılarla yeniden düzenlenmesi önem arz etmektedir. Ancak sözleşmelerin aşırı farklılaşması durumunda, Kanun'un 9. maddesinin işlevselliği zayıflayabileceğinden, Kurul tarafından belirlenen standart çerçeve hükümlerine sadık kalınması tavsiye edilmektedir. Nitekim KVKK'nın 12. maddesi, kişisel verilerin hukuka aykırı işlenmesini ve erişilmesini önlemek, kişisel verilerin muhafazasını temin etmek amacıyla uygun güvenlik düzeyini sağlayacak tedbirlerin alınmasını veri sorumlularının asli görevleri arasında saymıştır[443].

Kurul kararlarında da şifreleme yapılmaksızın veri aktarımı gerçekleştiren veri sorumlularına idari para cezaları verildiği görülmektedir[444]. Bununla birlikte, sızma testlerinin düzenli olarak yapılması, veri maskeleme tekniklerinin kullanılması ve aktarım sonrasında verilerin geri getirilemeyecek şekilde imha edilmesi de teknik güvenlik kapsamında anonim şirketlerin yerine getirmesi gereken yükümlülüklerdendir[445]. Bu yükümlülüklerin somutlaştırılması amacıyla Kişisel Verileri Koruma Kurulu, "Veri Güvenliği Rehberi'ni" yayımlamış ve alınması gereken idari ve teknik tedbirleri detaylı şekilde açıklamıştır[446]. İdari tedbirler çerçevesinde ise, şirketlerin kapsamlı bir kişisel veri işleme politikası oluşturması, çalışanlara düzenli olarak kişisel veri koruma eğitimleri vermesi ve veri aktarımı yapılan üçüncü taraflarla yapılacak sözleşmelere özel güvenlik hükümleri eklemesi zorunludur[447]. Kurul'un çeşitli kararlarında, çalışan eğitimlerinin eksik olması veri ihlallerinin temel nedenlerinden biri olarak gösterilmiştir[448]. Öte yandan, standart sözleşme kapsamında yapılan veri aktarımlarında, ilgili kişilere aktarımın hukuki dayanağı, verilerin hangi ülkeye ve kimlere aktarılacağı gibi bilgilerin

---

[442] Kemal Gözler. *Türkiye Hukuk Ansiklopedisi (TÜHA),* Cilt 3, "Sorumluluk" md., s. 422-423.
[443] 6698 sayılı Kişisel Verilerin Korunması Kanunu, m. 12, RG, 7.4.2016, S. 29677.
[444] KVK Kurulu, 2020/915 sayılı Kararı, https://www.kvkk.gov.tr/Icerik/6872/2020-915, (Erişim Tarihi: 27 Nisan 2025).
[445] KVK Kurulu, 11 Mart 2021 tarihli, 2021/238 sayılı Kararı, https://www.kvkk.gov.tr/Icerik/6903/VERBIS-E-KAYIT-SURELERININ-UZATILMASI-HAKKINDA-DUYURU, 27.08.2019 tarih ve 2019/255 sayılı Kararı, https://www.kvkk.gov.tr/Icerik/5537/2019-255.
[446]Kişisel Verileri Koruma Kurulu, "Veri Güvenliği Rehberi (Teknik ve İdari Tedbirler)", 2019, https://www.kvkk.gov.tr/Icerik/6633/Veri-Guvenligi-Rehberi, (Erişim Tarihi: 27 Nisan 2025).
[447] Kişisel Verileri Koruma Kurulu, "İdari ve Teknik Tedbirler Rehberi", 2021.
[448] KVK Kurulu, 23 Temmuz 2019 tarihli, 2019/225 sayılı Kararı, https://www.kvkk.gov.tr/Icerik/5545/2019-225.

bildirilmesi, aydınlatma yükümlülüğü kapsamında zorunlu tutulmuştur[449]. Bu yükümlülüğün ihlali, idari para cezalarına yol açabileceği gibi, veri ihlali halinde veri sorumlusunun hukuki, idari ve cezai sorumluluğu da doğurabilecektir.

Hukuki sorumluluk bağlamında, veri sorumlusu şirket, kişisel verilerin hukuka aykırı işlenmesi veya aktarılması nedeniyle zarar gören ilgili kişilere karşı maddi ve manevi tazminat ödemek zorunda kalabilir[450].

İdari sorumluluk kapsamında ise, Kurul tarafından öngörülen bildirim ve bilgilendirme yükümlülüklerine uyulmaması halinde idari para cezaları uygulanabilecektir[451]. Ayrıca, kişisel verilerin hukuka aykırı olarak kaydedilmesi veya aktarılması gibi eylemler, Türk Ceza Kanunu hükümleri uyarınca cezai sorumluluğu da gündeme getirebilir[452].

Teknik tedbirler kapsamında anonim şirketler öncelikle yetki matrisi oluşturarak kişisel verilere yalnızca iş tanımı gereği ihtiyaç duyan personelin erişimini sağlamalıdır[453].Ayrıca veri aktarımı sırasında verilerin güvenliğini sağlamak için şifreleme yöntemleri kullanılmalı ve etkin anahtar yönetim süreçleri oluşturulmalıdır. Kurul, şifreleme yapılmaksızın kişisel verilerin elektronik ortamda paylaşılması sebebiyle uyguladığı idari para cezalarıyla bu tedbirin önemine işaret etmiştir[454]. Bunun yanı sıra erişim, değiştirme ve silme işlemlerinin kayıt altına alınması, düzenli log takibi yapılması ve bu kayıtların güvenliğinin sağlanması gerekmektedir. Veri aktarımı süreçlerinde ağ güvenliğinin sağlanması adına firewall ve saldırı tespit sistemleri kurulmalı; ayrıca sızma testleri düzenli olarak gerçekleştirilmelidir. Gerekli durumlarda veri

[449] KVK Kurulu, Amazon Turkey Perakende Hizmetleri Limited Şirketi hakkındaki başvuru ile ilgili Kişisel Verileri Koruma Kurulunun 27/02/2020 Tarihli ve 2020/173 Sayılı Kararı. https://www.kvkk.gov.tr/Icerik/6739/2020-173, (Erişim Tarihi: 27 Nisan 2025).

[450] Yargıtay 4. HD, 14.03.2019, E. 2019/979, K. 2019/2679. Bu kararda, bir anonim şirket olan telekomünikasyon şirketinin bayisi, davacının kimlik bilgilerini kullanarak rızası dışında hat çıkarmış ve bu hat üzerinden borçlandırma yapılmıştır. Yargıtay, şirketin bayisini seçme ve denetleme yükümlülüğünü yerine getirmediğini belirterek, şirketin manevi tazminat ödemesine hükmetmiştir. https://www.lexpera.com.tr/ictihat/yargitay/4-hukuk-dairesi-e-2019-979-k-2019-2679-t-8-5-2019, (E.T.: 19/05/2025).

[451] KVK Kurulu,13/02/2020 tarihli, 2020/124 sayılı Kararı.
Bu karar, veri sorumlularının, çalışanlarının kişisel verilere erişimini kontrol altına alacak teknik ve idari tedbirleri uygulamalarının önemini vurgulamaktadır. Ayrıca, çalışanların görevlerini kötüye kullanarak kişisel verileri hukuka aykırı işlemesini önlemek için gerekli önlemlerin alınması gerektiğini ortaya koymaktadır. (Erişim Tarihi: 27 Nisan 2025).

[452] Türk Ceza Kanunu, m.135-140.

[453] Kişisel Verileri Koruma Kurulu, "Veri Güvenliği Rehberi", s. 11-12.

[454] Kişisel Verileri Koruma Kurulu Kararı, 25/03/2021 tarih ve 2021/311 sayılı Kararı. Bu karar, kişisel verilerin güvenliğinin sağlanmasında şifreleme ve etkin anahtar yönetimi gibi teknik ve idari tedbirlerin önemini vurgulamaktadır. Veri sorumlularının, kişisel verilerin işlenmesi ve aktarılması süreçlerinde bu tür tedbirleri almamaları durumunda ciddi idari yaptırımlarla karşılaşabilecekleri unutulmamalıdır. https://www.kvkk.gov.tr/Icerik/7001/2021-311, (Erişim Tarihi: 27 Nisan 2025).

maskeleme yöntemleri uygulanmalı ve veri aktarımı sona erdiğinde verilerin geri alınamayacak şekilde imha edilmesi sağlanmalıdır[455].

İdari tedbirler bakımından ise, anonim şirketlerin kişisel veri işleme faaliyetlerini kapsayan açık ve şeffaf veri işleme politikaları oluşturması büyük önem arz etmektedir[456]. Çalışanlara yönelik düzenli eğitim programları düzenlenmeli, veri koruma bilincinin tüm organizasyona yayılması sağlanmalıdır. Kurul'un bir kararında çalışanlara gerekli eğitimlerin verilmemesinin veri ihlallerini artıran bir unsur olarak değerlendirildiği göz önüne alındığında[457], eğitim faaliyetlerinin önemi daha iyi anlaşılmaktadır. Ayrıca, üçüncü taraflarla yapılacak veri aktarımı sözleşmelerine veri güvenliğine ilişkin özel hükümler konulmalı ve aktarım yapılan tarafların da benzer koruma standartlarına riayet etmesi sağlanmalıdır[458]. Yurt dışına veri aktarımı öncesinde ise risk analizi yapılmalı ve özellikle hassas kişisel verilerin aktarımı durumunda veri koruma etki değerlendirmeleri hazırlanmalıdır. Kurul'un 2022/249 sayılı kararında bu yükümlülüğü yerine getirmeyen veri sorumlularına idari yaptırımlar uyguladığı görülmektedir[459].

Son olarak, kişisel veri ihlallerinin etkin şekilde yönetilebilmesi için önceden belirlenmiş ihlal müdahale planları hazırlanmalı ve olası bir ihlal durumunda ilgili veri sahiplerine ve Kurul'a yapılacak bildirim prosedürleri önceden belirlenmelidir[460]. Bu çerçevede, anonim şirketlerin yurt dışına veri aktarımı süreçlerinde yalnızca hukuki metinlerin hazırlanmasıyla yetinmeyip, teknik ve idari güvenlik tedbirlerini bütüncül bir yaklaşımla uygulamaları; KVKK'ya uyumluluğun sağlanması ve olası idari yaptırımlardan kaçınılması bakımından elzemdir.

---

[455] Zeynep Yürük, "Veri Sorumlusunun Veri Güvenliğine İlişkin İdari ve Teknik Tedbirleri Alma Yükümlülüğü", *İstanbul Ticaret Üniversitesi Sosyal Bilimler Dergisi*, C. 22, S. 48, 2023, s. 899-920, https://doi.org/10.46928/iticusbe.1218693, (E.T. 20.05.2025).

[456] Kişisel Verileri Koruma Kurulu, "Veri Güvenliği Rehberi", s. 9-20.

[457] Kişisel Verileri Koruma Kurulu Kararı, 01/12/2020 tarih ve 2020/915 sayılı Karar, https://www.kvkk.gov.tr/Icerik/6872/2020-915, (Erişim Tarihi: 27 Nisan 2025).

[458] Kişisel Verileri Koruma Kurulu, "Yurt Dışına Veri Aktarımı Standart Sözleşmeleri", https://www.kvkk.gov.tr/Icerik/7929/Standart-Sozlesmeler (Erişim Tarihi: 27 Nisan 2025).

[459] Kişisel Verileri Koruma Kurulu Kararı, 17/03/2022 tarih ve 2022/249 sayılı Kararı.
Bu karar, veri sorumlularının özel nitelikli kişisel verilerin aktarımı gibi yüksek riskli işlemler öncesinde VKED hazırlamalarının önemini vurgulamaktadır. Ayrıca, veri güvenliğini sağlamak için gerekli teknik ve idari tedbirlerin alınmaması durumunda ciddi idari yaptırımların uygulanabileceğini göstermektedir. https://www.kvkk.gov.tr/Icerik/7558/2022-249, (Erişim Tarihi: 09 Mayıs 2025).

