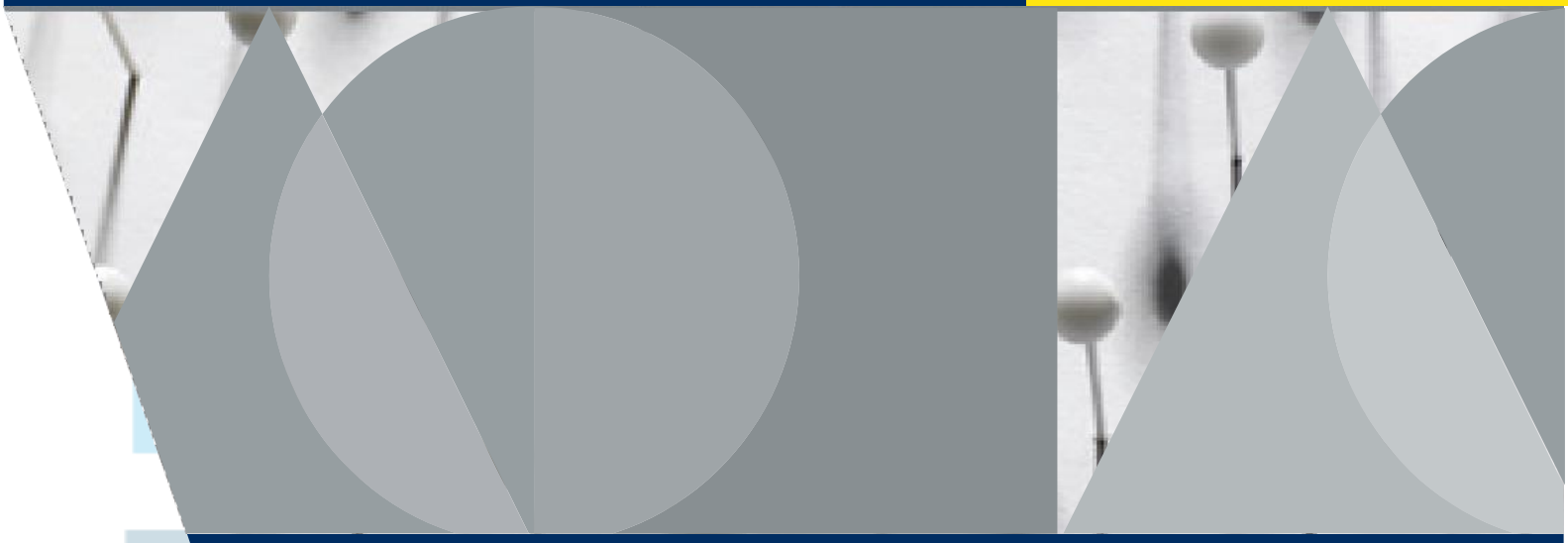
EL KİTABI



Avrupa veri koruma mevzuatı El Kitabı

2018 baskısı

FRA
EUROPEAN UNION AGENCY FOR FUNDAMENTAL RIGHTS

EUROPEAN COURT OF HUMAN RIGHTS
COUR EUROPÉENNE DES DROITS DE L'HOMME

COUNCIL OF EUROPE
CONSEIL DE L'EUROPE

EDPS

Bu el kitabı Nisan 2018'de tamamlanmıştır.

Güncellemeler ileride FRA'nın internet sitesi fra.europa.eu, Avrupa Konseyi'nin internet sitesi coe.int/dataprotection, Avrupa İnsan Hakları Mahkemesi'nin internet sitesi enhr.coe.int'de bulunan İçtihat menüsü altında ve Avrupa Veri Koruma Denetçisi'nin internet sitesi edps.europa.eu'da mevcut olacaktır.

Fotoğraf (kapak&iç kısım): iStockphoto

Luxembourg: Publications Office of the European Union, 2018

CoE:	ISBN 978-92-871-9849-5		
FRA – print:	ISBN 978-92-9491-903-8	doi:10.2811/58814	TK-05-17-225-EN-C
FRA – web:	ISBN 978-92-9491-901-4	doi:10.2811/343461	TK-05-17-225-EN-N

Lüksemburg'ta Imprimerie Centrale tarafından basılmıştır.

Baskı, klorsuz geri dönüştürülmüş kağıda (OCF) basılmıştır.

Bu el kitabı İngilizce olarak hazırlanmıştır. Avrupa Konseyi (CoE) ve Avrupa İnsan Hakları Mahkemesi (AİHM), diğer dillere yapılan çevirilerin kalitesinden sorumlu değildir. Bu el kitabında ifade edilen görüşler Avrupa Konseyini ve AİHM'i bağlamaz. El kitabı bir dizi yorum ve yönergeye atıfta bulunmaktadır. Avrupa Konseyi ve AİHM, içerikten sorumlu tutulamaz ve bu listeye dahil edilmeleri ve bu yayınların herhangi bir şekilde onaylanması anlamına gelmemektedir. AİHM kütüphanesinin internet sayfalarında echr.coe.int diğer yayınlar listelenmiştir.

Bu el kitabının içeriği, Avrupa Veri Koruma Denetçisi'nin (EDPS) resmi bir konumunu sunmamakta ve EDPS'yi yetkinliklerini kullanma konusunda bağlamamaktadır. EDPS, İngilizce dışındaki dillere yapılan çevirilerin kalitesinden sorumlu değildir.

Avrupa veri koruma hukuku
El Kitabı

2018 baskısı

ÖNSÖZ

Toplumlarımız her geçen gün daha da dijitalleşmektedir. Teknolojik gelişmelerin hızı ve kişisel verilerin nasıl işlendiği hepimizi bu değişimler ışığında etkilemektedir. Avrupa Birliği (AB) ve Avrupa Konseyi'nin gizliliği ve kişisel verileri koruyan yasal çerçeveleri yakın zamanda gözden geçirilmiştir.

Avrupa, dünya çapında veri korumasının ön safhalarında yer almaktadır. AB'nin veri koruma standartları 108 sayılı Avrupa Konseyi Anlaşması, Avrupa Birliği Genel Veri Koruma Regülasyonu ve Polis ve Ceza Yargılama Kurumlarında Veri Koruma Yönergesi de dahil ve Avrupa İnsan Hakları Mahkemesi ve Avrupa Birliği Adalet Divanı'nın ilgili içtihatları da dahil olmak üzere AB araçları.

AB ve Avrupa Konseyi tarafından yürütülen veri koruma reformları geniş kapsamlı yararlar ve bireyler ve işletmeler üzerindeki etkileri sebebiyle geniş ve bazen karmaşık olmaktadır. Bu el kitabı, özellikle çalışmalarında veri koruma meselelerini ele alan uzman olmayan hukukçular arasında farkındalığı arttırmayı ve veri koruma kuralları hakkında bilgilendirme sağlamayı amaçlamaktadır.

Bu el kitabı AB Temel Haklar Ajansı (FRA), Avrupa Konseyi (Avrupa İnsan Hakları Mahkemesi Sicili ile birlikte) ve Avrupa Veri Koruma Denetçisi tarafından hazırlanmıştır. 2014 baskısını güncellemektedir ve FRA ve Avrupa Konseyi tarafından ortak yapılan el kitapları serisinin bir parçasıdır.

Belçika, Estonya, Fransa, Gürcistan, Macaristan, İrlanda, İtalya, Monako, İsviçre ve Birleşik Krallık'ın veri koruma kurumlarına el kitabının taslak versiyonundaki yararlı geri bildirimlerinden dolayı teşekkürlerimizi sunarız. Ayrıca, Avrupa Komisyonu'nun Veri Koruma Birimi ve Uluslararası Veri Akışları ve Koruma Birimi'ne teşekkürlerimizi sunarız. Avrupa Birliği Adalet Divanı'na bu el kitabının hazırlık çalışmaları sırasında sağlanan belgeler için teşekkür ediyoruz.

Christos Giakoumopoulos

Avrupa Konseyi İnsan Hakları
Hukukun Üstünlüğü Genel Müdürü

Giovanni Buttarelli

Avrupa Veri Koruma
Denetçisi

Michael O'Flaherty

Temel İnsan Hakları
Avrupa Birliği
Ajansı Müdürü

İÇİNDEKİLER

KISALTMALAR

BCR	Bağlayıcı şirket kuralları
CCTV	Kapalı devre kamera sistemleri
CETS	Avrupa Antlaşma Serisi
Charter	Avrupa Birliği Temel Haklar Bildirgesi
CIS	Gümrük Bilgi Sistemi
ABAD	Avrupa Birliği Adalet Divanı (Aralık 2009 Avrupa Adalet Divanı öncesi)
CoE	Avrupa Konseyi
Sözleşme 108	108 sayılı Avrupa Kişisel Verilerin Otomatik İşleme Tabi Tutulması Karşısında Bireylerin Korunması Sözleşmesi
	Antlaşma 108'de değişiklik yapılması Protokolü (CETS No.223), Avrupa Konseyi Bakanlar Komitesi tarafından 18 Mayıs 2018 tarihinde Danimarka'nin Elsinore kentinde düzenlenen 128. Oturumda kabul edildi. "Modernize Edilen Antlaşma 108"e yapılan atıflar, 223 sayılı CETS Protokolü ile değiştirilen Antlaşma'ya atıfta bulunmaktadır.
CRM	Müşteri ilişkileri yönetimi
C-SIS	Merkezi Schengen Bilgi Sistemi
DPO	Veri Koruma Görevlisi
DPA	Veri Koruma Otoritesi
EAW	Avrupa Tutuklama Emri
EDPB	Avrupa Veri Koruma Kurulu
EC	Avrupa Topluluğu
AİHS	Avrupa İnsan Hakları Sözleşmesi
AİHM	Avrupa İnsan Hakları Mahkemesi
EDPS	Avrupa Veri Koruma Denetçisi
EEA	Avrupa Ekonomik Alanı
EFSA	Avrupa Gıda Güvenliği Kurumu
EFTA	Avrupa Serbest Ticaret Birliği
ENISA	Avrupa Ağ ve Bilgi Güvenliği Ajansı
ENU	Avrupa Polis Teşkilatı Ulusal Birimi
EPPO	Avrupa Savcılık Ofisi

ESMA	Avrupa Menkul Kıymetler ve Piyasalar Otoritesi
eTEN	Trans-Avrupa Telekomünikasyon Ağları
EU	Avrupa Birliği
EuroPriSe	Avrupa Gizlilik Mührü
eu-LISA	AB Büyük Ölçekli Bilişim Teknolojileri Sistemleri Ajansı
FRA	Avrupa Birliği Temel Haklar Ajansı
GDPR	Avrupa Birliği Veri Koruma Regülasyonu
GPS	Küresel Konumlandırma Sistemi
ICCPR	Uluslararası Medeni ve Siyasi Haklar Sözleşmesi
ICT	Bilgi ve iletişim teknolojisi
ISP	İnternet servis sağlayıcısı
JSB	Ortak Denetim Kurumu
NGO	Sivil Toplum Kuruluşu
N-SIS	Ulusal Schengen Bilgi Sistemi
OECD	İktisadi Kalkınma ve İşbirliği Örgütü
OJ	Resmi Gazete
PIN	Kişisel Kimlik Numarası
PNR	Yolcu isim kaydı
SCG	Denetim Koordinasyonu Grubu
SEPA	Ortak Euro Ödeme Bölgesi
SIS	Schengen Bilgi Sistemi
SWIFT	Dünya Bankalararası Mali İletişim Topluluğu
TEU	Avrupa Birliği Anlaşması
TFEU	Avrupa Birliği'nin İşleyişi Hakkında Antlaşma
UDHR	İnsan Hakları Evrensel Beyannamesi
UN	Birleşmiş Milletler
VIS	Vize Bilgi Sistemi

El kitabının nasıl kullanılacağı

Bu el kitabı Avrupa Birliği (AB) ve Avrupa Konseyi (CoE) tarafından veri korumasına ilişkin belirlenen kuralları açıklamaktadır. El kitabı, avukatlar, hakimler ve diğer hukukçular dahil olmak üzere veri koruma alanında uzman olmayan hukukçuların yanı sıra, sivil toplum kuruluşları (STK) gibi diğer kurumlar için çalışan bireyler gibi veri korumasına ilişkin hukuki sorunlarla karşı karşıya kalabilecek kişilere yardımcı olmak için tasarlanmıştır.