[460] Kişisel Verileri Koruma Kurulu, "Veri İhlali Bildirimi Usul ve Esasları", https://www.kvkk.gov.tr/Icerik/6787/Veri-Ihlali-Bildirimi, (Erişim Tarihi: 27 Nisan 2025).

### D. Standart Sözleşmeler Çerçevesinde Anonim Şirketin Yükümlülükleri ve Sorumluluğu

6698 sayılı Kişisel Verilerin Korunması Kanunu uyarınca veri sorumluları, kişisel verilerin işlenmesi ve özellikle yurt dışına aktarılması süreçlerinde birtakım yükümlülüklere tabidir. Bu yükümlülükler yalnızca hukuka uygunluk sağlamakla sınırlı olmayıp, kişisel verilerin korunmasına ilişkin temel ilkelere ve ilgili kişilerin haklarına saygı gösterilmesi bakımından da büyük önem arz etmektedir. KVKK'nın 9. maddesinde yapılan değişiklikler neticesinde, kişisel verilerin yurt dışına aktarılmasında, yeterlilik kararı bulunmayan ülkelere veri aktarımı bakımından standart sözleşme mekanizması temel araçlardan biri olarak düzenlenmiş ve böylece anonim şirketlerin bu süreçteki sorumlulukları daha da somutlaşmıştır[461]. Bu çerçevede anonim şirketler, kişisel verilerin yurt dışına aktarımını gerçekleştirmeden önce, aktarım yapılacak ülkenin kişisel verilerin korunması bakımından yeterli bir koruma düzeyine sahip olup olmadığını değerlendirmek ve yeterli koruma bulunmadığı durumlarda Kanun'da öngörülen güvencelere uygun hareket etmekle yükümlüdürler[462]. Anonim şirketlerin bu süreçte öncelikli olarak kişisel verileri yurt dışına aktarırken ilgili kişileri aydınlatmaları zorunlu olup, aydınlatmanın içeriğinde aktarımın dayandığı hukuki sebep, aktarımın yapılacağı ülke veya ülke grubu, veri alıcıları ve aktarım amacı gibi hususlara açık ve anlaşılır bir şekilde yer verilmesi gerekmektedir[463]. Özellikle standart sözleşmeye dayalı aktarımlar bakımından, bu durumun aydınlatma metinlerinde açıkça belirtilmesi ve ilgili kişilerin bilgilendirilmesi ayrıca önem arz etmektedir. Bunun yanı sıra, anonim şirketlerin ilgili kişiler tarafından yapılan başvuruları etkin şekilde cevaplama yükümlülüğü de bulunmaktadır. KVKK'nın 11. ve 13. maddeleri çerçevesinde, ilgili kişiler veri işleme faaliyetleri hakkında bilgi talebinde bulunabilir ve anonim şirketler bu başvurulara en geç otuz gün içinde cevap vermekle yükümlüdürler. İlgili kişilerin taleplerine zamanında ve doğru şekilde cevap verilmemesi halinde Kurul tarafından idari yaptırımlar uygulanabilecektir.

Standart sözleşme hükümleri çerçevesinde gerçekleştirilecek veri aktarımlarında, taraflarca imzalanan sözleşmenin yürürlüğe girmesinden itibaren en geç beş iş günü içinde Kişisel Verileri Koruma Kurulu'na bildirimde bulunulması zorunludur[464]. Bu bildirimin hem veri

---

[461] KVKK m.9/2 ve 14.09.2023 tarihli ve 2023/1578 sayılı Kurul Kararı. https://www.kvkkarar.com/?_sft_kanun_maddesi=kvkk-madde-09, (Erişim Tarihi:27.04.2025).

[462] KVKK, https://www.kvkk.gov.tr/Icerik/8142/Kisisel-Verilerin-Yurt-Disina-Aktarilmasi-Rehberi, (Erişim Tarihi:27.04.2025).

[463] KVKK m.10; Aydınlatma Yükümlülüğü Tebliği, m.4., https://www.kvkk.gov.tr/Icerik/4108/Aydinlatma-Yukumlulugunun-Yerine-Getirilmesinde-Uyulacak-Usul-ve-Esaslar-Hakkinda-Teblig-Resmi-Gazetede-yayinlanmistir, (Erişim Tarihi:27.04.2025).

[464] KVKK m.9/5; Standart Sözleşme Duyurusu, 2024.

gönderici hem de veri alıcı tarafından yapılması gerekmekte olup, söz konusu yükümlülüğün ihlali halinde idari yaptırımlarla karşılaşılması söz konusu olabilecektir[465]. Standart sözleşmenin, Kurul tarafından yayımlanan haliyle kullanılmadan üzerinde herhangi bir değişiklik yapılması durumunda ise veri sorumlularının taahhütname alma sürecini işletmeleri gerekecektir[466]. Ayrıca, veri aktarımına başlanmadan önce, anonim şirketlerin kapsamlı bir aktarım etki değerlendirmesi gerçekleştirmeleri de büyük önem taşımaktadır. Bu değerlendirme sürecinde, aktarım yapılacak ülkenin veri koruma seviyesi, potansiyel riskler ve bu risklere karşı alınması gereken teknik ve idari tedbirler detaylı bir biçimde analiz edilmelidir[467]. Böylece alınacak önlemlerin, aktarımın güvenliğini temin edecek düzeyde olup olmadığı objektif ölçütler çerçevesinde belirlenebilecektir.

Anonim şirketlerin ayrıca, Kişisel Verileri Koruma Kurulu tarafından oluşturulan Veri Sorumluları Sicili Bilgi Sistemi'ne ("VERBİS") kayıt yükümlülükleri kapsamında, yurt dışına veri aktarımı gerçekleştirdiklerini de doğru ve güncel şekilde bildirmeleri gerekmektedir[468]. Bu bildirimin, standart sözleşmeye dayalı aktarım yapmadan önce tamamlanması, veri işleme faaliyetlerinde şeffaflık ilkesinin sağlanması açısından zorunludur. Ayrıca, üst başlıkta açıkladığımız üzere KVKK'nın 12. maddesi kapsamında veri güvenliğine ilişkin gerekli tüm teknik ve idari tedbirlerin alınması sorumluluğu da anonim şirketlerin üzerinde bulunmaktadır. Bu kapsamda, şifreleme, yetki sınırlamaları, erişim kontrolleri, loglama ve veri maskeleme gibi teknik önlemler ile, kişisel veri güvenliğine ilişkin politika ve prosedürlerin oluşturulması gibi idari düzenlemelerin eksiksiz biçimde hayata geçirilmesi gerekmektedir[469]. Ayrıca, kişisel verilerin saklanması ve imhası süreçlerine ilişkin olarak anonim şirketlerin bir kişisel veri saklama ve imha politikası hazırlamaları ve bu politikaya uygun şekilde kişisel verilerin silinmesi, yok edilmesi veya anonim hale getirilmesi yükümlülüğünü yerine getirmeleri zorunludur[470]. Standart sözleşme metinleri de taraflara belirli güvenlik önlemlerini alma ve sürdürme yükümlülüğü yüklemekte olup, bu yükümlülüğün ihlali durumunda hem hukuki hem de cezai sorumluluk doğabilecektir[471]. İlaveten, anonim şirketlerin, kişisel veri sahiplerinin KVKK'nın 11. maddesinde düzenlenen haklarının kullanılmasını temin etmeleri gerekmektedir[472]. Bu nedenle, standart sözleşmelerde veri alıcısının ilgili kişilerin haklarına

[465] KVKK m.18.
[466] Kişisel Verileri Koruma Kurulu, Standart Sözleşmeler Hakkında Kamuoyu Duyurusu, 2024.
[467] Avrupa Veri Koruma Kurulu ("EDPB") Aktarım Etki Değerlendirmeleri Rehberi, 2021.
[468] VERBİS Kılavuzu, KVK Kurulu, 2022.
[469] KVKK m.12; Kişisel Veri Güvenliği Rehberi, 2020
[470] Kişisel Veri Saklama ve İmha Politikası Hazırlama Rehberi, KVK Kurumu, 2018.
[471] KVKK, m. 12 ve Standart Sözleşme Örneği (KVK Kurumu 2024).
[472] KVKK m.11.

saygı göstereceğine dair açık taahhütlerin bulunması önem arz etmektedir. İlgili kişiler, kişisel verilerinin işlenip işlenmediğini öğrenme, verilerin amacına uygun kullanılıp kullanılmadığını sorgulama, eksik veya yanlış işlenmiş verilerin düzeltilmesini talep etme, işlenmesini gerektiren sebeplerin ortadan kalkması halinde verilerin silinmesini veya yok edilmesini isteme ve işlenmesine itiraz etme gibi haklara sahiptirler. Bu nedenle, standart sözleşmelerde veri alıcısının ilgili kişilerin haklarına saygı göstereceğine dair açık taahhütlerin bulunması önem arz etmektedir. Ayrıca, anonim şirketlerin sorumluluğu yalnızca ilk veri aktarımı ile sınırlı kalmamakta, veri alıcısının kişisel verileri üçüncü kişilere aktarımı gibi sonraki aktarım işlemlerinde de devam etmektedir. Bu bağlamda, sonraki aktarımlara ilişkin olarak sözleşmeye özel düzenlemeler eklenmeli, veri alıcısının verileri yalnızca belirlenen amaçlar doğrultusunda işlemesi ve üçüncü kişilere aktarım yapmaması güvence altına alınmalıdır. Gerekli görülmesi halinde, veri alıcılarının düzenli raporlamalar yapması ve anonim şirketin yerinde denetim hakkını saklı tutması da veri aktarım zincirinde güvenliğin sürdürülebilirliğini sağlamak bakımından önemli bir tedbir olarak değerlendirilmelidir[473].

Sonuç olarak, KVKK uyarınca anonim şirketlerin yurt dışına kişisel veri aktarımı süreçlerindeki yükümlülükleri, yalnızca veri transferinin gerçekleştirilmesi aşamasıyla sınırlı olmayıp, aktarımın tüm aşamalarında devam eden kapsamlı bir gözetim ve denetim sorumluluğunu da içermektedir. Bu süreçte standart sözleşmeler, anonim şirketler açısından yalnızca veri aktarımına aracılık eden bir belge değil, aynı zamanda uyulması zorunlu hukuki, idari ve teknik yükümlülükleri belirleyen bağlayıcı düzenlemeler niteliği taşımaktadır. Bu nedenle anonim şirketlerin, yurt dışına veri aktarım süreçlerini büyük bir dikkat, özen ve şeffaflık içerisinde yürütmeleri hem KVKK hükümlerine hem de uluslararası veri koruma standartlarına tam uyum sağlamaları kritik bir zorunluluk olarak ortaya çıkmaktadır.

[473] KVKK m.9/6; Onward Transfer İlkeleri, EDPB Rehberi, 2022.

# SONUÇ

6698 sayılı Kişisel Verilerin Korunması Kanunu'nun 9. maddesinde yapılan son değişiklikler, kişisel verilerin yurt dışına aktarılmasında büyük bir dönüşüm yaşanmasına yol açmıştır. Özellikle, açık rızanın artık istisnai bir yöntem olarak değerlendirilmesi ve standart sözleşmelerin ana mekanizma olarak kabul edilmesi, Türkiye'deki anonim şirketlerin veri aktarım süreçlerini hukuki ve operasyonel açıdan önemli ölçüde etkilemiştir. Standart sözleşmeler, kişisel verilerin korunması ve yurt dışına aktarılması konusunda önemli bir araç olarak ortaya çıkmıştır. Bu sözleşmeler, yalnızca yurt dışı ile uyum sağlamakla kalmayıp, aynı zamanda veri sorumlularının yükümlülüklerini net bir şekilde belirleyerek, şeffaflık ve hesap verebilirlik ilkesini güçlendirmektedir.

Çalışmamızda ele aldığımız gibi, anonim şirketler açısından, veri aktarımının her aşamasında yasal sorumlulukların yerine getirilmesi, veri güvenliğinin sağlanması ve veri sahiplerinin haklarının korunması gerekliliği oldukça önemlidir. Standart sözleşmeler, veri sorumlularının bu yükümlülükleri yerine getirmelerinde, özellikle denetleme ve izleme süreçlerinde kritik bir rol oynamaktadır. Bu sözleşmeler, veri sorumlularının, veri alıcılarının veri güvenliği ile ilgili sorumluluklarını ve veri ihlali durumunda alınacak önlemleri belirlemelerine olanak tanır. Ayrıca, anonim şirketlerin yurt dışına veri aktarımını gerçekleştirirken, verilerin nasıl işleneceğine dair açık ve net düzenlemeler yaparak, ilgili kişilere aydınlatma yükümlülüğü sağlamaları gerektiği unutulmamalıdır. Bu bağlamda, standart sözleşmelerin içerdiği güvence mekanizmaları, yalnızca ulusal değil, aynı zamanda uluslararası veri güvenliğini temin etmede de önemli bir araç haline gelmektedir.

KVKK'nın güncellenen 9. maddesiyle birlikte, Türkiye'deki anonim şirketlerin veri aktarım süreçlerinde daha şeffaf, denetlenebilir ve güvenli bir yapı kurulduğu gözlemlenmektedir. Uluslararası düzenlemelerle yapılan kıyaslamalar, Türkiye'nin veri koruma politikalarının, özellikle Avrupa Birliği Genel Veri Koruma Tüzüğü (GDPR) ile uyumlu hale gelmeye başladığını göstermektedir. Ancak, Türkiye'deki standart sözleşmelerin, AB'deki "Standard Contractual Clauses" (SCC) ile tam uyumlu olmaması, uygulamada bazı zorluklara yol açabilmektedir. Bu nedenle, Türkiye'deki mevzuatın Avrupa ile daha paralel bir yapıya kavuşturulması, veri güvenliği açısından daha sağlam bir temel sağlayacaktır.

Bununla birlikte, yurt dışına kişisel veri aktarımı süreçlerinin yalnızca hukuki metinlerle değil, aynı zamanda sektörel rehberlerle, uygulama örnekleriyle ve denetim standartlarıyla desteklenmesi gerektiği açıktır. Özellikle finans, sağlık ve teknoloji gibi yüksek regülasyon

içeren sektörlerde, sektöre özgü rehber dokümanların geliştirilmesi, uygulayıcıların tereddüt yaşadığı noktaları ortadan kaldırabilir. Bu doğrultuda, Kurul'un yayımlayacağı rehberlerin ve kamuoyuna açık karar örneklerinin, uygulamada yeknesaklık sağlamaya katkı sunması beklenmektedir. Ayrıca, veri koruma kültürünün sadece yükümlülük temelli değil, risk temelli bir yaklaşım üzerinden geliştirilmesi, anonim şirketlerin veri aktarım süreçlerinde daha etkin bir yönetim ve denetim sistemi kurmasına yardımcı olacaktır.

Sonuç olarak, anonim şirketlerin kişisel veri aktarımı sürecinde kullandıkları standart sözleşmeler hem yasal uyumu sağlamak hem de veri güvenliğini garanti altına almak açısından hayati bir öneme sahiptir. Standart sözleşmelerin etkin bir şekilde uygulanması, sadece yurt dışı ile uyum sağlama açısından değil, aynı zamanda veri sahiplerinin haklarını ihlal etmeden, veri koruma yükümlülüklerini yerine getirme açısından da kritik bir role sahiptir. Bu sayede anonim şirketler, yalnızca hukuki yükümlülüklerini yerine getirmekle kalmayıp, aynı zamanda kurumsal itibarlarını güçlendirebilir ve uluslararası düzeyde güvenli bir veri aktarımı gerçekleştirebilirler. KVKK'nın 9. maddesiyle sağlanan bu güncellenmiş düzenlemeler, Türkiye'deki anonim şirketlerin veri güvenliği ve yasal uyum süreçlerinde önemli bir dönüm noktasıdır ve bu süreçlerin daha şeffaf, güvenilir ve etkili bir biçimde işlemesine olanak tanımaktadır.

## KAYNAKÇA


- **Akbulak**, Yavuz, "TTK Işığında Anonim Şirketlerde Pay Senetleri", *Ankara Barosu Dergisi*, Sayı:1, Ocak 2016. https://dergipark.org.tr/tr/download/article-file/398510.
- **Akçakoca**, Murat, *Tıp Ceza Hukukunda Kişisel Sağlık Verilerinin Korunması,* Adalet yayınevi, 1. Baskı, Ankara, 2022.
- **Akkurt**, Sinan Sami, Kişisel Veri Kavramının Hukuki Niteliğine İlişkin Yaklaşımlara Mukayeseli Bir Bakış, *T.C. Selçuk Üniversitesi Hukuk Fakültesi Kişisel Verileri Koruma Dergisi,* Cilt: 2, Sayı: 1.
- **Akkurt**, Sinan Sami, "Kişisel Verilerin Korunması Hakkının Hukuki Niteliği" Hukuk ve Bilişim Dergisi, https://hukukvebilisim.org/kisisel-verilerin-korunmasi-hakkinin-hukuki-niteligi.
- **Akgül,** Aydın**,** *"Danıştay ve Avrupa İnsan Hakları Mahkemesi Kararları Işığında Kişisel Verilerin Korunması*", Beta Yayınları, Ankara, 2016.
- **Akgül**, Aydın, *Danıştay ve Avrupa İnsan Hakları Mahkemesi Kararları Işığında Kişisel Verilerin Korunması*, İstanbul, Legal Yayıncılık, 2010.
- **Aksoy**, Hüseyin Can, *Medeni Hukuk ve Özellikle Kişilik Hakkı Yönünden Kişisel Verilerin Korunması*, Ankara, Çakmak Yayınevi, 2010.
- **Alçın**, Ayşe Aslı, 'Türk Hukukunda Kişisel Sağlık Verileri ve İdarenin Kişisel Sağlık Verilerini Koruma Yükümlülüğü', *TAAD*, sayı:51, Temmuz 2022.
- **Altaş**, Soner, *"Uygulamalı Anonim Şirketler Hukuku",* Ankara, Seçkin Hukuk, 2021.
- **Ayhan** Rıza, Hayrettin **Çağlar,** Mehmet **Özdamar**, *Şirketler Hukuku Genel Esaslar*, 4.baskı, Ankara: Yetkin Yayınevi, 2022.
- **Ayözger Öngün**, A. Çiğdem, *Elektronik Haberleşme Sektörüne İlişkin Özel Düzenlemeler Dahil Kişisel Verilerin Korunması Hukuku*, İstanbul, Beta Yayıncılık, 2019.
- **Bahtiyar**, Mehmet, *"Ortaklıklar Hukuku"* Ankara, Beta Yayıncılık, 15. Bası, 2021.
- **Bakırel**, Nur Buğçe, *Veri Sorumlusu ve Veri İşleyen Arasındaki Sorumluluk Paylaşımı Avrupa Birliği Genel Veri Koruma Tüzüğü ve Kişisel Verilerin Korunması Kanunu Çerçevesinde Değerlendirilmesi,* Ankara, Seçkin Hukuk, 1. Baskı, 2021.
- **Bartow**, Ann, "Our Data, Ourselves: Privacy, Propertization and Gender", *University of San Francisco Law Review*, C. 34, 1999.

- **Başalp,** Nilgün**,** "*Kişisel Verilerin Korunması ve Saklanması",* Ankara, Yetkin Yayıncılık, 1. Baskı, 2004.
- **Batan**, Ali, A Quick Overview of Know Your Customer (KYC) in Financial Industry, https://www.researchgate.net/publication/357173989_A_Quick_Overview_of_Know_Your_Customer_KYC_in_Financial_Industry.
- **Bayraktar**, Müzeyyen, *Kişisel Sağlık Verilerinin İşlenmesi ve Korunması,* Marmara Üniversitesi Sosyal Bilimler Enstitüsü Yayımlanmamış Yüksek Lisans Tezi, 2022.
- **Baysal**, Mustafa, *KVKK Kişisel Verilerin Korunması Kanunu El Kitabı*, Ankara, Seçkin Yayıcılık, 7. Baskı, 2024.
- **Bello**, Allıy, **Oduro**, Davıd Amoah, **Opoku**, Emmanuel, **Bello**, Adepeju Deborah, Adenıjı Omotayo Leo, Chıoma Emmanuel Ukatu, Nonso Okıka, Enhancing Know Your Customer (Kyc) And Anti-Money Laundering (Aml) Compliance Using Blockchain: A Business Analysis Approach. Iconıc Research And Engıneerıng Journals, Volume 8 Issue 9, Mar 2025. https://www.researchgate.net/publication/389814116_Enhancing_Know_Your_Customer_KYC_and_AntiMoney_Laundering_AML_Compliance_Using_Blockchain_A_Business_Analysis_Approach.
- **Bilgili**, Fatih ve Ertan **Demirkapı***, Şirketler Hukuku*, 9. baskı., Bursa, Dora Yayıncılık, Ocak 2013.
- **Bozkurt,** Tamer, "*Şirketler Hukuku"*, Legem Yayıncılık, 2018.
- **Braun,** Cihan Avcı, Kişisel Verilerin İşlenmesinde Rıza, *Yeditepe Üniversitesi Hukuk Fakültesi Dergisi*, 2018, C. 15, S.1.
- **Civelek**, Dilek Yüksel, Kişisel Verilerin Korunması ve Bir kurumsal Yapılanma Önerisi, *Bilgi Toplumu Dairesi Başkanlığı,* Ankara, 2011. https://www.sbb.gov.tr/wp-content/uploads/2022/08/Kisisel-Verilerin-Korunmasi-ve-Bir-Kurumsal-Yapilanma-Onerisi-Dilek-Yuksel-Civelek.pdf.
- **Çağlar,** Hayrettin, Rıza **Ayhan** ve Mehmet **Özdamar**, "Şirketler Hukuku Genel Esaslar", Ankara, Yetkin Hukuk Yayıncılık, 2019.
- **Çebi,** Hakan, *Şirketler Hukuku*, 1. baskı, Ankara: Seçkin Yayıncılık, 2020.
- **Çekin**, Mesut Serdar, *Avrupa Birliği Hukukuyla Mukayeseli Olarak 6698 Sayılı Kanun Çerçevesinde Kişisel Verilerin Korunması Hukuku,* İstanbul, On İki Levha Yayıncılık, 3. Baskı, 2020.
- **Çelik** Aytekin, *Ticaret Hukuku*, 13. baskı, Ankara: Seçkin Yayıncılık, 2023.