El kitabı, ilgili AB hukuku ve Avrupa İnsan Hakları Sözleşmesi'nin (AİHS) yanı sıra, Avrupa Kişisel Verilerin Otomatik İşleme Tabi Tutulması Karşısında Bireylerin Korunması Antlaşması (Antlaşma 108) ve diğer Avrupa Konseyi araçlarının ilk referans noktasıdır.

Her bölüm, ilgili bölümde ele alınan konuyla ilgili olan kanun hükümlerini belirten bir tablo ile başlamaktadır. Bu tablo hem Avrupa Konseyi ve Avrupa Birliği hukukunu hem de Avrupa İnsan Hakları Mahkemesi'nin (AİHM) ve Avrupa Birliği Adalet Divanı'nın seçili içtihatlarını içermektedir. İki farklı Avrupa düzeninin ilgili mevzuatı, ele alınan konular için geçerli olduklarında sırayla sunulmuştur. Bu yöntem, okuyucunun iki sistemin hangi konularda kesişip hangi konularda farklılık gösterdiğini anlamasına yardımcı olmaktadır. Ayrıca bu yöntem, özellikle yalnızca Avrupa Konseyi hukukuna tabi olunacağı durumlarda, okuyucunun kendi durumuna ilişkin kilit bilgileri bulmasına yardım eder. Bazı bölümlerde içeriğin tutarlı bir şekilde sunulması açısından bu sıra farklılık gösterebilir. El kitabı ayrıca Birleşmiş Milletler çerçevesinin de genel bir görünümünü sunmaktadır.

Avrupa Konseyi üyesi olan ve AİHS ile Antlaşma 108'e taraf olan AB dışı ülkelerdeki hukukçular kendilerini ilgilendiren bilgilere doğruca Avrupa Konseyi bölümlerine bakarak ulaşabilecektir. AB üyesi olmayan ülkelerdeki hukukçuların, AB Genel Veri koruma Regülasyonu'nun kabul edilmesi sebebiyle, kişisel verileri işleyip veri sahiplerine Birlik içerisinde ürün ve hizmet sunmaları veya bu veri sahiplerinin davranışlarını izlemeleri halinde AB veri koruma kurallarına tabi olacaklarını göz önünde bulundurmaları gerekmektedir.

AB Üye Ülkelerdeki hukukçuların ise her iki hukuk düzeni ile de bağlı olacaklarından her iki düzeni de göz önünde bulundurmaları gerekmektedir. Avrupa'daki veri koruma kurallarının reformu ve yenileştirmesinin hem Avrupa Konseyi (CETS Protokol 223 ile değiştirilen yeni Anlaşma 108) hem de EB (Genel Veri Koruma Regülasyonu ve 2017/680/AB Yönergesi'nin kabulü) ile paralel olarak yürütüldüğü göz önünde bulundurulmalıdır. Her iki yasal sistemdeki düzenleyiciler, iki yasal çerçeve arasında tutarlılık ve uyumluluk sağlanmasına büyük özen göstermişlerdir. Bu doğrultuda yapılan yenilikler Avrupa Konseyi ve AB veri koruma hukuku arasında daha fazla uyum sağlamıştır. Belirli bir konuda daha fazla bilgiye ihtiyaç duyan bireyler için "İleri Analiz" bölümünde özel nitelikli materyallere yer verilmiştir. Değişiklik Protokol'üün yürürlüğe gireceği tarihe kadar uygulanacak olan Anlaşma 108 ve 2001 Ek Protokol'ü için okuyucular el kitabının 2014 baskısına göz atmalıdır.

Avrupa Konseyi hukuku seçili Avrupa İnsan Hakları Mahkemesi içtihatlarına yapılan kısa referanslar ile sunulmuştur. Bu seçili içtihatlar, veri koruma meselelerine ilişkin çok sayıda Avrupa İnsan Hakları Mahkemesi'nin kararı arasından seçilmiştir.

İlgili AB hukuku, kabul edilmiş olan yasal önlemleri, antlaşmalardaki ilgili hükümleri ve Avrupa birliği Temel Haklar Şartı'nı, Avrupa Birliği Adalet Divanı içtihadında yorumlandığı şekilde içermektedir. Ek olarak, bu el kitabı, AB Üye Ülkelerine uzman tavsiyesinde bulunmak

üzere Veri Koruma Regülasyonu altında görevlendirilen ve Avrupa Veri koruma Kurulu (EDPB) tarafından 25 Mayıs 2018 tarihinden itibaren yenilenecek olan danışma organı olan 29. Çalışma Grubu tarafından kabul edilen görüş ve kılavuzları sunmaktadır. Avrupa Veri Koruma Denetçisinin görüşleri de AB hukukunun yorumlanmasında önemli görüşler sağlar ve bu nedenle el kitabına dahil edilmiştir.

Bu el kitabında açıklanan veya alıntı yapılan içtihatlar, Avrupa İnsan Hakları Mahkemesi ve Avrupa Birliği Adalet Divanı içtihat hukukunun önemli bir bölümünden örnekler vermektedir. El kitabının sonundaki kılavuzlar okuyuculara içtihat araştırmasında yardımcı olmayı amaçlamaktadır. Yer verilen Avrupa Birliği Adalet Divanı içtihatları eski Veri Koruma yönergesi ile ilgilidir. Bununla birlikte, Avrupa Birliği Adalet Divanı'nın yorumları, Genel Veri Koruma Regülasyonu tarafından belirlenen ilgili hak ve yükümlülüklere uygulanabilir olmaya devam etmektedir.

Ayrıca, mavi arka plana sahip metin kutularında varsayımsal senaryolara sahip pratik uygulama örnekleri sağlanmıştır. Bunlar ayrıca, özellikle ilgili AİHM veya ABAD içtihat hukukunun mevcut olmadığı durumlarda, Avrupa veri koruma kurallarının pratikte uygulanışını göstermektedir. Diğer metin kutulara -gri arka plana sahip olanlar- 29. Maddenin Çalışma Grubu tarafından yayımlanan mevzuat ve görüşler gii AİHM ve ABAD içtihat hukuku dışındaki kaynaklardan alınan örnekleri sunmaktadır.

El kitabı AİHS ve AB hukuku (Bölüm 1) tarafından belirlenen iki hukuk sisteminin rolünün kısa bir açıklaması ile başlar. 2. Bölümden 10. Bölüme kadar olan kısım ise aşağıdaki konuları içermektedir:

- Veri koruma terminolojisi;
- Avrupa veri koruma mevzuatının kilit kuralları;
- Avrupa veri koruma mevzuatının kuralları;
- Bağımsız denetim;
- Veri sahiplerinin hakları ve bunların uygulanışı;
- Kişisel verilerin sınır ötesi transferi ve akışı;
- Polis ve ceza yargılamasında kişisel verilerin korunması
- Spesifik alanlarda Avrupa veri koruma kuralları
- Kişisel verilerin korunmasında karşılaşılan güncel sorunlar**;**

1. Avrupa veri koruma hukukunun içeriği ve arka planı

Avrupa Birliği	Ele Alınan Konular	Avrupa Konseyi
Veri Koruma Hakkı		
Avrupa Birliğinin İşleyişine İlişkin Antlaşma, Madde 16 Avrupa Birliği Temel Haklar Bildirgesi (Bildirge), Madde 8 (kişisel veri koruma hakkı) Bireylerin kişisel verilerin işlenmesi karşısında korunması ve bu verilerin serbest dolaşımına ilişkin 95/46/EC sayılı Yönerge (Veri Koruma Regülasyonu), OJ 1995 L 281 (Mayıs 2018'e kadar yürürlükte) Cezai konularda polis ve adli işbirliği bağlamında işlenen kişisel verilerin korunmasına ilişki 2008/977/JHA sayılı Konsey Çerçeve Kararı, OJ 2008 L 350 (Mayıs 2018'e kadar yürürlükte) Kişisel verilerin işlenmesi ve bu verilerin serbest dolaşımı konusunda gerçek kişilerin korunmasına ve 95/46/EC sayılı Yönergenin yürürlükten kaldırılmasına ilişkin 2016/679 sayılı Yönetmelik (AB) 2008/977/JHA sayılı Çerçeve Konsey Kararını (Polis ve Adli Makamlarda Veri Koruması) yürürlükten kaldıran ve cezai suçların önlenmesi, soruşturulması, tespit edilmesi veya kovuşturulması veya ceza yasalarının uygulanması amacıyla yetkili makamlarca kişisel verilerin işlenmesi ile ilgili gerçek kişilerin korunmasına ilişkin 2016/680		AİHS Madde 8 (özel ve aile yaşamına, ev ve yazışmalara saygı gösterme hakkı) Kişisel Verilerin Otomatik Olarak İşlenmesi İle İlgili Bireylerin Korunması İçin Modernize Edilen Sözleşme (Modernize Edilen Sözleşme 108)

1.1 Kişisel verileri koruma hakkı

Kilit noktalar

- AİHS'nin 8. Maddesi uyarınca, bir kişinin kişisel verilerinin işlenmesiyle ilgili olarak korunma hakkı, özel be aile yaşamına, ev ve yazışmalar saygı gösterme hakkının bir parçasını oluşturur.
- Avrupa Konseyi Sözleşme 108, veri koruma ile ilgili ilk ve bugüne kadar yasal olarak bağlayıcı tek uluslararası araçtır. Sözleşme, değişiklik yapan 223 sayılı CETS Protokolünün kabulü ile tamamlanan bir modernizasyon sürecinden geçmiştir.
- AB mevzuatına göre, veri korumanın ayrı bir temel hak olduğu kabul edilmiştir. Bu aynı zamanda AB'nin İşleyişine İlişkin Antlaşma'nın 16. Maddesinde ve AB Temel Haklar Bildirgesinin 8. Maddesi'nde doğrulanmıştır.
- AB mevzuatı uyarınca veri koruma ilk kez 1995'te Veri Koruma Yönergesi ile düzenlenmiştir.
- Hızlı teknolojik gelişmeler ışığında AB, veri koruma kurallarını dijital çağa uyarlamak için 2016 yılında yeni yasalar kabul etti. Genel Veri Koruma Regülasyonu Mayıs 2018'de yürürlüğe girdi ve Veri Koruma Direktifini yürürlükten kaldırdı.
- Genel Veri Koruma Regülasyonu ile birlikte AB, kişisel verilerin yasa koyma amacıyla devlet yetkilileri tarafından işlenmesiyle ilgili kanunu kabul etti. (AB) 2017/680 sayılı Yönerge, cezai suçları önleme, soruşturma, tespit etme ve kovuşturma amacıyla kişisel veri işlemeyi yöneten veri koruma kural ve ilkelerini belirler.