- **Çelik**, Işıl, *6698 Sayılı Kişisel Verilerin Korunması Kanunu ve 2016/679 Sayılı Avrupa Birliği Genel Veri Koruma Tüzüğü Kapsamında Kişisel Verilerin Yurt Dışına Aktarılması*, On İki Levha Yayıncılık, 2022.
- **Çelikel**, Serdar, "Kişisel Verilerin İşlenmesinde, Açık Rıza Hukuka Uygunluk Nedeninin, 95/46 Sayılı Direktif ve GDPR' la Karşılaştırmalı Olarak İncelenmesi", *Uyuşmazlık Mahkemesi Dergisi*, Yıl 9, Sayı 17, Haziran 2021.
- **Çetiner**, Selma ve Armağan Ebru Bozkurt **Yüksel**, *Ticari İşletme ve Şirketler Hukuku*, Ankara, Seçkin Yayıncılık, 2024.
- **Demirel**, Duygu, "Anonim Şirketlerde Yönetim Yetkisinin Devri", *Hacettepe Hukuk Fakültesi Dergisi,* Cilt 7, Sayı 2, 2017.
- **Demirtaş,** Ahmet, "ChatGPT'nin Gölgesinde Kişisel Verilerin Korunması", *Kişisel Verileri Koruma Dergisi*, C.6, S.1.
- **Deniz,** Miray Özer, "Kişisel Verilerin İşlenmesinin Türleri ve Hukuki Nitelikleri" *Necmettin Erbakan Üniversitesi Hukuk Fakültesi Dergisi*, cilt:6, S. 1, 2023.
- **Deniz,** Miray Özer*, Özel Nitelikli Kişisel Verilerin İşlenmesi ve Bundan Doğan Sorumluluk*, İstanbul, Oniki Levha Yayıncılık, 1. Baskı 2022.
- **Doğan**, Beşir Fatih. *6102 Sayılı Türk Ticaret Kanunu'na Göre Anonim Şirket Yönetim Kurulunun Organizasyonu ve Yönetim Yetkisinin Devri*. İstanbul, Vedat Kitapçılık, 2011.
- **Doğan**, Beşir Fatih, "Yönetim Kurulunun Devredilemez Yetkileri ve Yönetim Yetkisinin Devri", *Dergipark,* Cilt:18, Sayı:2, 2012.
- **Doğan,** Buse, *''Kişisel Verilerin İşlenme Şartları Bağlamında Açık Rıza''* Yayınlanmamış Yüksek Lisans Tezi, 2019.
- **Dülger,** Murat Volkan, *Kişisel Verilerin Korunması Hukuku,* İstanbul, Hukuk Akademisi, 1. Baskı, 2019.
- **Dülger**, Murat Volkan, *Kişisel Verilerin Korunması Hukuku,* İstanbul, Hukuk Akademisi, 3. Baskı, 2020.
- **Ekmekçi** Ömer, Nafiye **Yücedağ,** Elif Beyza **Akkanat-Öztürk**, Şehriban İpek **Aşıkoğlu**, Kişisel Verilerin Korunması Hukuku, On İki Levha Yayıncılık, 1.baskı, İstanbul 2024.
- **Erdoğmuş**, Elif, *6698 Sayılı Kişisel Verilerin Korunması Kanunu Kapsamında Açık Rıza,* Ankara, Seçkin Yayıncılık, 1. Baskı, 2022.

- **Galandarlı** Arzu, "KVKK ve GDPR: Standart Sözleşme Maddeleri Arasındaki Farklar", Hukuk ve Bilişim Dergisi, 21. Sayı, 2 Ocak 2025, https://www.hukukvebilisimdergisi.com/kvkk-ve-gdpr-standart-sozlesme-maddeleri-arasindaki-farklar/.
- **GDPR** (2016). *Avrupa Birliği Genel Veri Koruma Tüzüğü (Regulation Eu 2016/679)*. Avrupa Birliği.
- **Günal,** Ayşe Nida, "İş İlişkilerinde Kişisel Verilerin İşlenmesinde Hukuka Uygunluk Sebebi Olarak "Meşru Menfaat", *Kişisel Verileri Koruma Dergisi*, C.4, S.2, s. 1-18.
- **Gözler**, Kemal, *Türkiye Hukuk Ansiklopedisi (TÜHA),* Cilt 3.
- **Gözler**, Kemal, *"TÜHAS: Türk Hukuk Atıf Usulleri",* Bursa, Ekin.2024, *https://books.google.com.tr/books?id=srruEAAAQBAJ&printsec=frontcover&hl=tr&source=gbs_ge_summary_r&cad=0#v=onepage&q&f=false*.
- **Güney**, Necla Akdağ, "*Anonim Şirket Yönetim Kurulu"*, 2. Baskı, İstanbul, Vedat Kitapçılık, 2016.
- **Hocaoğlu**, Hatice**,** Fatma Sümeyra **Doğan**, Zeynep Sena **Saltık**, "Bulut Yasası ve Schrems II Kararı Işığında Türkiye'de Müşteri Hizmeti Uygulamaları Hakkında Uygulamacı Perspektifinden Değerlendirmeler"*, Terazi Hukuk Dergisi*, Cilt: 16, Sayı: 174, Şubat 2021.
- **İkiler**, Bora ve Y. Sertaç **Serter**, *Şirketler İçin Kişisel Verilerin Korunması Hukuku Rehberi*, On İki Levha Yayıncılık, İstanbul 2023.
- **İmançlı,** Canan, *Kişisel Sağlık Verilerinin Korun(A)Mamasından Doğan Özel Hukuk Sorumluluğu*, On İki Levha Yayıncılık, İstanbul, 2020.
- **İmançlı**, Canan, "Kişisel Sağlık Verilerinin Korunamamasından Doğan Özel Hukuk Sorumluluğu", Sosyal Bilimler Enstitüsü, Özel Hukuk Anabilim Dalı, Yayınlanmamış Yüksek Lisans Tezi, İstanbul 2019.
- **Kalender**, Süleyman, *Anonim Şirketlerde Yönetim ve Temsil Yetkisinin Devri Halinde Yönetim Kurulu Üyelerinin Hukuki Sorumluluğu*, Ankara, Adalet Yayınevi, 2024.
- **Kartalcı**, Saadet, "Kişisel Verilerin Korunması Hakkı ve Hukuki Niteliği", *Hukuk ve Bilişim Dergisi*, https://hukukvebilisim.org/kisisel-verilerin-korunmasi-hakkinin-hukuki-niteligi.
- **Kaya,** Mehmet Bedi, *KVKK Reformu 2024 Değişiklikleri,* Dijital Baskı v1.0- Mart 2024, *https://mbkaya.com/hukuk/kvkk-reformu.pdf*.

- **Kaya**, Mehmet Bedi, Furkan Güven **Taştan**, *Kişisel Veri Koruma Hukuku*, Çevrimiçi Sürüm 3.0 Ocak 2025, s.25. https://mbkaya.com/hukuk/veri-koruma-hukuku.pdf.
- **Kaya,** Mehmet Bedi, "Kişisel Verilerin Korunmasında Yeni Paradigma: Hesap Verebilirlik İlkesi," *İstanbul Hukuk Mecmuası*, Cilt 78, Sayı 4, 2020, s. 1859-1897, http://dergipark.gov.tr/iuhfm,
- **Kaya**, Zeynep Ebrar, KVKK ve GDPR Arasında Kişisel Verilerin İşlenmesine İlişkin Genel İlkelerin Kıyası, *Hukuk ve Bilişim Dergisi,* sayı:10, https://www.hukukvebilisimdergisi.com/kvkk-ve-gdpr-arasinda-genel-ilkelerin-kiyasi/.
- **Kayıhan**, Şaban, *Şirketler Hukuku,* Ankara, Seçkin Hukuk, 2024.
- **Kılıçoğlu**, Ahmet M., "Fikri Hakların İhlalinde Hukuksal Koruma Yolları (Sınai Haklarla Karşılaştırmalı Olarak)", *Türkiye Barolar Birliği Dergisi*, S. 54, 2004.
- **Kırca,** İsmail, Feyzan Hayal **Şehirali Çelik**, Çağlar **Manavgat**, *"Anonim Şirketler Hukuku",* Cilt 1, Temel Kavramlar ve İlkeler, Kuruluş, Yönetim Kurulu, Ankara, Banka ve Ticaret Hukuku Araştırma Enstitüsü, 2013.
- **Köksal**, Aytaç, Bağımsız Denetim Sözleşmesi, 1. Bası, Beta, İstanbul 2009.
- **Köksal**, Aytaç, Türk Ticaret Kanunu Tasarısının 397 ila 406. Maddeleri Arasında düzenlenen Denetçinin Anonim Ortaklığın Organı Olup Olmadığı Sorunu, Prof. Dr. Fırat Öztan'a Armağan Cilt 1.
- **Kuner,** Christopher, *Transborder Data Flows And Data Privacy Law*. Oxford University Press, 2020.
- **Kuner,** Christopher, *European Data Protection Law,* s.98, k.n.2.87.
- **Kuner,** Christopher, GDPR Article 49: The EU General Data Protection Regulation: A Commentary Update of Selected Articles, Christopher Kuner, Lee A. Bygrave, Christopher Docksey, Oxford: *Oxford University Press,* 2021. https://ssrn.com/abstract=3839645.
- **Kuner**, Christopher, Lee A. Bygrave, Christopher Docksey, *The EU General Data Protection Regulation (GDPR) A Commentary,* Oxford University Yayınları, 2020.
- **Kuyumcu**, Seda, *"6698 Sayılı Kişisel Verilerin Korunması Kanunu Kapsamında Kişisel Verilerin Yurt Dışına Aktarılması ve Aktarım Koşullarının Değerlendirilmesi"*, (Yüksek Lisans Tezi, Danışman Dr. Öğr. Üyesi Mehtap İpek İşleten, İstanbul, Galatasaray Üniversitesi Sosyal Bilimler Enstitüsü Özel Hukuk Anabilim Dalı

Yayımlanmamış Yüksek Lisans Tezi, Mayıs 2024, (https://tez.yok.gov.tr/UlusalTezMerkezi/tezSorguSonucYeni.jsp).

- **KVKK,** "Kanunlarda Öngörülme Kişisel Veri İşleme Şartına İlişkin Bilgi Notu", *KVKK Yayınları no:62*, Mart 2025, Ankara.
- **Küzeci,** Elif, Kişisel Verilerin Korunması, Ankara, Turhan Kitabevi, 3. Baskı, 2019.
- **Lessig**, Lawrence, "Privacy as Property", *Social Research*, C. 69, S. 1, 2002
- **Memiş,** Tekin, "Veri Sorumlusu ve Veri İşleyen Arasındaki İlişkiler ve Sorumluluk Düzeni", *Beykent Üniversitesi Hukuk Fakültesi Dergisi,* Cilt:3, Sayı:6, Aralık 2017.
- **Oğuz,** Sefer, "Kişisel Verilerin Korunması Hukukunun Genel İlkeleri", *Bilgi Ekonomisi ve Yönetimi Dergisi,* 2018, Cilt:13, Sayı:2 (121-138). https://dergipark.org.tr/tr/pub/beyder/issue/41709/425303#article_cite.
- **Orak,** Beşir, *Kişisel Sağlık Verilerin Korunması*, Ankara, Yetkin Yayıncılık, 1. Baskı, 2020.
- **Oğuzman,** M. Kemal; Özer **Seliçi** ve Saibe **Oktay**, *Kişiler Hukuku (Gerçek ve Tüzel Kişiler)*, İstanbul, Filiz Kitabevi, 2002.
- **Oğuzman,** M. Kemal ve Turgut Öz, *Borçlar Hukuku Genel Hükümler*, İstanbul: Filiz Kitabevi, 2000.
- **Özbağ** Zikrullah, "*Anonim Şirket Yönetim Kurulu Üyelerinin Cezai Sorumlulukla Bağlantılı Hukuki Sorumluluğu",* Ankara, Adalet Yayınevi, 2024.
- **Özkan,** Oğulcan, *"Kişisel Verilerin Korunması",* Ankara Üniversitesi Sosyal Bilimler Enstitüsü Özel Hukuk Anabilim Dalı, Ankara, 2020, Yayımlanmamış Yüksek Lisans Tezi.
- **Özkan,** Rabia, "Kişisel Veri Koruma Hukukunun Kişilik Hakkının Korunması Çerçevesinde Değerlendirilmesi", *Ankara Sosyal Bilimler Üniversitesi Hukuk Fakültesi Dergisi*, Cilt 3, Sayı:2.
- **Öztürk,** Bahri, Elif **Altınok Çalışkan**, Serkan **Seyhan**, *Kişisel Verilerin Korunması Hukuku Teorik ve Pratik Çalışma Kitabı*, Ankara, Seçkin Hukuk, 3. Baskı, 2024.
- **Öztürk**, Elif Beyza Akkanat, *Karşı Edim Olarak Kişisel Veriler,* İstanbul, Oniki Levha Yayıncılık, 1. Baskı 2022.
- **Palta,** Nihan, Türk ve İsviçre Anonim Şirketler Hukukunda Organ Kavramı, *Akdeniz Üniversitesi Hukuk Fakültesi Dergisi,* Haziran 2022, cilt 12, Sayı:1.
- **Paslı**, Ali, "Compliance" Kavramının Anonim Ortaklıklar Hukukundaki Anlamı ve Sorumluluk Sistemine Etkisi", *İÜHFM,* Cit 71, Sayı 2, 2013.