1.1.1 Özel hayatın gizliliği ve kişisel verilerin korunması hakkı: Kısa bir giriş

Özel hayatın gizliliğine saygı ve kişisel veri koruma hakkı, yakından ilişkili olmasına rağmen ayrı haklardır. Avrupa hukukunda özel hayata saygı gösterilmesi hakkı olarak belirtilen özel hayatın gizliliği, 1948'de kabul edilen İnsan Hakları Evrensel Bildirgesi'nde (UDHR) korunan temel insan haklarından biri olarak ortaya çıkmıştır. UDHR'nin kabulünden kısa bir süre sonra Avrupa da bu hakkı 1950'de hazırlanan ve Taraf Ülkeler için bağlayıcı olan Avrupa İnsan Hakları Sözleşmesi (AİHS)'de doğrulamıştır. AİHS, herkesin kendi özel ve aile yaşamına, evine ve yazışmalarına saygı gösterme hakkına sahip olduğunu belirtir. Demokratik toplumlarda bu hakka herhangi bir kamu otoritesi tarafından müdahale edilmesi, kanunun veya meşru kamu menfaatinin gerekli kıldığı durumlar haricinde yasaktır.

UDHR ve AİHS, bilgisayarlar, internet ve bilgi toplumlarının yükselişinden çok öne kabul edilmiştir. Bu gelişmeler, bireylere ve toplumlara yaşam kalitesini, verimliliği ve üretkenliği arttıran pek çok fayda sağlamıştır. Aynı zamanda, özel hayata saygı gösterilmesi hakkı bakımından da pek çok risk taşımaktadırlar. Kişisel bilgilerin toplanmasını ve kullanılmasını düzenleyen belirli kurallara duyulan gereksinime yanıt olarak, bazı yargı alanlarında 'bilgi gizliliği' olarak bilinen ve başkalarınca 'right to informational self-determination'[1] olarak anılan yeni bir gizlilik kavramı ortaya

[1] Federal Alman anayasa Mahkemesi right to informational self-determination'a 1983 tarihli *Volkszählungsurteil*, BVerfGE Bd. 65, S. 1ff kararında değinmiştir. Mahkeme, informational self- determination hakkının Alman

çıkmıştır. Bu kavram, kişisel verilerin korunmasını sağlayan özel yasal düzenlemelerin geliştirilmesine yol açmıştır.

Avrupa'da veri koruması 1970lerde bazı devletler tarafından, kişisel bilgilerin kamu otoriteleri ve büyük şirketler tarafından işlenmesini kontrol etmek üzere yasaların kabul edilmesi ile başladı. [2] Daha sonra Avrupa düzeyinde[3] veri koruma araçları oluşturulmuştur ve yıllar içinde veri koruması, özel hayata saygı hakkı içerisine dahil edilmiş bir hak olmaktan çıkmıştır. AB hukuk düzeninde veri koruma, özel hayata gösterilmesi hakkının yanı sıra temel bir hak olarak kabul edilir. Bu ayrılık, bu iki hak arasındaki benzerlik ve farklılıklar sorununu gündeme getirmektedir.

Özel hayata saygı gösterilmesi hakkı ve kişisel verileri koruma hakkı yakından ilişkilidir. Her ikisi de benzer değerleri, yani bireylere kişiliklerini özgürce geliştirebilecekleri, düşünebilecekleri ve düşüncelerini şekillendirebilecekleri kişisel bir alan vererek bireylerin özerkliğini ve insan onurunu korumayı amaçlamaktadır. Dolayısıyla, her ikisi de, ifade özgürlüğü, barışçıl toplanma özgürlüğü ve din özgürlüğü gibi diğer temel özgürlüklerin kullanılması için bir ön koşuldur.

İki hak, formülleştirilmeleri ve kapsamları bakımından farklıdır. Özel hayata saygı hakkı, belirli durumlarda müdahaleyi haklı gösterebilecek bazı kamu yararı kriterlerine tabi olmak üzere, müdahaleye ilişkin genel bir yasaktan oluşur. Kişisel verilerin korunması, modern ve aktif[4] bir hak olarak görülmekte olup, kişisel veriler işlendiğinde bireyleri korumak için bir kontrol ve denge sistemi ortaya koymaktadır. Süreç, kişisel veri korumanın temel bileşenlerine, yani bağımsız denetim ve veri sahibinin haklarına[5] saygı gösterilmesine uymalıdır. AB Temel Haklar Bildirgesi'nin (Bildirge) 8. Maddesi sadece kişisel bilgilerin korunma hakkını teyit etmekle kalmayıp aynı zamanda bu hakla ilgili temel değerleri belirtmektedir. Bunlar, kişisel verilerin işlenmesinin, belirli amaçlar doğrultusunda olmasını ve ilgili kişinin rızasına veya kanunların öngördüğü meşru bir temele dayanarak yapılmasını sağlamaktadır. Bireylerin kişisel verilerine ulaşma ve bunların düzeltilmesini sağlama hakkına sahip olması gerekmektedir; bu hakla uygunluk ise bağımsız bir otorite tarafından kontrol edilmek zorundadır.

Kişisel verilerin işlenme hakkı, kişisel veriler işlendiği anda devreye girer; bu nedenle özel hayata saygı gösterme hakkından daha geniştir. Kişisel verilerin herhangi bir şekilde işlenmesi uygun korumaya tabi olacaktır. Veri koruma gizlilik üzerindeki ilişki

---

Anayasası'nda korunan temel haklardan biri olan kişiliğe saygı duyulması hakkından türediğini belirtmiştir. AİHM, 2017 tarihli bir kararında, AİHS'in 8. Maddesi'nin right to informational self-determination hakkını da kapsadığını belirtmiştir. Bkz. AİHM *Satakunnan Markkinapörssi Oy and Satamedia Oy v. Finland*, No. 931/13, 27 Haziran 2017, parag. 137.

[2] Almanya'nın Hesse Eyaleti, 1970'te yalnızca bu eyalette uygulanan ilk veri koruma yasasını kabul etti. 1973'te İsveç dünyanın ilk ulusal veri koruma kanununu kabul etti. 1980'nin sonuna doğru bazı Avrupa ülkeleri (Fransa, Almanya, Hollanda ve İngiltere) de veri koruma yasaları kabul etti.

[3] Avrupa Kişisel Verilerin Otomatik İşleme Tabi Tutulması Karşısında Bireylerin Korunması Sözleşmesi (Sözleşme 108) 1981'de kabul edilmiştir. AB, 1995 yılında ilk kapsamlı veri koruma aracını benimsemiştir: 95/46/EC sayılı verilerin işlenmesi ve serbest dolaşımı karşısında bireylerin korunması Yönergesi.

[4] Avukat General Sharpston, bunları iki ayrı hak olarak nitelendirdi: "klasik" özel hayatın korunması hakkı ve daha "modern" bir hak olan veri koruma hakkı. Bkz. ABAD'nın birleştirilmiş davaları C-92/09 ve C-93/02 *Volker und Markus Schecke GbR v. Land Hessen, Opinion of Advocate General Sharpston*, 17 Haziran 2010, parag. 71

[5] Hustinx, P., EDPS Speeches & Articles, *EU Data Protection Law: the Review of Directive 95/46/EC and the Proposed General Data Protection Regulation*, Temmuz 2013

ve etkiden bağımsız olarak her türlü kişisel veri ve veri işlenmesi ile ilgilidir. Kişisel verilerin işlenmesi, aşağıdaki örneklerde gösterildiği gibi, özel yaşam hakkını da ihlal edebilir. Bununla birlikte, veri koruma kurallarının tetiklenmesi için özel hayatın ihlal edildiğinin gösterilmesi gerekli değildir.

Özel hayatın gizliliği hakkı, bir bireyin menfaatinin veya "özel yaşamının" tehlikede olduğu durumlarla ilgilidir. Bu el kitabında gösterildiği gibi, "özel yaşam" kavramı, içtihat hukukunda, mahrem durumları, hassas veya gizli bilgileri, haklın bir bireye karşı algısını zedeleyebilecek bilgileri ve hatta bir kişinin mesleki hayatı ve toplumsal davranışlarını önemseyen bilgiler olarak geniş bir şekilde yorumlamıştır. Ancak, "özel hayata" müdahale olup olmadığının değerlendirilmesi, her olayın özelliklerine bağlıdır.

Buna karşılık, kişisel verilerin işlenmesini içeren herhangi bir işlem, veri koruma kuralları kapsamına girebilir ve kişisel veri koruma hakkını tetikleyebilir. Örneğin, bir işverenin, çalışanların isimleri ve çalışanlara ödenen ücretlerle ilgili bilgileri kaydetmesi durumunda, bu bilgilerin yalnızca kaydedilmesi özel hayata müdahale olarak değerlendirilemez. Bununla birlikte, böyle bir müdahale, örneğin işveren, çalışanların kişisel bilgilerini üçüncü şahıslara aktarması durumunda tartışılabilir. İşverenler her durumda veri koruma kurallarına uymak zorundadır, çünkü çalışanların bilgilerini kaydetmek veri işleme faaliyeti teşkil eder.