- **Pulaşlı,** Hasan, "Compliance Kavramı ve Yönetim Organının Compliance Sorumluluğu", *BATIDER*, Cilt 35, Sayı 2, 2019.
- **Pulaşlı,** Hasan, *Şirketler Hukuku Genel Esasları*, Ankara, Adalet Yayınevi, 6. Baskı, 2020.
- **Pulaşlı,** Hasan, *Şirketler Hukuku Genel Esasları*, Ankara, Adalet Yayınevi, 4. Baskı, 2016.
- **Pulaşlı,** Hasan, *Şirketler Hukuku şerhi,* Cilt I, Ankara, Adalet Yayınevi, 2018.
- **Pulaşlı,** Hasan, "Anonim Ortaklık Yönetim Kurulunda Yönetim Kurulu Üyeliğinin Temsili", *Prof. Dr. Fahiman Tekil'in Anısına Armağan*, İstanbul, MÜ Hukuk Fakültesi Yayınları, 2003.
- **Prins**, Corien, "When Personal Data, Behavior and Virtual Identities Become a Commodity: Would a Property Rights Approach Matter?", *Script-ed*, C. 3, S. 4, 2006.
- **Saat**, Dursun, "Kişisel Verilerin Korunması Kanunu'nda Öngörülen Meşru Menfaat Kavramının Ticaret Şirketleri Bakımından Değerlendirilmesi*", Anadolu Üniversitesi Hukuk Fakültesi Dergisi,* Cilt: 10, Sayı: 2, Temmuz 2024, s. 617-638. https://earsiv.anadolu.edu.tr/xmlui/bitstream/handle/11421/28842/10.54699-andhd.1491304-3962034.pdf.
- **Samuelson**, Pamela, "Privacy as Intellectual Property?", *Stanford Law Review*, C. 52, 2000.
- **Şener**, Oruç Hami, Teorik ve Uygulamalı *Ortaklıklar Hukuku Ders Kitabı*, 4. Baskı, Ankara 2019.
- **Taştan,** Furkan Güven, Türk *Sözleşme Hukukunda Kişisel Verilerin Korunması*, İstanbul, On İki Levha, 2017.

- **Tekinalp,** Ünal**,** Reha **Poroy**, Ersin **Çamoğlu**, *Ortaklıklar Hukuku*, 14. Baskı, Vedat Kitapçılık, İstanbul, 2019.
- **Tekinalp,** Ünal, *Tek Kişi Ortaklık,* Vedat Kitapçılık, İstanbul 2011.
- **Uçak,** Murat, "Kişisel Verilerin Ölümden Sonra Korunması", *İMHFD*, C. VI, S. 10, 2021.
- **Uyarer,** Sinem Göçmen, *Kişisel Verilerin Korunması Kanunu ve Türk Ceza Kanunu Kapsamında Kişisel Verilerin Korunması,* Ankara, Seçkin Yayıncılık, 2. Baskı, 2020.
- **Yaşar**, Anonim Şirketler Hukukunda Uyum (Compliance)

- **Yıldırım,** Suat, "Türk Ticaret Kanunu'na Göre Anonim Şirketlerde Denetçi", Mali Çözüm Dergisi, Cilt 21, Sayı 106, 2011.
- **Yıldız**, Şükrü, Türk Ticaret Kanunu Tasarısına Göre Limited Şirketler Hukuku, İstanbul, Arıkan Yayınevi, 2007.
- **Yılmaz**, Süleyman, **Erkan**, Vehbi Umut; "Sosyal Medya Hesaplarının Miras Yoluyla İntikal Edip Edemeyeceği Sorusunun Kişisel Verileri Koruma Hukuku Kapsamında İncelenmesi", *İnönü Üniversitesi Hukuk Fakültesi Dergisi*, C. 11, S. 2, s. 574; **Dinç**, Yasemin, Maraşlı, "Ölümden Sonra Sosyal Medya Hesaplarının Hukuki Akıbeti: Dijital Miras", *TBBD*, S. 142, 2019, (aktaran: Miray Özer Deniz, *Özel Nitelikli Kişisel Verilerin İşlenmesi ve Bundan Doğan Sorumluluk*, On İki Levha Yayıncılık, İstanbul 2022).
- **Yılmaz**, Tüze, *Avrupa Birliğinde Kişisel Verilerin Korunması Hukuku*, Adalet Yayınevi, Ankara, 1. Baskı, 2022.
- **Yosif**, Umniyahasghar, Kişisel Verilerin İşlenmesi Şartları ve 6698 Sayılı Kişisel Verilerin Korunması Kanununun Ruhu Olarak Genel İlkeler, *Selçuk Üniversitesi Adalet Meslek Yüksekokulu Dergisi,* Cilt 4, Sayı 1, 2021.
- **Yücedağ**, Nafiye, ''Kişisel Verilerin Korunması Kanunu Kapsamında Genel İlkeler'', *Kişisel Verileri Koruma Dergisi*, Cilt 1, Sayı 1, 2019.
- **Yüksek**, Furkan Kaan, AİHM İçtihatlarında Kişisel Verilerin Korunması, *Dokuz Eylül Üniversitesi Hukuk Fakültesi Dergisi,* Cilt: 25, Sayı: 1, 2023. https://dergipark.org.tr/tr/download/article-file/3056573.
- **Yüksel**, Gürbüz, ''Kişisel Sağlık Verilerinin Hukuki Korunması*'', Sağlık Akademisyenleri Dergisi*, Ankara, 2019.
- **Yürük,** Zehra, *Kişisel Verilerin İhlalinden Doğan Özel Hukuk Sorumluluğu*, İstanbul Ticaret Üniversitesi Sosyal Bilimler Enstitüsü Özel Hukuk Anabilim Dalı, Yüksek Lisans Tezi, 2021.
- **Yürük,** Zeynep, "Veri Sorumlusunun Veri Güvenliğine İlişkin İdari ve Teknik Tedbirleri Alma Yükümlülüğü", *İstanbul Ticaret Üniversitesi Sosyal Bilimler Dergisi*, C. 22, S. 48, 2023. https://doi.org/10.46928/iticusbe.1218693.
- **Zittrain**, Jonathan, "What the Publisher Can Teach the Patient: Intellectual Property and Privacy in an Era of Trusted Privication", *Stanford Law Review*, C. 52, 2000.
- **Zor,** Abdülhamid, *Veri Sorumlusunun Yükümlülükleri ve Bu Yükümlülükleri İhlalinden Doğan Özel Hukuk Sorumluluğu*, On İki Levha Yayıncılık, İstanbul 2020.

- Avrupa veri koruma mevzuatı El Kitabı, Lüksemburg, 2018, https://itlaw.bilgi.edu.tr/media/2020/3/30/Bilgi_Avrupa_Veri_Koruma_Mevzuatı_El_Kitabı_2018_TR_v01_16022019.pdf.


**Resmî ve Uluslararası Belgeler**


- Avrupa Adalet Divanı (CJEU), "Data Protection Commissioner v Facebook Ireland Ltd and Maximillian Schrems (Schrems II)", C-311/18, 16 Temmuz 2020, https://curia.europa.eu/.
- Avrupa Adalet Divanı (CJEU), "Fashion ID Kararı (C-40/17)", https://curia.europa.eu/juris/document/document.jsf?text=&docid=216555&doclang=EN.
- Avrupa Adalet Divanı (CJEU), "Müşterek Veri Sorumluluğuna İlişkin Karar", https://www.gsghukuk.com/....
- Avrupa Birliği Adalet Divanı, C-268/21, Norra Stockholm Bygg AB v. Per Nycander AB, karar tarihi: 04.05.2023, para. 45, https://curia.europa.eu/juris/document/document.jsf?text=&docid=270823&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=2078240 >.
- Avrupa İnsan Hakları Mahkemesi, "Avrupa İnsan Hakları Sözleşmesi 8. Madde Rehberi", https://inhak.adalet.gov.tr/....
- Avrupa Komisyonu, "Yeterlilik Kararları", https://commission.europa.eu/law/.../adequacy-decisions_en.
- Avrupa Komisyonu – TİTCK, "İdari Anlaşma (Kişisel Verilerin Aktarımı)", https://titck.gov.tr/Dosyalar/.../1IdariAnlasma.pdf.
- CJEU, Nowak v. Data Protection Commissioner, Case C-434/16, ECLI:EU:C:2017:994; ayrıca bkz. Avrupa Konseyi, Convention 108+.
- UK Information Commissioner's Office (ICO), "Legitimate Interests", Guide to the General Data Protection Regulation (GDPR), https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/legitimate-interests/.
- Modernised Convention for the Protection of Individuals with Regard to the Processing of Personal Data, 2018.
- Fransa, Loi Informatique et Libertés, Yasa No. 78-17, 06.01.1978, m.85, https://www.legifrance.gouv.fr/.

- Québec, Act to Modernize Legislative Provisions Respecting the Protection of Personal Information (Bill 64), 2021, https://www.cai.gouv.qc.ca/loi-modernisee/.
- Japan, Act on the Protection of Personal Information (APPI), rev. 2020, https://www.ppc.go.jp/en/.
- Almanya, Bundesdatenschutzgesetz (BDSG), 30.06.2017, yürürlük: 25.05.2018, §1(1).
- İsviçre, Datenschutzgesetz (DSG), 25.09.2020, Art. 2(1), https://www.fedlex.admin.ch/eli/cc/2022/491/fr.


**Avrupa Veri Koruma Kurulu (EDPB) ve EDPS Belgeleri**


- Avrupa Veri Koruma Kurulu (EDPB), *Guidelines 2/2018 on Derogations of Article 49*, 25 Mayıs 2018, https://edpb.europa.eu/.
- EDPB, *Guidelines 2/2020 on Article 46(2)(a) and 46(3)(b)*, 18 Ocak 2020, https://edpb.europa.eu/...guidelines_202002...
- EDPB, "Schrems II Sonrası Rehber", https://www.edpb.europa.eu/....
- European Data Protection Supervisor (EDPS), "Transfer Impact Assessments (TIA) and Data Protection Impact Assessments (DPIA) Guidelines", 2021, https://edps.europa.eu/.
- Data Protection. WP, Consent.
- EDPB, "Guidelines 05/2020 on consent under Regulation 2016/679", https://www.edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-052020-consent-under-regulation-2016679_en.