Örnek: *Dijital Haklar İrlanda*[6]'da, ABAD, AB Temel Haklar Bildirgesi'nde belirtilen, kişisel verilerin korunması ve özel hayata saygı hakkındaki temel haklar ışığında 2006/24/EC sayılı Yönergenin geçerliliği konusunda karar vermeye çağırılmıştır. Verilerin suçların önlenmesi, soruşturma ve kovuşturma amacıyla erişilebilir olmasını sağlamak için vatandaşların telekomünikasyon verilerini iki yıla kadar tutmak için kamuya açıl elektronik iletişim hizmetleri veya kamu iletişim ağlarının yönetimini gerektirmiştir. Ölçü yalnızca meta veriler ve konum verileri ve aboneyi veya kullanıcıyı tanımlamak için gerekli veri ve verilerle ilgilidir. Elektronik iletişim içeriği için uygulanmaz. ABAD, direktifi "kişisel verilerin işlenmesini[7] sağladığı için" kişisel veri korumaya yönelik temel haklara müdahale olarak görmüştür. Ayrıca direktifin özel hayata saygı hakkını[8] engellediğini tespit etmiştir. Bu durum bir bütün olarak ele alındığında, yetkili makamlarca erişilebilecek olan direktif uyarınca tutulan kişisel veriler, "günlük yaşam, kalıcı veya geçici ikamet yerleri, günlük veya diğer hareketler, yürütülen sosyal faaliyetler, bu kişilerin sosyal ilişkileri ve sıkça karşılaşılan sosyal ortamlar gibi, verileri elinde tutulan kişilerin özel yaşamlarına ilişkin çok kesin sonuçlar"[9] çıkarılmasını mümkün kılabilir. İki hakka müdahale oldukça önemli ve geniş kapsamlıdır.

ABAD, meşru bir amaç izlese de, kişisel verilerin korunması ve özel hayatın gizliliği haklarına müdahalenin ciddi olduğunu ve gerekli olanlarla sınırlı olmadığını tespit ettiği için 2006/24/EC sayılı Direktifi geçersiz ilan etmiştir.

[6] ABAD'ın birleştirilmiş davaları C-293/12 ve C-594/12; *Digital Rights Ireland Ltd v. Minister for Communications, Marine and Natural Resources and Others* and *Kärntner Landesregierung and Others* [GC], 8 Nisan 2014

[7] *A.g.e.*, para. 36.
[8] *A.g.e.*, paras. 32-35.
[9] *A.g.e.*, para. 27.

1.1.2 Uluslararası hukuki çerçeve: Birleşmiş Milletler

Birleşmiş milletler çerçevesi kişisel verilerin korunmasını temel bir hak olarak görmese de, gizlilik hakkı uluslararası hukuk düzeninde köklü bir temel haktır. UDHR'nin özel hayat ve aile yaşamına[10] saygı ile ilgili 12. Maddesi, bireyin ilk kez bir kişinin özel alanını, özellikle devletten başkalarının girmesine karşı koruma hakkını ortaya koyduğu uluslararası bir araç olduğunu ortaya koymuştur. Bağlayıcı olmamasına rağmen, UDHR uluslararası insan hakları hukukunun temel aracı olarak önemli bir yere sahiptir ve Avrupa'daki diğer insan hakları araçlarının gelişimi etkilemiştir. Uluslararası Medeni ve Siyasi Haklar Sözleşmesi (ICCPR) 1976'da yürürlüğe girmiştir. ICCPR, hiç kimsenin mahremiyetine, evine veya yazışmalarına keyfi veya yasadışı müdahale veya onur ve itibarına hukuka aykırı saldırılarda bulunulamayacağını belirtmektedir. ICCPR, taraf olan 169 ülkeyi, mahremiyet dahil, bireylerin medeni haklarının kullanılmasına saygı duymaya ve bu hakların uygulanmasını sağlamaya adayan bir antlaşmadır.

Birleşmiş Milletler, 2013'ten bu yana, yeni teknolojilerin geliştirilmesinden hareketle "dijital çağda gizlilik hakkı"dip[11] başlıklı, gizlilik konularında ve bazı eyaletlerde yapılan kitlesel gözetim hakkındaki keşiflerle ilgili iki karar aldı (Snowden keşifleri). Bu keşifler kitlesel gözetimi şiddetle kınamakta ve bu tür bir gözetimin gizlilik ve ifade özgürlüğünün temel haklarına ve canlı ve demokratik bir toplumun işleyişine olan etkisinin altını çizmektedir. Yasal olarak bağlayıcı olmasalar da gizlilik, yeni teknolojiler ve gözetim hakkındaki önemli bir uluslararası üst düzey siyasi tartışma başlatmışlardır. Ayrıca, bu hakkın geliştirilmesi ve korunması için özel hayatın gizliliği hakkı konusunda Özel bir Raportör kurulmasına yol açmışlardır. Raportörün özel görevleri arasında, gizlilik ve yeni teknolojilerden kaynaklanan zorluklarla ilgili ulusal uygulamalar ve deneyimler hakkında bilgi toplanması, en iyi uygulamaların değiş tokuş edilmesi, teşvik edilmesi ve olası engellerin belirlenmesi yer almaktadır.

Daha önceki kararlar, kitlesel gözetimin olumsuz etkilerine ve devletlerin istihbarat makamlarının yetkilerini kısıtlama sorumluluğuna odaklanırken, daha yeni kararlar Birleşmiş Milletler'deki[12] gizliliğe ilişkin tartışmalardaki kilit bir gelişmeyi yansıtmaktadır. 2016 ve 2017'de kabul edilen kararlar, istihbarat teşkilatının yetkilerini sınırlandırma ve kitlesel gözetimi kınama gereğini teyit etmektedir. Bununla birlikte, açıkça "ticari işletmelerin kişisel verileri toplama, işleme ve kullanma yeteneklerinin artmasının, dijital çağda gizlilik hakkının kullanılması için bir risk oluşturabileceğini" açıkça belirtmektedirler. Bu nedenle, devlet yetkililerinin sorumluluğuna ek olarak, kararlar özel sektörün insan haklarına saygı gösterme sorumluluğuna işaret etmekte ve şirketleri kişisel verilerin toplanması, kullanılması, paylaşılması ve saklanması ve şeffaf işleme politikaları oluşturulması konusunda bilgilendirmeleri yönünde çağrı yapmaktadır.

1.1.3 Avrupa İnsan Hakları Sözleşmesi

Avrupa Konseyi, İkinci Dünya Savaşı'nın sonunda, hukuk devleti, demokrasi, insan hakları ve

[10] Birleşmiş Milletler (BM), İnsan Hakları Evrensel Bildirgesi (UDHR), 10 Aralık 1948.

[11] Bkz. A/RES/68/167 sayılı BM Genel Kongresi, Dijital çağda özel hayatın gizliliği hakkı hakkında Karar, New York, 18 Aralık 2013 ; ve A/C.3/69/L.26/rev.1 sayılı BM Genel Kongresi, Dijital çağda özel hayatın gizliliği hakkı hakkında revize edilmiş taslak karar New York, 19 Kasım 2014

[12] BM Genel Kongresi, A/C.3/71/L.39 Rev.1 sayılı Dijital çağda özel hayatın gizliliği hakkı hakkında revize edilmiş taslak karar, New York, 16 Kasım 2016; BM, İnsan Hakları Komisyonu, dijital çağda özel hayatın gizliliği, A/HRC/34/L.7/rev.1, 22 Mart 2017

sosyal kalkınmayı teşvik etmek için Avrupa ülkelerini bir araya getirmek üzere kuruldu. Bu amaçla 1950 tarihinde 1953'te yürürlüğe giren AİHS'i kabul etti.

AİHS'e Taraf Ülkeler'in anlaşmaya uyma konusunda uluslararası yükümlülüğü bulunmaktadır. Tüm Avrupa Konseyi üyesi ülkeler artık AİHS'i sözleşme hükümlerine uygun hareket etmelerini zorunlu kılan ulusal yasalarına dahil etmiştir. Taraf Ülkeler, herhangi bir faaliyet veya yetkiyi yerine getirirken sözleşmede gösterilen haklara saygı göstermelidir. Bu yükümlülük, ulusal güvenlik için yürütülen faaliyetleri de içermektedir. Avrupa İnsan Hakları Mahkemesi'nin (AİHM) dönüm noktası kararları, ulusal güvenlik hukuku ve uygulamasının[13] hassas alanlarında devlet faaliyetlerini içermektedir. Mahkeme, gözetim faaliyetlerinin özel hayata saygılı bir girişim[14] teşkil ettiğini doğrulamaktan çekinmemiştir.

Taraf Ülkelerin AİHS uyarınca sahip oldukları yükümlülükleri yerine getirmelerini sağlamak için AİHM 1959'da Fransa'nın Strasbourg kentinde kurulmuştur. AİHM, devletlerin Sözleşme'deki yükümlülüklerini, sözleşmeyi ihlal ettiği iddiası olan bireylerden, birey gruplarından, STK'lardan veya tüzel kişilerden gelen şikayetleri dikkate alarak bu yükümlülükleri yerine getirmelerini sağlar. AİHM ayrıca bir veya daha fazla Avrupa Konseyi üyesi olan ülkenin getirdiği devletlerarası davaları başka bir üye devlete karşı da inceleyebilir.

2018 itibariyle, Avrupa Konseyi, 28'i AB üyesi olan 79 Taraf Devlet'ten oluşmaktadır. AİHM'e başvuran kişinin Taraf Ülkelerden birinin vatandaşı olması gerekmemekle birlikte, iddia edilen ihlallerin Akit Taraflardan birinin yetkisi dahilinde gerçekleştirilmesi gerektiği iddia edilmiştir.

Kişisel veri koruma hakkı, AİHS'in 8. Maddesi uyarınca korunan ve özel hayat ve aile yaşamına, ev ve yazışmalara saygı gösterilmesini garanti altına alan ve bu hakkın kısıtlanmasına izin verilen koşulları[15] ortaya koyan hakların bir parçasını oluşturur.

AİHM, veri koruma konularını içeren birçok durumu incelemiştir. Bunlar arasında, iletişimin kesilmesi[16], hem özel hem de kamu sektörleri[17] tarafından çeşitli gözetleme biçimleri ve kişisel verilerin kamu yetkililerinden[18] depolanmasına karşı korunma sayılabilir. Gizlilik hakkının kullanılması, ifade özgürlüğü ve bilgiye erişim gibi diğer hakları tehlikeye sokabileceğinden özel hayata saygı mutlak bir hak değildir. Dolayısıyla AİHM, söz konusu farklı haklar arasında bir denge bulmaya çalışmaktadır. AİHS'in 8. Maddesinin yalnızca devletlerin bu sözleşmeyi ihlal edebilecek herhangi bir eylemden kaçınmaya mecbur olmadığını, aynı zamanda özel durumlarda ve aile hayatına[19] etkin bir şekilde saygı duymalarını sağlamak için belirli yükümlülükler altında olduklarını açıkça ortaya koymaktadır. İlgili bölümlerde bu vakaların

[13] Bkz örneğin: AİHM, *Klass and Others v. Germany*, No. 5029/71, 6 Eylül 1978; AİHM, *Rotaru v. Romania* [GC], No. 28341/95, 4 Mayıs 2000 ve AİHM, *Szabó and Vissy v. Hungary*, No. 37138/14, 12 Ocak 2016.

[14] *A.g.e.*

[15] Avrupa Konseyi, European Convention on Human Rights, CETS No. 005, 1950.

[16] Bkz. Örneğin: AİHM, *Malone v. the United Kingdom*, No. 8691/79, 2 Ağustos 1984; AİHM, *Copland v. the United Kingdom*, No. 62617/00, 3 Nisan 2007, or AİHM, *Mustafa Sezgin Tanrıkulu v. Turkey*, No. 27473/06, 18 Temmuz 2017.

[17] Bkz. Örneğin: AİHM, *Klass and Others v. Germany*, No. 5029/71, 6 Eylül 1978; AİHM, *Uzun v. Germany*, No. 35623/05, 2 Eylül 2010

[18] Bkz. Örneğin: AİHM, *Roman Zakharov v. Russia*, No. 47143/06, 4 Aralık 2015; AİHM, *Szabó and Vissy v. Hungary*, No. 37138/14, 12 Ocak 2016.

[19] Bkz. Örneğin: AİHM, *I v. Finland*, No. 20511/03, 17 Temmuz 2008; AİHM, *K.U. v. Finland*, No. 2872/02, 2 Aralık 2008

birçoğu ayrıntılı olarak açıklanmaktadır.

1.1.4 Avrupa Konseyi Sözleşme 108

Bilgi teknolojisinin 1960'larda ortaya çıkmasıyla birlikte, bireylerin korunması için kişisel verileri korunması hususunda daha ayrıntılı kurallara artan bir ihtiyaç vardı. 1970'lerin ortalarına gelindiğinde, Avrupa Konseyi Bakanlar Komitesi, AİHS[20]'in 8. Maddesine atıfta bulunarak kişisel verilerin korunmasına ilişkin çeşitli kararlar almıştır. 1981'de Kişisel Verilerin Otomatik Olarak İşlenmesi Karşısında Bireylerin Korunması hakkında Sözleşme (Sözleşme 108)[21] imzaya açılmıştır.

Sözleşme 108, yargı ve kolluk kuvvetleri tarafından veri işleme dahil olmak üzere hem özel hem de kamu sektörleri tarafından gerçekleştirilen tüm veri işleme işlemlerine uygulanır. Bireyleri, kişisel verilerin işlenmesine eşlik edebilecek suistimallere karşı korur ve aynı zamanda, kişisel verilerin sınır ötesi akışını düzenlemeyi amaçlar. Kişisel verilerin işlenmesiyle ilgili olarak Sözleşmede belirtilen ilkeler, özellikle meşru ve amaca yönelik olarak verilerin adil ve hukuka uygun toplanması ve otomatik olarak işlenmesiyle ilgilidir. Bu, verilerin bu amaçlarla uyumsuz amaçlarda kullanılmaması ve gerekenden daha uzun süre saklanmaması gerektiği anlamına gelir. Ayrıca, bu ilkeler, verilerin niteliği, özellikle de yeterli, alakalı ve fazla olmamaları (orantılılık) ve doğru olmaları ile ilgilidirler.

Kişisel verilerin işlenmesi ve veri güvenliği yükümlülüklerine ilişkin garantiler sağlamanın yanı sıra, uygun yasal güvencelerin eksik olması durumunda bir kişinin ırkı, siyasi düşüncesi, sağlığı, dini, cinsel yaşamı ve sabıka kaydı gibi 'hassas' verilerinin de işlenebileceğini belirtmektedir.

Sözleşme ayrıca, bireyin kendisine ait bilgilerin saklandığını bilme ve gerekirse düzeltilmesini talep etme haklarını saklı tutmaktadır. Sözleşme'de belirtilen haklara getirilen kısıtlamalar, yalnızca devlet güvenliği veya savunma gibi tehlikelerin mevcudiyetinde mümkün olacaktır. Ayrıca, sözleşme Akit Taraflar arasında kişisel verilerin serbest akışını sağlar ve yasal düzenlemelerin eşdeğer koruma sağlamadığı ülkelere veri akışına bazı kısıtlamalar getirmektedir.

Sözleşme 108'in onaylayan ülkeler için bağlayıcı olduğu önem taşımaktadır. Ayrıca Sözleşme, AİHM'in adli denetime tabi değildir ancak AİHM içtihatlarında AİHS Madde 8 kapsamında dikkate alındığı görülmektedir. Mahkeme, yıllar içinde kişisel verilerin korunmasının özel hayatın gizliliği hakkının önemli bir parçası olduğuna karar vermiştir (Madde 8) ve temel haklara[22] bir müdahale olup olmadığına karar verirken Sözleşme 108'in ilkelerinden faydalanmıştır.

Sözleşme 108'de belirtilen genel ilke ve kuralları daha da geliştirmek için Avrupa Konseyi Bakanlar Komitesi yasal olarak bağlayıcı olmayan birkaç öneride bulunmuştur. Bu öneriler Avrupa'da veri koruma hukukunun gelişimini etkilemiştir. Örneğin, Avrupa'da yıllarca kişisel

[20] Avrupa Konseyi Bakanlar Komitesi (1973), özel sektördeki elektronik veri bankalarına karşı bireylerin mahremiyetinin korunması hakkında Karar No (73) 22, 26 Eylül 1973; Avrupa Konseyi Bakanlar Komitesi (1974), özel sektördeki elektronik veri bankalarına karşı bireylerin mahremiyetinin korunması hakkında Karar No (74) 29, 20 Eylül 1974.
[21] Avrupa Konseyi, Kişisel Verilerin Otomatik Olarak İşlenmesi Karşısında Bireylerin Korunması Hakkında Sözleşme, CETS No. 108, 1981
[22] Bkz. Örneğin, AİHM, *Z v. Finland*, No. 22009/93, 25 February 1997.

verilerin kullanımı konusunda rehberlik sağlayan tek araç Polis Tavsiyesi[23] olmuştur. Veri dosyalarının saklanması ve bu dosyalara erişimine izin verilen kişiler üzerinde net kuralların uygulanması ihtiyacı gibi önerilerde yer alan ilkeler daha da geliştirilmiş ve sonraki AB mevzuatına[24] yansıtılmıştır. Daha yeni öneriler dijital çağın zorluklarını ele almaya çalışmaktadır- örneğin, istihdam bağlamında veri işlenmesi. (9. Bölüm'e bakınız)

Tüm AB Üye Devletleri, Sözleşme 108'i onaylamıştır. 1999'da AB'nin bir taraf olmasına olanak sağlayan Sözleşme 108 değişiklikleri teklif edilmiş ancak hiçbir zaman yürürlüğe girmemiştir[25]. 2001 yılında, Sözleşme 108 Ek Protokol'ü kabul edilmiştir. Bu Ek Protokol, üçüncü ülke olarak adlandırılan taraf olmayanlara ve ulusal veri koruma denetim otoritelerinin[26] zorunlu olarak kurulmasına yönelik sınır ötesi veri akışlarına ilişkin hükümler getirmiştir.

Sözleşme 108, Avrupa Konseyi'nin Akit Tarafları tarafından katılıma açıktır. Sözleşmenin evrensel bir standart olma potansiyeli ve açık karakteriyle birlikte, küresel düzeyde veri korumanın desteklenmesi için bir temel teşkil etmektedir. Bugün itibariyle, 51 ülke Sözleşme 108'e taraftır. Bu ülkeler, Avrupa Konseyi'nin tüm üye devletleri (47 ülke); Ağustos 2013'te Avrupa dışından katılan ilk ülke olan Uruguay ve 2016 ve 2017 katılan Moritus, Senegal ve Tunus'tan oluşmaktadır.

Sözleşme yakın zamanda bir modernleşme süreci geçirmiştir. 2011 yılında yapılan bir kamuoyu yoklaması, bu çalışmanın iki ana hedefini doğrulamıştır: dijital arenada gizliliğin korunmasını güçlendirmek ve sözleşmenin takip mekanizmasını güçlendirmek. Modernleşme süreci de bu hedeflere odaklanmıştır ve Sözleşme 108'i değiştiren bir protokolün kabulü ile tamamlanmıştır (Protokol CETS No. 223). Çalışma, uluslararası veri koruma araçlarına yapılan diğer reformlara paralel olarak ve 2012 yılında başlatılan AB veri koruma kurallarına ilişkin reformlarla birlikte gerçekleştirilmiştir. Avrupa Konseyi ve AB düzeyindeki düzenleyiciler, iki yasal çerçeve arasında tutarlılık ve uyumluluk sağlanmasına büyük özen göstermişlerdir. Modernizasyon, sözleşmenin genel ve esnek karakterini korumakta ve veri koruma mevzuatında evrensel bir araç olma potansiyelini taşımaktadır. Kişisel verileri işleyen kurumların sorumluluklarını arttırırken ve daha geniş bir sorumlu tutulma mekanizması sağlarken bireylere yeni haklar sunmakta ve bazı önemli ilkeleri yeniden onaylamakta ve dengelemektedir. Örneğin, kişisel verileri işlenmekte olan bireyler, işbu veri işleme hakkında bilgi edinme ve bu işleme itiraz etme hakkına sahiptir. Çevrimiçi dünyada artan profil kullanımına karşı koymak içi, sözleşme aynı zamanda, bireye kendi görüşlerini dikkate alınmadan yalnızca otomatik işlemeye dayalı kararlara maruz kalmama hakkını da vermektedir. Akit Taraflardaki bağımsız denetim otoriteleri tarafından veri koruma kurallarının etkin bir şekilde uygulanması, sözleşmenin pratik uygulamasının merkezini oluşturur. Bu amaçla, modernize edilmiş sözleşme, denetim otoritelerinin yetki ve işlevlere sahip olma ve görevlerini yerine getirirken gerçek bağımsızlık kazanma ihtiyacının altını çizmektedir.

1.1.5 Avrupa Birliği Veri Koruma Hukuku

[23] Avrupa Konseyi Bakanlar Komitesi (1987), Üye devletlere polis sektöründe kişisel verilerin kullanımı düzenleyen Tavsiye Rec(87)15, Strazburg, 17 Eylül 1987.
[24] Avrupa Parlamentosu ve Konseyin 24 Ekim 1995 tarihli Bireylerin kişisel verilerin işlenmesi karşısında korunması ve bu verilerin serbest dolaşımına ilişkin 95/46/EC sayılı Yönerge, OJ 1995 L 281, 23 Kasım 1995
[25] 15 Haziran 1999'da Strazburg'da Bakanlar Komitesi tarafından Kabul edilen Avrupa Konseyi, Kişisel Verilerin Otomatik Olarak İşlenmesi Karşısında Bireylerin Korunması Hakkında Sözleşme, (ETS No.108)
[26] Avrupa Konseyi Kişisel Verilerin Otomatik Olarak İşlenmesi, denetim kurumları ve sınır ötesi veri akışı karşısında bireylerin korunması hakkında sözleşme Ek Protoklü, CETS No.181,2001. Sözleşme 108'in modernizasyonu ile bu Protokol, hükümleri Modernize Edilmiş Sözleşme'ye uyarlandığı ve entegre edildiği için artık uygulanmamaktadır.