**Kişisel Verileri Koruma Kurumu Belgeleri**


- KVKK, 6698 sayılı Kişisel Verilerin Korunması Kanunu ve Tam Gerekçesi, https://kvkk.pro/kvkk-gerekcesi.html.
- KVKK, Açık Rıza, https://www.kvkk.gov.tr/SharedFolderServer/CMSFiles/e3c6aa10-9de4-46f8-9b51-71bcf07c09b5.pdf.
- KVKK, "Kişisel Verilerin Yurt Dışına Aktarılması Rehberi", Mart 2024 ve Ocak 2025 baskıları, https://www.kvkk.gov.tr/Icerik/8142/.
- KVKK, "Yurt Dışına Veri Aktarımında Kullanılacak Standart Sözleşmelere İlişkin Duyuru", 4 Haziran 2024, https://www.kvkk.gov.tr/Icerik/7929/.
- KVKK, "Standart Sözleşme Bildirim Usul ve Esasları", 2025, https://www.kvkk.gov.tr/Icerik/8355/.

- KVKK, "Bağlayıcı Şirket Kuralları Hakkında Duyuru ve Yardımcı Kılavuz", https://www.kvkk.gov.tr/Icerik/6728/ve https://www.kvkk.gov.tr/Icerik/7935/.
- KVKK, "Veri Güvenliği Rehberi (Teknik ve İdari Tedbirler)", Ocak 2018, https://www.kvkk.gov.tr/yayinlar/veri_guvenligi_rehberi.pdf.
- KVKK, "Kişisel Veri İşleme Envanteri Hazırlama Rehberi", 2020, https://www.kvkk.gov.tr/Icerik/5446/.
- KVKK, "Kişisel Verilerin İşlenme Şartları Rehberi", www.kvkk.gov.tr.
- KVKK, "Aydınlatma Yükümlülüğü Tebliği", https://www.kvkk.gov.tr/Icerik/4108/.
- KVKK, "İlgili Kişi Kimdir?", https://www.kvkk.gov.tr/Icerik/2034/.
- KVKK, "VERBİS Hakkında SSS" ve "SORULARLA VERBİS", https://www.kvkk.gov.tr/Icerik/5414/ ve https://verbis.kvkk.gov.tr/UploadedFiles/SORULARLA_VERBİS.pdf.
- KVKK, "Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi Hakkında Yönetmelik", https://www.mevzuat.gov.tr/....
- KVKK, "Veri İhlali Bildirim Formu", https://www.kvkk.gov.tr/SharedFolderServer/....
- KVKK, "Kanunlarda Öngörülme Kişisel Veri İşleme Şartına İlişkin Bilgi Notu", Mart 2025.
- KVKK, "KVKK 9. Madde Değişiklikleri", Resmî Gazete, 12 Mart 2024.


**Kişisel Verileri Koruma Kurumu Kurul Kararları:**


- 2018/10 sayılı kararı.
- 02.04.2018 tarihli ve 2018/87 sayılı karar.
- 31.05.2018 tarihli ve 2018/63 sayılı kararı.
- 19.07.2018 sayılı 2018/88 sayılı kararı.
- 24.01.2019 tarihli 2019/10 sayılı karar.
- 07.03.2019 tarihli ve 2019/53 sayılı karar.
- 25.03.2019 tarihli ve 2019/78 sayılı karar.
- 25.03.2019 tarihli ve 2019/81 sayılı karar.
- 02.05.2019 tarih ve 2019/125 sayılı karar.
- 31.05.2019 tarihli 2019/162 sayılı karar.
- 18.07.2019 tarihli ve 2019/225 sayılı karar.
- 27.08.2019 tarih ve 2019/255 sayılı karar.

- 27.08.2019 tarihli ve 2019/296 sayılı karar.
- 07.11.2019 tarihli ve 2019/331 sayılı karar.
- 09/12/2019 tarih ve 2019/372 sayılı karar.
- 30.01.2020 tarihli ve 2020/71 sayılı karar.
- 13.02.2020 tarihli ve 2020/124 sayılı karar.
- 27.02.2020 tarihli ve 2020/167 sayılı karar.
- 27.02.2020 tarihli 2020/173 sayılı karar.
- 2020/225 sayılı karar.
- 05.05.2020 tarihli ve 2020/344 sayılı karar.
- 20/05/2020 tarihli ve 2020/404 sayılı karar.
- 23.06.2020 tarihli ve 2020/481 sayılı karar.
- 22.07.2020 tarihli ve 2020/559 sayılı karar.
- 08.10.2020 tarihli ve 2020/765 sayılı karar.
- 09.10.2020 tarih ve 2020/787 sayılı karar.
- 01.12.2020 tarihli 2020/915 sayılı karar.
- 22.12.2020 tarih ve 2020/966 sayılı karar.
- 12.01.2021 tarihli kamuoyu duyurusu.
- 11.03. 2021 tarihli 2021/238 sayılı karar.
- 25.03.2021 tarihli ve 2021/311 sayılı karar.
- 25.11.2021 tarihli ve 2021/1262 sayılı karar.
- 10.03.2022 tarihli ve 2022/229 sayılı karar.
- 17.03.2022 tarih ve 2022/249 sayılı karar.
- 2022/489 sayılı karar.
- 03.08.2022 tarihli ve 2022/774 sayılı karar.
- 04.08.2022 tarihli ve 2020/797 sayılı karar.
- 02.09.2022 tarihli ve 2022/902 sayılı karar.
- 08.09.2022 tarih ve 2022/924.
- 24.11.2022 tarihli ve 2022/1249 sayılı karar.
- 23.12.2022 tarihli ve 2022/1358 sayılı karar.
- 2022/987 sayılı karar.
- 26.01.2023 tarihli ve 2023/78 sayılı karar.
- 17.03.2023 tarihli ve 2023/389 sayılı karar.

- 02.05.2023 tarihli ve 2023/692 sayılı karar.
- 01.06.2023 tarih ve 2023/924 sayılı karar.
- 09.06.2023 tarihli ve 2023/1153 sayılı kurul karar.
- 03.08.2023 tarihli ve 2023/1310 sayılı karar.
- 14.09.2023 tarihli 2023/1578 sayılı karar.
- 01.06.2023 tarih ve 2023/924 sayılı karar.
- 4.06.2024 tarihli 2024/959 sayılı karar.

**Yardımcı ve Akademik Kaynaklar**

- Kişisel Verilerin Korunmasına İlişkin Bankacılık Sektörü İyi Uygulamalar Rehberi.
- İstanbul Bilgi Üniversitesi Bilişim ve Teknoloji Hukuku Enstitüsü, "Final Veri Aktarımı Raporu", 30 Mart 2020, https://itlaw.bilgi.edu.tr/...

**DİĞER KAYNAKLAR**

- 6698 sayılı Kişisel Verilerin Korunması Kanunu, Resmî Gazete, 7 Nisan 2016, Sayı: 29677.
- 6098 sayılı Türk Borçlar Kanunu, Resmî Gazete, 4 Şubat 2011, Sayı: 27836.
- 5237 sayılı Türk Ceza Kanunu, Resmî Gazete, 12 Ekim 2004, Sayı: 25611.
- 5411 sayılı Bankacılık Kanunu, Kabul Tarihi: 19.10.2005, RG: 01.11.2005, Sayı: 25983.
- EUR-Lex GDPR Metni, https://eur-lex.europa.eu/eli/reg/2016/679/oj.
- Aydınlatma Yükümlülüğünün Yerine Getirilmesinde Uyulacak Usul ve Esaslar Hakkında Tebliğ, Resmî Gazete, 10.03.2018, Sayı: 30356.
- Avrupa Parlamentosu ve Konseyi, *Genel Veri Koruma Tüzüğü (EU) 2016/679*, 27 Nisan 2016, Gerekçe, https://www.privacy-regulation.eu/en/recital-26-GDPR.htm.
- Veri Sorumluları Sicili Hakkında Yönetmelik, RG: 30.12.2017, Sayı: 30286.
- AWS, "Veri Güvenliği ve Gizlilik," 2023, https://aws.amazon.com/compliance/data-privacy/.
- Kişisel Verilerin İşlenmesine İlişkin Temel İlkeler *https://www.kvkk.gov.tr*
- 108 No'lu Kişisel Verilerin Otomatik İşleme Tabi Tutulması Karşısında Bireylerin Korunması Sözleşmesi, Strazburg, 1981.

- Avrupa Birliği Genel Veri Koruma Tüzüğü (2016) "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)" R.G. Tarih: 23.05.2018 sayı: OJ L 119, 04.05.2016; cor. OJ L 127.
- 95/46/EC sayılı Direktif.
- Niğde Ömer Halisdemir Üniversitesi Kişisel Verilerin Korunması ve İşlenmesi Politikası, https://ohu.edu.tr/kvkk/sayfa/kvk-ve-islenmesi-politikasi.
- İstanbul Gelişim Üniversitesi Kişisel Verileri Koruma Komisyonu Çalışma Usul ve Esaslarına İlişkin Yönerge, https://resim.gelisim.edu.tr/YONETMELIK_YONERGE/kisiselverilerikorumakomisyonucalismausulveesaslarinailiskinyonerge_09_06_2023.pdf.
- Kişisel Verilerin Korunmasına İlişkin Düzenlemeler Çerçevesinde Uluslararası Veri Aktarımı Yeni Gelişmeler ve Uygulamaya İlişkin Hukuki Değerlendirmeler, İstanbul, *https://itlaw.bilgi.edu.tr/media/2020/3/30/Final%20Veri_Aktarimi_Raporu_30.03.2020.pdf*.
- Kişisel Verilerin İşlenme Şartları https://www.kvkk.gov.tr.
- Kişisel Sağlık Verileri Hakkında Yönetmelik, RG, T. 21.06.2019, S. 30808.
- "Kişisel Verilerin Korunması Hakkının Hukuki Niteliği." Hukuk ve Bilişim Dergisi, https://hukukvebilisim.org/kisisel-verilerin-korunmasi-hakkinin-hukuki-niteligi
- https://www.linkedin.com/pulse/microsoft-türkiyeden-kvkk-ve-gdpr-uyumu-peakuptechnologies-ehi9f/
- https://fra-europa-eu.translate.goog/en/law-reference/european-convention-human-rights-article-8-0?_x_tr_sl=en&_x_tr_tl=tr&_x_tr_hl=tr&_x_tr_pto=tc.
- *https://kvkkblog.com/kisisel-verilerin-korunmasi-tarihine-yolculuk/*
- *https://www.kvkk.gov.tr/Icerik/2052/Yurtici-Aktarim*.
- GDPR, https://www.ab.gov.tr/siteimages/resimler/Nihai-ABB-HCDB-GDPR.pdf.
- Hesap verilebilirlik ilkesi Bknz.*https://kvkkblog.com/hesap-verilebilirlik/#:~:text=Hesap%20verilebilirlik%20ilkesi%20uyarınca%2C%20veri,getirildiğini%20ispat%20edebilecek%20durumda%20olmalıdır*.
- https://commission-europa-eu.translate.goog/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en?_x_tr_sl=en&_x_tr_tl=tr&_x_tr_hl=tr&_x_tr_pto=tc.