AB hukuku, birincil ve ikincil AB hukukundan oluşur. Avrupa Birliği Antlaşması (AB Antlaşması) ve Avrupa Birliği'nin İşleyişi Antlaşması (ABİHA), tüm AB Üye Devletleri tarafından onaylanmıştır ve "birincil AB hukukunu" oluştururlar. AB'nin yönetmelikleri, yönergeleri ve kararları, antlaşmalar çerçevesinde bu yetki verilen AB kurumları tarafından kabul edilmiştir ve "ikincil AB hukukunu" oluştururlar.

Birincil AB hukukunda veri koruma

Avrupa Topluluklarının orijinal antlaşmaları, Avrupa Ekonomik Topluluğu'nun başlangıçta ekonomik entegrasyon ve ortak bir pazarın kurulmasına odaklanan bölgesel kuruluş olarak öngörülmesi koşuluyla, insan haklarına veya bunların korunmasına ilişkin herhangi bir referans içermemekteydi. Avrupa Topluluklarının yaratılmasının ve geliştirilmesinin temelini oluşturan -ve bugün eşit derecede geçerli olan- temel bir ilke görüşme ilkesidir. Bu ilkeye göre AB, yalnızca AB antlaşmalarında belirtildiği gibi, Üye Devletler tarafından kendisine verilen yetkilerin sınırları dahilinde hareket eder. Avrupa Konseyi'nin aksine, AB antlaşmaları temel haklar konusunda açık bir yetkinlik içermemektedir.

Avrupa Birliği kanunları kapsamındaki alanlarda insan hakları ihlalleri iddiasıyla ABAD'ın önünde dava açıldığında, ABAD anlaşmalar hakkında önemli bir yorumda bulunmuştur. Bireylere koruma sağlamak için, Avrupa hukukunun sözde temel ilkelerine temel haklar getirilmiştir. ABAD'a göre, bu genel ilkeler, ulusal anayasalarda ve insan hakları antlaşmalarında, özellikle de AİHS'de bulunan insan haklarının koruma içeriğini yansıtmaktadır. ABAD, AB hukukunun bu ilkelere uygunluğunu sağlayacağını belirtmiştir.

Politikalarının insan hakları üzerinde bir etkisi olabileceğini ve vatandaşların AB'ye 'daha yakın' hissetmelerini sağlama çabasıyla, 2000 yılında AB, Avrupa Birliği Temel Haklar Bildirgesi'ni (Bildirge) ilan etmiştir. Bildirge üye Devletler için ortak olan anayasal gelenekleri ve uluslararası yükümlülükleri sentezleyerek, Avrupa vatandaşlarının tüm medeni, siyasi, ekonomik haklarını kapsamaktadır. Bildirge'de açıklanan haklar altı bölüme ayrılmıştır: insan onuru, özgürlükler, eşitlik, dayanışma, vatandaşların hakları ve adalet.

İlk başta yalnızca siyasi bir belge olan Bildirge, 1 Aralık 2009[27]'da Lizbon Antlaşması'nın yürürlüğe girmesiyle AB birincil hukuku olarak (AB Antlaşması Madde 6) yasal olarak bağlayıcı[28] olmuştur. Bildirge'nin hükümleri, görevlerini yerine getirirken burada listelenen haklara saygı duyma mecburiyetinde bulunan AB kurum ve kuruluşlarına yöneliktir. Bildirge'nin hükümleri ayrıca AB yasalarının uygulandığı Üye Devletleri de bağlamaktadır.

Bildirge sadece özel ve aile yaşamına saygı gösterme hakkını temin etmekle kalmaz (Madde 7), ayrıca kişisel verilerin korunması hakkını da tesis eder (Madde 8). Bildirge, bu korumanın seviyesini AB hukukunda temel bir hak seviyesine açıkça yükseltmektedir. AB kurumları ve organları, AB yasalarını uygularken Üye Devletler gibi bu hakkı güvence altına almalı ve hakka saygı göstermelidir (Bildirge Madde 51). Veri Koruma Regülasyonu'ndan birkaç yıl sonra formüle edildiğinde, Bildirge'nin 8. Maddesinin önceden mevcut AB veri koruma yasasını teşkil ettiği anlaşılmalıdır. Dolayısıyla, Bildirge yalnızca açıkça Madde 8 (1)'de veri koruma hakkına değinmekle kalmaz, aynı zamanda Madde 8 (2)'deki temel veri koruma ilkelerine atıfta

[27] Avrupa Topluluklarının konsolide versiyonlarına bakınız (2012), Avrupa Birliği Antlaşması, OJ 2012 C 326; ve Avrupa Toplulukları (2012), ABİH, OJ 2012 C 326.
[28] AB (2012), Avrupa Birliği İnsan Hakları Bildirgesi, OJ 2012 C 326

bulunur. Son olarak, Bildirge'nin 8 (3). Maddesi uyarınca bu ilkelerin uygulanmasını kontrol etmek için bağımsız bir otorite gerekmektedir.

Lizbon Antlaşması'nın kabulü, sadece Bildirge'yi birincil hukuk seviyesinde bağlayıcı bir yasal belge statüsüne yükseltmek için değil, aynı zamanda kişisel veri koruma hakkını sağlama açısından da veri koruma yasasının geliştirilmesinde bir dönüm noktasıdır. Bu hak, Avrupa Birliği'nin İşleyişi Antlaşması'nın 16. Maddesinde, AB'nin genel prensiplerine adanmış antlaşma kapsamında özel olarak sağlanmıştır. 16. Maddede ayrıca, AB'ye veri koruma konularında yasama yetkinliği tanıyan yeni bir yasal dayanak yaratmaktadır. Bu önemli bir gelişmedir, çünkü AB veri kuralları -özellikle Veri Koruma Direktifi- başlangıçta iç pazarın yasal temeline ve AB içindeki verilerin serbest dolaşımının engellenmemesi için ulusal yasalara yaklaşma ihtiyacına dayanmaktadır. Avrupa Birliği'nin İşleyişi Antlaşması'nın 16. Maddesi şimdi, cezai konularda polis ve adli iş birliği dahil olmak üzere tüm AB yetkinliği konularını kapsayan, modern ve kapsamlı bir veri koruma yaklaşımı için bağımsız bir yasal temel sunmaktadır. Avrupa Birliği'nin İşleyişi Antlaşması'nın 16. Maddesi de, kendine göre kabul edilen veri kurallarına uygunluğun, bağımsız denetim otoritelerinin kontrolüne tabi olması gerektiğini beyan etmektedir. Madde 16, 2016 yılında kapsamlı veri koruma kurallarına ilişkin reformun kabul edilmesi için yasal bir temel işlevi görmüştür, örneğin Genel Veri Koruma Regülasyonu ve Polis ve Ceza Yargılaması Kurumlarında Veri Koruma Direktifi (aşağıya bakınız).

Genel Veri Koruma Regülasyonu

1995'ten Mayıs 2018'e kadar AB'nin veri koruma konusundaki yasal aracı, bireylerin kişisel verilerin işlenmesi ve serbest dolaşımı karşısında korunmasına ilişkin Avrupa Parlamentosu'nun 24 Ekim 1995 tarihli ve 95/46/EC sayılı Direktif'i olmuştur (Veri Koruma Direktifi).[29] Direktif, birçok Üye Devletin zaten ulusal veri koruma yasalarını[30] kabul ettiği ve bu ulusal yasaların uyumlaştırılarak üst düzey bir koruma sağlanması gerekliliğinin bulunduğu 1995 yılında kabul edilmiştir. Malların, sermayenin, hizmetlerin ve insanların iç pazardaki serbest dolaşımı, Üye Devletler aynı düzeyde yüksek veri koruma seviyesini oluşturamadıkça gerçekleşememekteydi.

Veri Koruma Direktifi, ulusal yasalarda ve Sözleşme 108'de yer alan veri koruma ilkelerini yansıtırken, genellikle bunları genişletmektedir. Direktif, Sözleşme 108'in 11. Maddesinde öngörülen koruma araçlarının eklenmesi olasılığına dikkat çekmiştir. Özellikle, bağımsız denetim direktifinin veri koruma kurallarının uygunluğunun arttırılması için bir araç olarak kabul edilmesi, Avrupa veri koruma hukukunun etkin işleyişine önemli bir katkı olduğunu kanıtlamıştır. Sonuç olarak, bu özellik 2001 yılında Sözleşme 108'e Ek Protokol tarafından Avrupa Konseyi yasalarına dahil edilmiştir. Bu, iki aracın yıllar boyunca birbirleri üzerindeki yakın etkileşimini ve olumlu etkisini göstermektedir.

Veri Koruma Direktifi, AB'de ayrıntılı ve kapsamlı bir veri koruma sistemi oluşturmuştur. Bununla birlikte, AB yasal sistemine göre direktifler doğrudan geçerli değildir, geçerli olabilmeleri için Üye Devletlerin ulusal yasalarına aktarılmalıdır. Kaçınılmaz olarak, Üye

[29] Bireylerin kişisel verilerin işlenmesi ve serbest dolaşımı karşısında korunmasına ilişkin Avrupa Parlamentosu'nun 24 Ekim 1995 tarihli ve 95/46/EC sayılı Direktif, OJ 1995 L 281.

[30] Almanya'nın Hesse eyaleti 1970 yılında sadece bu eyalette uygulanan dünyanın ilk veri koruma kanununu kabul etmiştir. İsvel 1973'te *Datalagen*'i; Almanya 1976'da *Bundesdatenschutzgestez*'i; Fransa 1977'de *Loi relatif à l'informatique, aux fichiers et aux libertés*'i kabul etmiştir. Birleşik Krallık'ta Veri Koruma Yasası 1984'te kabul edildi. Son olarak Hollanda, *Wet Persoonregistraties*'i 1989'da kabul etti.

Devletler direktifin hükümlerini aktarmada bir takdir yetkisine sahiptir. Direktifin tam bir uyum[31] sağlama (ve tam bir koruma seviyesi) sağlaması gerekmesine rağmen, uygulamada Üye Devletler'de farklı şekilde aktarılmıştır. Bu durum, AB genelinde farklı veri koruma kurallarının oluşturulmasına ve ulusal yasalarda farklı şekilde yorumlanan tanımlara ve kurallara yol açmıştır. Uygulama düzeyleri ve yaptırımların ciddiyeti Üye Devletler arasında da değişmiştir. Son olarak, 1990'lı yılların ortalarında direktifin hazırlanmasından bu yana bilgi teknolojisinde önemli değişiklikler olmuştur. Birlikte ele alındığında, bu nedenler AB veri koruma mevzuatında reform yapılmasına neden olmuştur.