- https://www.mevzuat.gov.tr/mevzuat?MevzuatNo=6698&MevzuatTur=1&MevzuatTertip=5.
- https://kvkk.gov.tr/yayinlar/KİŞİSEL%20VERİLERİN%20KORUNMASI%20KANUNU%20VE%20UYGULAMASI.pdf.
- *https://www.mevzuat.gov.tr/mevzuat?MevzuatNo=6698&MevzuatTur=1&MevzuatTertip=5*.
- https://fra-europa-eu.translate.goog/en/law-reference/european-convention-human-rights-article-8-0?_x_tr_sl=en&_x_tr_tl=tr&_x_tr_hl=tr&_x_tr_pto=tc.
- *https://inhak.adalet.gov.tr/Resimler/Dokuman/2712020140848108_tur.pdf*.
- *Https://Www.Kvkk.Gov.Tr/Icerik/4197/Kisisel-Verilerin-Korunmasi-Kanununa-Iliskin-Uygulama-Rehberi*.
- *https://kvkkblog.com/kisisel-verilerin-korunmasi-tarihine-yolculuk/* .
- https://dergipark.org.tr/en/download/article-file/1671800.
- *https://www.kvkk.gov.tr/Icerik/4106/Kisisel-Verilerin-Yurtdisina-Aktarilmasi*.
- Niğde Ömer Halisdemir Üniversitesi Kişisel Verilerin Korunması ve İşlenmesi Politikası, https://ohu.edu.tr/kvkk/sayfa/kvk-ve-islenmesi-politikasi,
- İstanbul Gelişim Üniversitesi Kişisel Verileri Koruma Komisyonu Çalışma Usul ve Esaslarına İlişkin Yönerge, https://resim.gelisim.edu.tr/YONETMELIK_YONERGE/kisiselverilerikorumakomisyonucalismausulveesaslarinailiskinyonerge_09_06_2023.pdf.
- Basel Committee on Banking Supervision (2017). Sound Management of Risks Related to Money Laundering and Financing of Terrorism. https://www.bis.org/bcbs/publ/d505.pdf, Financial Action Task Force (FATF) (2021). Anti-Money Laundering and Counter-Terrorist Financing Measures, https://www.fatf-gafi.org/en/countries/detail/Turkey.html.
- Microsoft, "Veri Güvenliği ve Gizlilik Politikası," 2023, https://www.microsoft.com/en-us/trust-center.
- https://titck.gov.tr/Dosyalar/VeriKoruma/tr/1IdariAnlasma.pdf.
- https://www.kvkk.gov.tr/SharedFolderServer/CMSFiles/aaf0eeec-9599-4c68-8b7a-33039059ca41.pdf.
- https://www.kvkk.gov.tr/Icerik/7899/Taahhutname-Basvurusu-Hakkinda-Duyuru.

- Veri Koruma Derneği, "Data Privacy Türkiye KVKK Standart Sözleşme Atölyesi- Veri Koruma Derneği Platform Toplantısı Çıktıları", *YouTube*, 13 Şubat 2024. https://www.youtube.com/watch?v=K-zdTpx2l3E.
- Veri Koruma Derneği, "Data Privacy Türkiye KVKK Yurt Dışı Kişisel Veri Aktarımı Soru-Cevap Etkinliği", *YouTube*, 29 Eylül 2023, https://www.youtube.com/watch?v=k8KKAisrvgQ.
- Fransız veri koruma otoritesi, Cookies in the Context of the French Data Protection Authority's (CNIL)'ın Google kararı için bknz. https://dergipark.org.tr/tr/download/article-file/2710039.
- https://www.mavicompany.com/i/assets/documents/Kisisel_Veri_Koruma_Politikası_22.pdf.
- https://www.turkishairlines.com/tr-tr/yasal-uyari/veri-koruma-aydinlatma-metni/
- https://kvkk.subu.edu.tr/tr/acik-riza-formu.
- https://www-edps-europa-eu.translate.goog/data-protection/data-protection/reference-library/internationaltransfers_en?_x_tr_sl=en&_x_tr_tl=tr&_x_tr_hl=tr&_x_tr_pto=tc.
- https://www.bis.org/bcbs/publ/d505.pdf.
- https://www.fatf-gafi.org/en/countries/detail/Turkey.html.
- *https://www.kvkk.gov.tr/Icerik/2052/Yurtici-Aktarim*.
- https://www.ab.gov.tr/siteimages/resimler/Nihai-ABB-HCDB-GDPR.pdf.
- https://www-edps-europa-eu.translate.goog/data-protection/data-protection/reference-library/international-transfers_en?_x_tr_sl=en&_x_tr_tl=tr&_x_tr_hl=tr&_x_tr_pto=tc.
- https://commission-europa-eu.translate.goog/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en?_x_tr_sl=en&_x_tr_tl=tr&_x_tr_hl=tr&_x_tr_pto=tc.
- https://www.linkedin.com/pulse/microsoft-türkiyeden-kvkk-ve-gdpr-uyumu-peakuptechnologies-ehi9f/
- https://www.mevzuat.gov.tr/mevzuat?MevzuatNo=6698&MevzuatTur=1&MevzuatTertip=5.
- https://kvkk.gov.tr/yayinlar/KİŞİSEL%20VERİLERİN%20KORUNMASI%20KANUNU%20VE%20UYGULAMASI.pdf.
- *https://inhak.adalet.gov.tr/Resimler/Dokuman/2712020140848108_tur.pdf*.

- https://www.kvkk.gov.tr/Icerik/5410/Is-Basvurusu-Surecinde-Islenen-Kisisel-Verilerin-Hukuka-Aykiri-Sekilde-Paylasilmasi.
- https://www.kvkk.gov.tr/Icerik/5364/2018-143.
- https://www.dataprivacyframework.gov.
- https://www.bfdi.bund.de/EN/Home/home_node.html?cms_param3=JSoff&cms_param=1825034415105.
- Virginia Consumer Data Protection Act (VCDPA), Code of Virginia § 59.1-575 et seq., yürürlük: 01.01.2023, https://law.lis.virginia.gov/vacode/title59.1/chapter53/.
- Colorado Privacy Act (CPA), Colo. Rev. Stat. § 6-1-1301 et seq., yürürlük: 01.07.2023, https://coag.gov/resources/colorado-privacy-act/.
- Connecticut Data Privacy Act (CTDPA), Public Act No. 22-15, yürürlük: 01.07.2023, https://www.cga.ct.gov/2022/ACT/PA/PDF/2022PA-00015-R00SB-00006-PA.PDF.
- Utah Consumer Privacy Act (UCPA), Utah Code Ann. § 13-61-101 et seq., yürürlük: 31.12.2023, https://le.utah.gov/~2022/bills/static/SB0227.html.
- California Consumer Privacy Act (CCPA), cal. Civ. Code § 1798.100 et seq., yürürlük: 01.01.2020, https://oag.ca.gov/privacy/ccpa.
- California Privacy Rights Act (CPRA), cal. Civ. Code § 1798.100-1798.199.100, yürürlük: 01.01.2023, https://cppa.ca.gov/regulations/.

**YARGITAY KARARLARI**

- Yargıtay Ceza Genel Kurulu, E: 2012/12-1510, K: 2014/331, T.17.06.2014.
- Yargıtay 4. HD, 13.12.2017, E. 2016/2970, K. 2017/8273. .https://www.lexpera.com.tr/ictihat/yargitay/3-hukuk-dairesi-e-2021-273-k-2021-12613-t-7-12-2021.
- Yargıtay 4. HD, 14.03.2019, E. 2019/979, K. 2019/2679. https://www.lexpera.com.tr/ictihat/yargitay/4-hukuk-dairesi-e-2019-979-k-2019-2679-t-8-5-2019.
- Yargıtay 6. Hukuk Dairesi'nin 30.09.2015 tarihli kararı, https://eshukuk.com/Icerik/davali-davada-dayanilan-kira-sozlesmesindeki-imzasini-inkar-etmemektedir-kira-s.
- Yargıtay 3. Hukuk Dairesi'nin 07.12.2021 tarihli, 2021/12613 sayılı kararı.
- Yargıtay Hukuk Genel Kurulu, E. 2023/618, K. 2023/..., www.karamercanhukuk.com/yetki-belgesi-gecersiz-karar.

- Yargıtay 3. Hukuk Dairesi, E. 2002/414, K. 2002/1200, "Vekilin özel yetkisi olmadan yaptığı işlemler", Dergipark, https://dergipark.org.tr/tr/download/article-file/1878517.
- Yargıtay 11. Hukuk Dairesi'nin 04.05.2009 tarihli, 2009/2051 E. – 2009/5292 K. sayılı kararı.
- Yargıtay 11. Hukuk Dairesi'nin 05.02.2019 tarihli, 2017/5003 E. – 2019/842 K. sayılı kararı.
- İstanbul BAM 43. Hukuk Dairesi'nin 04.03.2021 Tarihli 2020/201 E. – 2021/249 K. Sayılı Kararı.
- Yargıtay 11. Hukuk Dairesi'nin 2020 tarihli, 2018/3182 E. – 2020/2652 K. sayılı kararı.

**EKLER**

**EK 1** : Örnek Standart Sözleşme Taslağı

**EK 2** : Kurulun Yayınladığı Standart Sözleşme Taslağı

**EK 1: Örnek Standart Sözleşme Taslağı**

**KİŞİSEL VERİLERİN YURT DIŞINA AKTARIMINA İLİŞKİN STANDART SÖZLEŞME TASLAĞI**

Taraflar:

Veri Gönderici:

[Şirket Adı]

[Ticaret Sicil Numarası]

[Adres]

[VERBİS Kayıt Bilgileri]

(Kısaca "Veri Gönderici" olarak anılacaktır.)

Veri Alıcı:

[Şirket Adı]

[Ticaret Sicil Numarası/Vergi Numarası]

[Adres]

(Yabancı ülkede mukim, kısaca "Veri Alıcı" olarak anılacaktır.)

**Madde 1 – Sözleşmenin Konusu**

İşbu Sözleşme, 6698 sayılı Kişisel Verilerin Korunması Kanunu ("KVKK") uyarınca, Veri Gönderici tarafından işlenen kişisel verilerin Veri Alıcı'ya yurt dışına aktarılması sürecinde, kişisel verilerin korunmasını sağlamak amacıyla tarafların hak ve yükümlülüklerini düzenlemek amacıyla akdedilmiştir.

**Madde 2 – Tanımlar**

İşbu Sözleşme kapsamında:

Kişisel Veri: Kimliği belirli veya belirlenebilir gerçek kişiye ilişkin her türlü bilgiyi,

Özel Nitelikli Kişisel Veri: Irk, etnik köken, siyasi düşünce, dini inanç vb. gibi özel nitelikli verileri,

İlgili Kişi: Kişisel verisi işlenen gerçek kişiyi,

İşleme: Kişisel veriler üzerinde gerçekleştirilen her türlü işlemi, ifade eder.

**Madde 3 – Veri Aktarımının Kapsamı**

Veri Gönderici, işbu Sözleşme uyarınca, aşağıda belirtilen kişisel verileri, belirtilen amaçlarla ve işbu sözleşmede belirtilen güvenlik önlemleri çerçevesinde Veri Alıcı'ya aktaracaktır:

Aktarılan Veri Kategorileri: [Örn. İsim, soy isim, iletişim bilgileri, lokasyon verileri, finansal bilgiler]

Aktarımın Amacı: [Örn. Hizmet sunumu, müşteri ilişkileri yönetimi, iş ortaklığı süreçlerinin yürütülmesi]

İlgili Kişi Grupları: [Örn. Müşteriler, çalışanlar, potansiyel müşteriler]

**Madde 4 – Tarafların Yükümlülükleri**

4.1. Veri Gönderici, KVKK ve ilgili mevzuat hükümlerine uygun olarak veri işlemiş ve aktarım için gerekli tüm hukuki şartları sağlamış olduğunu beyan eder.

4.2. Veri Alıcı, aktarılan kişisel verileri yalnızca işbu Sözleşmede belirtilen amaçlar doğrultusunda işleyeceğini ve üçüncü kişilere aktarmayacağını taahhüt eder.

4.3. Veri Alıcı, kişisel verilerin korunmasına ilişkin uygun teknik ve idari tedbirleri almakla yükümlüdür.

4.4. Veri Alıcı, ilgili kişilerin KVKK'dan doğan haklarının kullanılmasını kolaylaştırmak için gerekli tedbirleri alacaktır.

4.5. Taraflar, yetkili makamların kişisel verilerle ilgili incelemeleri ve talepleri kapsamında iş birliği yapmakla yükümlüdür.