Reform, yıllarca süren yoğun tartışmaların ardından Nisan 2016'da Genel Veri Koruma Regülasyonu'nun kabul edilmesine yol açmıştır. AB veri koruma kurallarının modernleştirilmesinin gerekliliği konusundaki tartışmalar Komisyon'un 2009 yılında kişisel verilerin korunmasına ilişkin temel haklar için gelecekteki yasal çerçeve hakkında bir kamu istişaresi başlatması ile başlamıştır. Tüzük teklifi, Avrupa Parlamentosu ve AB Konseyi arasında uzun bir yasama müzakere süreci başlatarak Ocak 2012'de Komisyon tarafından yayınlanmıştır. Kabul edildikten sonra ise, Genel Veri Koruma Regülasyonu için iki yıllık bir geçiş süreci sağlanmıştır. Veri Koruma Direktifi'nin yürürlükten kaldırıldığı 25 Mayıs 2018 tarihinde ise Tüzük tam olarak uygulanabilir hale gelmiştir.

2016 yılında Genel Veri Koruma Regülasyonu'nun kabulü, AB veri koruma mevzuatını modernize etmiş, dijital çağın ekonomik ve sosyal zorlukları bağlamında temel hakların korunmasına elverişli hale getirmiştir. GDPR, Veri Koruma Direktifi'nde öngörülen verilerin temel ilkelerini ve haklarını korur ve geliştirir. Ek olarak, Tüzük bazı kuruluşlara tasarım ve varsayılan olarak veri koruması uygulanması yapılması, belirli durumlarda Veri Koruma Sorumlusu atanması, veri taşınabilirliği konusunda yeni yükümlülüklere uyulması gibi bazı sorumluluklar yüklemiştir. AB yasalarına göre, düzenlemeler doğrudan uygulanabilmektedir ve ulusal uygulamaya gerek yoktur. Böylece Genel Veri Koruma Regülasyonu, AB genelinde tek bir veri koruma kurallar bütünü oluşturmaktadır. Bu fürum, AB genelinde tutarlı veri koruma kuralları oluşturur ve ekonomik aktörlerin ve bireylerin "veri sahibi" olarak yararlanabileceği bir yasal bir kesinlik ortamı oluşturur.

Genel Veri Koruma Regülasyonu doğrudan uygulanabilir olmakla birlikte, Üye Devletlerin mevcut ulusal veri koruma yasalarının Tüzüğe tam olarak uyum sağlaması için güncellenmesi beklenirken 10. Beyan'da yer alan bazı özel hükümler bakımından takdir yetkisi saklı tutulmuştur. Tüzük'te belirlenen ana kurallar ve ilkeler ile bireylere sağladığı güçlü haklar, el kitabının büyük bir bölümünü oluşturmakta ve aşağıdaki bölümde sunulmaktadır. Düzenlemenin bölgesel anlamda kapsamlı kuralları vardır. AB'de kurulan işletmeler için geçerlidir ve AB'deki veri konularına mal veya hizmet sunan veya davranışlarını izleyen AB'de kurulmamış denetleyici ve işlemciler için de geçerlidir. Birkaç denizaşırı teknoloji işletmesi, Avrupa pazarında ve milyonlarca AB müşterisinde önemli bir paya sahip olduğu için, bu kuruluşları AB veri koruma kurallarına tabi tutmak, bireylerin korunmasını sağlamak ve aynı zamanda bir faaliyet alanı sağlamak açısından önem taşımaktadır.

Kolluk kuvvetlerinde veri koruma – 2016/680 sayılı Direktif

Kaldırılan Veri Koruma Direktifi, kapsamlı bir veri koruma rejimi sağlamıştır. Bu rejim, Genel

[31] ABAD Birleştirilmiş davalar C-468/10 and C-469/10, *Asociación Nacional de Establecimientos Financieros de Crédito (ASNEF) and Federación de Comercio Electrónico y Marketing Directo (FECEMD) v. Administración del Estado*, 24 November 2011, para. 29.

Veri Koruma Regülasyonu'nun kabul edilmesiyle daha da geliştirilmiştir. Kapsamlı olmakla birlikte, yürürlükten kaldırılan Veri Koruma Direktifi'nin uygulama alanı iç pazarda yer alan faaliyetlerle ve kolluk kuvvetlerinin dışındaki kamu otoritelerinin faaliyetleriyle sınırlıdır. Dolayısıyla, veri koruma ve diğer meşru menfaatler arasında gerekli açıklığı ve dengeyi sağlamak ve belirli sektörlerde özellikle ilgili zorlukları karşılamak için özel araçların benimsenmesi gerekmiştir. Bu durum, kişisel verilerin kolluk kuvvetleri tarafından işlenmesini düzenleyen kurallar için de geçerlidir.

Bu konuyu düzenleyen ilk AB yasal aracı, polis ve cezai konularda adli iş birliği konusunda 2008/877/JHA sayılı Konsey Çerçeve Kararı olmuştur. Bu Kararın kuralları, yalnızca Üye Devletler arasında değişim yapılırken yalnızca polis ve adli verilere uygulanmaktadır. Kişisel verilerin yasa uygulayıcı tarafından yerel olarak işlenmesi, uygulama kapsamı dışında tutulmuştur.

Cezai suçların önlenmesi, soruşturulması, tespit edilmesi veya kovuşturulması veya cezai yaptırımların uygulanması ve bu verilerin serbest dolaşımı[32] amacıyla, yetkili makamlarca kişisel verilerin işlenmesiyle ilgili gerçek kişilerin korunmasına ilişkin 2016/680 sayılı Polis ve Ceza Yargılaması Makamları için Veri Koruma Direktif'i bu durumu düzeltmiştir. Genel Veri Koruma Regülasyonu'na paralel olarak kabul edilen Direktif, 2008/977/JHA sayılı Çerçeve Kararı yürürlükten kaldırmış ve yasaların uygulanması bağlamında kapsamlı bir kişisel veri koruma sistemi kurmuştur; aynı zamanda kamu güvenliği ile ilgili veri işlemenin özelliklerini kabul etmiştir. Genel Veri Koruma Regülasyonu, bireyleri kişisel verilerin işlenmesi karşısında korumak ve bu verilerin AB içinde serbest dolaşımını sağlamak için genel kurallar koyarken, Direktif, cezai konularda adli iş birliği ve polis iş birliğine yönelik bazı özel kurallar koymaktadır. Yetkili bir makamın, cezai suçların önlenmesi, soruşturulması, tespit edilmesi veya kovuşturulması amacıyla kişisel verilerin işlemesi durumunda 2016/680 sayılı Direktif uygulanacaktır. Yetkili makamın kişisel verileri yukarıda belirtilenlerin dışındaki amaçlar için işlemesi durumunda, Genel Veri Koruma Regülasyonu kapsamındaki genel kurallar uygulanacaktır. Öncekinden farklı olarak (2008/977/JHA sayılı Konsey Çerçeve Kararı), 2016/680 sayılı Direktifin uygulama kapsamı, kişisel verilerin yasa uygulayıcı makamlar tarafından yerel olarak işlenmesini kapsamaktadır ve bu tür verilerin Üye Devletler arasındaki değişimiyle sınırlı değildir. Ek olarak Direktif, bireylerin hakları ile güvenlikle ilgili işlemlerin meşru amaçları arasında bir denge kurmaya çalışmaktadır.

Bu amaçla Direktif, Genel Veri Koruma Regülasyonu'nda yer alan kural ve ilkeleri yakından takip ederek, kişisel verilerin korunma hakkını ve veri işlemeyi içermesi gereken temel ilkeleri onaylamaktadır. Bireylerin hakları ve denetleyicilere uygulanan yükümlülükler -örneğin, veri güvenliği, tasarım ve varsayılan olarak veri koruma ve veri ihlali bildirimleriyle ilgili olarak- Genel Veri Koruma Regülasyonu'ndaki hak ve yükümlülüklere benzemektedir. Direktif ayrıca, yasa koyucu makamlar tarafından profil oluşturma tekniklerinin kullanılması gibi bireyler üzerinde özellikle ağır etki yaratabilecek ortaya çıkan ciddi teknolojik zorlukları da dikkate almakta ve ele almaya çalışmaktadır. Prensip olarak, yalnızca profil oluşturma dahil olmak üzere otomatik işlemeye dayalı kararlar yasaklanmalıdır[33]. Ayrıca, hassas verilere dayalı olmamalıdırlar. Bu ilkeler, Direktif'te belirtilen belirli istisnalara tabidir. Ek olarak böyle bir işlem hiç kimseye karşı[34] ayrımcılığa neden olmamalıdır.

[32] Avrupa Parlamentosu ve Konseyi'nin 27 Nisan 2016 tarihli Gerçek kişilerin kişisel verilerin yetkili kurumlar tarafından suçların önlenmesi, soruşturulması, tespiti, kovuşturulması veya cezai yaptırımların uygulanması ve bu verilerin serbest dolaşımı karşısında korunmasına ilişkin 2016/680 sayılı Direktif'I, IJ L 119, 4 Mayıs 2016
[33] Polis ve Ceza Yargılaması Kurumları için Veri Koruma Direktifi, Madde 11(1).
[34] *A.g.e.*, Art. 11 (2) and (3).

Direktif ayrıca veri sorumlularının hesap verme sorumluluğunu sağlamak için kurallar içermektedir. Veri koruma kurallarına uyumu izlemek, yükümlülüklerini yerine getiren işletmeyi ve çalışanları bilgilendirmek ve tavsiyede bulunmak ve denetim otoritesi ile iş birliği yapmak için bir veri koruma görevlisi belirlemelidirler. Polis ve ceza adaleti sektöründe kişisel verilerin işlenmesi şimdi bağımsız denetim otoritelerinin denetimine tabidir. Hem genel veri koruma yasal rejimi hem de kolluk kuvvetleri ve cezai meseleler için özel veri koruma rejimi, AB Temel Haklar Şartı'nın gereklerine eşit şekilde uymalıdır.

Polis ve Ceza Adaleti Makamları için Veri Koruma Direktifi tarafından kurulan adli iş birliği ve polis bağlamında veri işleme konusundaki özel rejim, 8. Bölümde ayrıntılı olarak açıklanmaktadır.

Gizlilik ve elektronik haberleşme Direktifi

Elektronik haberleşme sektöründe özel veri koruma kurallarının oluşturulması da gerekli görülmüştür. İnternetin gelişmesiyle birlikte sabit hat ve mobil telefon olarak, kullanıcıların gizlilik haklarına sahip olmalarını sağlamak önem taşımaktaydı. Kişisel verilerin işlenmesi ve elektronik iletişimde gizliliğin korunması ile ilgili 2002/58/EC[35] sayılı Direktif (Gizlilik ve elektronik iletişim veya e-Gizlilik hakkında Direktif), bu ağlardaki kişisel verilerin güvenliği, veri ihlallerinin bildirimi ve iletişimin gizliliği kurallarını belirlemektedir.