**Madde 5 – Güvenlik Tedbirleri**

Veri Alıcı, aktarılan kişisel verilerin gizliliğini, bütünlüğünü ve erişilebilirliğini sağlamak için KVKK'nın 12. maddesi ile uyumlu şekilde gerekli tüm teknik ve idari tedbirleri almak zorundadır. Bu kapsamda en az şunları uygulamakla yükümlüdür:

Veri şifreleme,

Erişim kısıtlamaları,

Kullanıcı kimlik doğrulama sistemleri,

Loglama ve izleme sistemleri,

Veri yedekleme ve felaket kurtarma planları.

**Madde 6 – Denetim Hakkı**

Veri Gönderici, Veri Alıcı'nın işbu Sözleşme kapsamında aktarılan kişisel verileri korumak için gerekli güvenlik önlemlerini alıp almadığını denetleme hakkına sahiptir. Bu kapsamda, Veri Gönderici, önceden makul bir süre bildirmek suretiyle ve ilgili ülke mevzuatına uygun olarak, Veri Alıcı nezdinde denetim veya bağımsız üçüncü kişiler vasıtasıyla denetim gerçekleştirebilir. Veri Alıcı, denetim faaliyetlerine her türlü kolaylığı sağlamakla ve talep edilen bilgi ve belgeleri sunmakla yükümlüdür.

**Madde 7 – İhlal Bildirimi**

Veri Alıcı, aktarılan kişisel verilere ilişkin herhangi bir veri ihlali meydana gelmesi halinde, en geç 48 saat içerisinde yazılı olarak Veri Gönderici ‘ye bildirimde bulunmakla yükümlüdür. Bildirimde, ihlalin niteliği, etkilenen veri kategorileri ve kişi sayısı, alınan veya önerilen düzeltici önlemler hakkında açık bilgi verilmelidir. Veri Alıcı, ihlalin etkilerini en aza indirmek ve tekrarını önlemek için derhal gerekli önlemleri almakla da yükümlüdür.

**Madde 8 – İlgili Kişilerin Hakları ve Başvuruların Yönetimi**

Veri Alıcı, KVKK'nın 11. maddesi kapsamında ilgili kişilere tanınan hakların kullanılmasını sağlamakla yükümlüdür. İlgili kişilerden gelecek başvuru ve talepleri, Veri Gönderici ile iş birliği içerisinde ve makul bir süre içerisinde sonuçlandıracaktır. Veri Alıcı, ilgili kişilerin başvurularını reddetmesi veya başvurulara geç cevap vermesi durumunda doğabilecek idari yaptırımlardan ve tazminat taleplerinden doğrudan sorumlu olacaktır.

**Madde 9 – Sözleşmenin Süresi ve Feshi**

İşbu Sözleşme, taraflar arasında imzalandığı tarihte yürürlüğe girer ve kişisel verilerin işlenmesi ve aktarımı süresince yürürlükte kalır. Veri aktarımının sona ermesi veya taraflardan birinin işbu Sözleşmeyi haklı nedenle feshetmesi halinde Veri Alıcı, aktarılan kişisel verileri imha edecek veya Veri Gönderici ‘nin talebi doğrultusunda başka bir şekilde işlem yapacaktır. İmha işleminin tamamlandığına dair yazılı bildirim Veri Gönderici ‘ye sunulacaktır.

**Madde 10 – Uygulanacak Hukuk ve Yetkili Mahkeme**

İşbu Sözleşmenin yorumlanması ve uygulanmasından doğacak uyuşmazlıklarda Türkiye Cumhuriyeti hukuku uygulanacak olup, İstanbul (Çağlayan) Adliyesi Mahkemeleri ve İcra Daireleri yetkilidir. Taraflar, dostane çözüm için öncelikle müzakere yoluna gitmeyi kabul eder.

**Madde 11 – Gizlilik**

Taraflar, işbu Sözleşme kapsamında öğrendikleri tüm bilgi ve belgelerin gizliliğini korumakla yükümlüdür. Gizlilik yükümlülüğü, sözleşmenin herhangi bir sebeple sona ermesinden sonra da süresiz olarak devam eder.

**Madde 12 – Diğer Hükümler**

İşbu Sözleşme, taraflar arasında kişisel verilerin aktarımı hususunda tam mutabakatı ifade eder ve önceki tüm yazılı ve sözlü anlaşmaların yerine geçer. Taraflardan birinin haklarından feragat etmesi, diğer haklardan da feragat ettiği anlamına gelmez. Sözleşmede yapılacak değişiklikler yazılı ve karşılıklı mutabakatla yapılır.

Taraflar, işbu Sözleşmenin bütün hükümlerini okuduklarını, anladıklarını ve kabul ettiklerini beyan ve taahhüt ederek .../.../... tarihinde iki nüsha olarak imzalamışlardır.

**İmza:**

**Veri Gönderici: _____**

**Veri Alıcı: _____**

**Ek-1: Aktarılacak Kişisel Veri Kategorileri ve Aktarım Amaçları**

| Kişisel Veri Kategorisi | Aktarım Amacı |
|---|---|
| Kimlik Bilgileri (Ad, soyad, TCKN vb.) | Taraflar arasında kimlik doğrulama, sözleşmenin ifası |
| İletişim Bilgileri (Telefon, e-posta, adres vb.) | İletişim kurulması, bilgilendirme yapılması |
| İşlem Güvenliği Verileri (IP adresi, oturum bilgileri vb.) | Sistem güvenliğinin sağlanması, erişim kontrolü |
| Finansal Bilgiler (Banka bilgileri, IBAN vb.) | Ödeme işlemleri, finansal mutabakat süreçleri |

| Kişisel Veri Kategorisi | Aktarım Amacı |
|---|---|
| Mesleki Bilgiler (Unvan, çalıştığı kurum vb.) | Hizmet sunumu, sözleşme yönetimi |
| Hukuki İşlem ve Uyum Verileri (İmza, onay kayıtları vb.) | Yasal yükümlülüklerin yerine getirilmesi, uyuşmazlık yönetimi |
| Görsel ve İşitsel Kayıtlar (Fotoğraf, video vb.) | Kimlik tespiti, etkinlik yönetimi |
| Lokasyon Verisi (Varsa) | Lokasyon bazlı hizmetlerin sunulması |

---

**Madde 13 – Yüksek Riskli Veri Transferlerinde Ek Yükümlülükler**

Taraflar, yüksek risk taşıyan kişisel veri transferlerinde (örneğin sağlık verileri, ceza mahkûmiyeti ve güvenlik tedbirlerine ilişkin veriler) özel koruma tedbirleri almayı taahhüt eder. Bu kapsamda:

- Veri şifreleme, takma adlandırma (pseudonymization) gibi teknik önlemler alınacaktır.
- Veri transferi sırasında yalnızca gerekli olan minimum veri seti aktarılacaktır.
- Yüksek riskli veri transferi öncesinde ilgili kişinin açık rızası alınacak veya diğer hukuki aktarım şartları sağlanacaktır.
- Bu tür verilerin işlendiği sistemlere erişim, sadece yetkilendirilmiş ve eğitimli personele sağlanacaktır.

Yüksek riskli verilerle ilgili ihlaller durumunda, Veri Alıcı, derhal Veri Göndericiyi haberdar etmekle ve risk değerlendirmesi yaparak ek önlemler almakla yükümlüdür.

---

GDPR Uyumlu Eklemeler

**Madde 14 – GDPR Kapsamında Ek Hak ve Yükümlülükler**
Eğer kişisel verilerin aktarımı Avrupa Birliği ülkelerine yapılacaksa veya Avrupa Birliği vatandaşlarına ait kişisel veriler işleniyorsa, taraflar, 2016/679 sayılı Genel Veri Koruma Tüzüğü'ne (GDPR) uygun hareket etmekle yükümlüdür. Bu çerçevede:

- Veri Sahibi, GDPR'ın 15-22. maddeleri kapsamında veri erişimi, düzeltilmesi, silinmesi, işlemeye itiraz, taşınabilirlik ve sınırlama haklarını kullanabilir.
- Taraflar, GDPR'ın 5. maddesindeki veri işleme ilkelerine (hukuka uygunluk, dürüstlük, şeffaflık, amaçla sınırlılık, veri minimizasyonu, doğruluk, saklama süresi ile sınırlılık, bütünlük ve gizlilik) riayet edeceklerdir.
- Taraflar, GDPR kapsamında gerekli olduğunda Veri Koruma Etki Değerlendirmesi (DPIA) yapacak ve gerekiyorsa Yetkili Denetim Otoritelerine danışacaktır.
- Kişisel verilerin Avrupa dışına aktarımında GDPR Madde 44-50 hükümlerine uygunluk sağlanacak; özellikle yeterlilik kararı olmayan ülkelerde standart sözleşme maddeleri (SCCs) veya bağlayıcı şirket kuralları (BCRs) gibi mekanizmalar kullanılacaktır.

**EK 2: (Kurulun yayınladığı Türkiye Uygulaması için Örnek Standart Sözleşme)**

**KİŞİSEL VERİ AKTARIMI STANDART SÖZLEŞMESİ**

Taraflar:

Veri Aktarıcı: [Veri Sorumlusu Şirket Adı, Adres, VERBİS Kaydı]

Veri Alıcı: [Yurtdışındaki Alıcı Kuruluş, Ülke, Yasal Durumu]

Madde 1 – Konu

Bu sözleşmenin konusu, KVKK'nın 9. maddesi uyarınca kişisel verilerin yurtdışına aktarımına ilişkin usul ve esasların belirlenmesidir.

Madde 2 – Tanımlar

Bu sözleşmede kullanılan kavramlar, KVKK ve ilgili yönetmeliklerde yer verilen tanımlarla paralel olarak kullanılmıştır.

Madde 3 – Aktarıma Konu Veriler

İlgili kişilere ait [kimlik, iletişim, sağlık vs.] veriler aktarılacaktır. Özel nitelikli kişisel veriler ayrıca belirtilmelidir.

Madde 4 – Amaç ve Hukuki Dayanak

Veri aktarımı, [sözleşmenin ifası, yasal yükümlülük vb.] amaçları kapsamında yapılmakta olup KVKK'nın 9/2 maddesi uyarınca standart sözleşmeye dayanılarak gerçekleştirilecektir.

Madde 5 – Veri Güvenliğine İlişkin Yükümlülükler

Taraflar, kişisel verilerin gizliliğini ve bütünlüğünü korumakla yükümlüdür. Veri alıcı, KVKK'nın 12. maddesine uygun teknik ve idari tedbirleri almakla yükümlüdür.

Madde 6 – Aktarılan Verilerin Saklama Süresi

Veriler sadece belirlenen amaç kapsamında saklanacak, süresi sonunda silinecek veya anonim hâle getirilecektir.

Madde 7 – Sonraki Aktarımlar

Veri alıcı, aktarılan verileri yalnızca sözleşmede belirtilen amaç kapsamında kullanacak ve üçüncü kişilere aktarmayacaktır. Sonraki aktarımlar için ayrıca yazılı izin alınması zorunludur.

Madde 8 – Denetim ve Bilgilendirme

Veri aktarımı hakkında veri sorumlusu periyodik olarak denetim yapabilir. Kurul’a yapılan bildirim tarihinden itibaren saklama süresi boyunca tüm kayıtlar tutulacaktır.

Madde 9 – Yürürlük ve Bildirim

Sözleşme, imza tarihinden itibaren yürürlüğe girer ve beş iş günü içinde Kurul’a bildirim yapılır. Bildirim yapılmaması hâlinde KVKK uyarınca idari yaptırımlar uygulanabilir.

Ekler:

Aktarıma konu veri kategorileri listesi

Alıcı ülkeye ilişkin yeterlilik kararı durumu

Teknik ve idari tedbir listesi

İmzalar:

Taraflar, bu sözleşmeyi [fiziki/KEP/güvenli elektronik imza] yoluyla imzalamışlardır.