Güvenlik konusunda, elektronik iletişim hizmetleri operatörleri, diğerlerinin yanı sıra, kişisel verilere erişimin yalnızca yetkili kişilerle sınırlı olmasını sağlamalı ve kişisel verilerin yok edilmesini, kaybolmasını veya kazara hasar görmesini önlemek[36] için önlemler almalıdır. Kamu iletişim ağının güvenliğinin belirli bir ihlal riski olduğunda, operatörler aboneleri risk hakkında bilgilendirmelidir[37]. Uygulanan güvenlik önlemlerine rağmen, bir güvenlik ihlali meydana gelirse, operatörler kişisel veri ihlali direktifinin uygulanması ve uygulanmasına görevli yetkili ulusal makamı bilgilendirmelidir. Operatörlerin, özellikle ihlalin kendi kişisel verilerini veya gizliliğini olumsuz yönde etkilemesi muhtemel olan hallerde kişisel veri ihlallerini bireylere bildirmeleri istenebilmektedir[38]. İletişimin gizliliği, iletişimin ve meta verilerinin dinlenmesi, kaydedilmesi, saklanması veya herhangi bir şekilde denetlenmesi veya durdurulmasının ilke olarak yasaklanmasını gerektirmektedir. Direktif ayrıca, kullanıcılar rıza vermediği ve bilgisayarlarda ve cihazlarda "çerezlerin" depolanmasıyla ilgili kurallar içermeyen, istenmeyen iletişimleri de (genellikle "spam" olarak adlandırılır) yasaklamaktadır. Bu temel olumsuz yükümlülükler, iletişimin gizliliğinin, Bildirge'nin 7. Maddesinde belirtilen özel hayata saygı gösterme hakkının ve Bildirgenin 8. Maddesinde yer alan kişisel veri koruma hakkının korunması ile önemli ölçüde bağlantılı olduğunu açıkça göstermektedir.

Ocak 2017'de, Komisyon, özel hayata saygı ve kişisel verilerin elektronik iletişimde korunmasına ilişkin bir e-Gizlilik Direktifi yayınlamıştır. Bu reform, elektronik haberleşmeyle ilgili kuralları Genel Veri Koruma Regülasyonu altında oluşturulan yeni veri koruma rejimi ile uyumlu hale getirmeyi amaçlamaktadır. Yeni düzenleme AB genelinde doğrudan uygulanacaktır; telekomünikasyon operatörleri ve işletmeleri AB genelinde netlik, yasal

[35] Avrupa Parlamentosu'nun ve Konseyin kişisel verilerin işlenmesi ve elektronik haberleşmede veri gizliliği hakkında 12 Temmuz 2002 tarihli ve 2002/58/EC sayılı Direktifi, OJ 201 (Gizlilik ve elektronik iletişim veya e-Gizlilik hakkında Direktif)
[36] Gizlilik ve elektronik haberleşme Direktifi, Madde 4(1).
[37] *A.g.e.*, Art. 4 (2).
[38] *A.g.e*, Art. 4 (3).

kesinlik ve tek bir kural düzeninin varlığından yararlanırken tüm bireyler elektronik iletişimin aynı seviyede korunmasından faydalanacaktır. Elektronik iletişimin gizliliği konusunda önerilen kurallar, e-Gizlilik Direktifi kapsamına olmayan elektronik iletişim hizmetleri sunan yeni oyuncular için de geçerli olacaktır. Sonuncusu yalnızca geleneksel telekomünikasyon hizmetleri sağlayıcılarını kapsamaktadır. Mesaj göndermek için veya çağrı yapmak için Skype, WhatsApp, Facebook Messenger ve Viber gibi hizmetlerin kullanımında büyük bir alım yapılması durumunda, bu genel kullanım (OTT hizmetleri) artık düzenleme kapsamına girecek ve veri koruma, gizlilik ve güvenlik konusundaki kurallara uymak zorunda kalacaktır. Bu el kitabının yayımlandığı tarihte e-Gizlilik kuralları hakkındaki yasama faaliyeti hala sürmekteydi.

45/2001 sayılı Yönetmelik

Veri Koruma Direktifi yalnızca AB Üye Ülkeleri için geçerli olabileceğinden, kişisel verilerin AB kurumları ve organları tarafından işlenmesi için veri korumasını sağlama amacıyla ek bir yasal araca ihtiyaç duyulmaktaydı. Topluluk kurumları ve organları tarafından kişisel verilerin işlenmesin karşısında bireylerin korunmasına ve bu verilerin serbest dolaşımına ilişkin 45/2001 (Avrupa Konseyi) sayılı Yönetmelik (AB Kurumları Veri Koruma Yönetmeliği) bu görevi yerine getirmektedir[39].

45/2001 sayılı Yönetmelik, genel AB veri koruma rejiminin ilkelerini yakından takıp etmekte ve bu ilkeleri, işlevlerini yerine getirirken AB kurumları ve organları tarafından yürütülen veri işlemlerine uygulamaktadır. Ayrıca, hükümlerinin uygulanmasını izlemek için bağımsız bir denetim otoritesi, Avrupa Veri Koruma Denetçisi (EDPS) kurulmaktadır. EDPS, denetleme yetkilerine ve kişisel kurumları AB kurum ve kuruluşlarında işlenmesini izleme ve veri koruma kurallarının ihlal edildiği iddiasıyla ilgili şikayetleri duyma ve soruşturma görevine sahiptir. Ayrıca EDPS, AB kurumlarına ve organlarına, kişisel verilerin korunmasına ilişkin tüm konularda, yeni mevzuat tekliflerinden, veri işleme ile ilgili iç kuralların oluşturulmasına kadar danışmanlık hizmeti vermektedir.

Ocak 2017'de, Avrupa Komisyonu, mevcut yönetmeliği yürürlükten kaldıracak olan AB kurumları tarafından veri işleme konusunda yeni bir düzenleme önerisi sunulmuştur. E-Gizlilik Direktifi reformunda olduğu gibi, 45/2001 sayılı Yönetmelik'te reformun kuralları, Genel Veri Koruma Yüzüğü altında oluşturulan yeni veri koruma rejiminde modernize edilecek ve uyumlu hale getirilecektir.

ABAD'ın Rolü

ABAD, bir ÜYE Devletin AB veri koruma yasası kapsamındaki yükümlülüklerini yerine getirip getirmediğinin belirlenmesinde ve Üye Devletler genelinde etkili ve düzgün bir şekilde uygulanmasını sağlamak için AB mevzuatının yorumlanmasına yetkisine sahiptir. Veri Koruma Direktifi'nin 1995'te kabul edilmesinden bu yana, veri koruma ilkelerinin kapsamını ve anlamını ve Bildirge'nin 8. Maddesinde yer alan kişisel veri korumaya ilişkin temel hakkı açıklığa kavuşturan kayda değer bir içtihat mevzuatı oluşmuştur. Direktif yürürlükten kaldırılmış ve yerine yeni bir yasal araç -Genel Veri Koruma Regülasyonu- gelmiş olsa bile, önceden var olan içtihat Veri Koruma Direktifinin ana prensip ve konseptleri GDPR'da yer

[39] Avrupa Parlamentosu ve Avrupa Konseyinin Topluluk kurumları ve organları tarafından kişisel verilerin işlenmesi karşısında bireylerin kişisel verilerin işlenmesi ve bu verilerin serbest dolaşımına ilişkin 45/2001 sayılı 18 Aralık 2000 tarihli Yönetmelik, OJ 2001 L8

aldığı ölçüde AB Veri Koruma İlkelerin yorumlanmasında ve uygulanmasında kullanılmaktadır.

1.2 . Kişisel verilerin korunması hakkının sınırlandırmaları

Kilit Noktalar

- Kişisel verilerin koruması hakkı mutlak bir hak değildir; genel menfaatler veya başkalarının hak ve özgürlüklerini korumak için gerekli olduğu hallerde sınırlandırılabilmektedir.
- Özel hayata ve kişisel verilerin korunmasına saygı hakkının sınırlandırılmasına ilişkin şartlar AİHS'in 8. Maddesinde ve Bildirgenin 52 (1). Maddesinde listelenmiştir. AİHM içtihatları ve ABAD aracılığıyla geliştirilmiş ve yorumlanmıştır.
- Avrupa Konseyi veri koruma hukuku uyarınca kişisel verilerin işlenmesi ancak aşağıdaki hallerle hukuki müdahale teşkil edecektir:
  - Kanuna uygunluk;
  - Meşru amaç izlenmesi;
  - Temel haklar ve özgürlüklerin özüne saygı gösterilmesi;
  - Demokratik toplumun meşru amacına ulaşması için gerekli ve orantılı olması.
- AB hukuk düzeni, Bildirge tarafından korunan temel haklar üzerindeki sınırlandırmaların uygulanmasında benzer koşullar talep etmektedir. Kişisel veri koruması dahil olmak üzere temel haklar üzerindeki sınırlandırmalar ancak aşağıdakilerin varlığı halinde hukuka uygun sayılacaktır:
  - Kanuna uygunluk;
  - Hakkın özüne saygı gösterilmesi;
  - Orantılılık prensibine konu olması veya gerekli olması; ve

AB tarafından tanınan bir genel çıkar hedefi veya başkalarının haklarını koruma ihtiyacı.

Bildirgenin 8. Maddesi uyarınca kişisel verilerin korunmasına ilişkin temel hak, mutlak bir hak değildir; "ancak toplumdaki işleviyle ilgili olarak dikkate alınmalıdır.[40]" Bu nedenle, Bildirge'nin 52 (1). Maddesi, Bildirge'nin 7. Ve 8. Maddelerinde belirtilenler gibi kısıtlamalar hak ve özgürlüklerin özüne, orantılılık ilkesine uygun ve gerekli olduğu ve AB tarafından tanınan genel çıkar hedeflerinin veya başkalarının hak ve özgürlüklerinin korunmasına uygun olduğu ölçüde mümkün olacaktır[41]. Benzer şekilde, AİHS sisteminde veri koruması, 8. Maddeyle güvence altına alınmıştır ve bu hakkın kullanılması meşru bir amaç için gerekli olduğunda sınırlandırılabilmektedir. Bu bölüm, AİHS içtihadında açıklandığı gibi AİHS kapsamındaki müdahale koşullarının yanı sıra, Bildirgenin 52. Maddesi uyarınca olan yasal sınırlama koşullarına atıfta bulunmaktadır.

1.2.1 AİHM uyarınca meşru müdahale için gerekenler

Kişisel verilerin işlenmesi, AİHS'in 8. Maddesi ile korunan, veri sahibinin özel hayata saygı hakkı ile etkileşime girmesine neden olabilmektedir[42]. Yukarıda açıklandığı gibi (bkz. Bölüm

[40] Bkz. Örneğin, ABAD Birleştirilmiş davaları C-92/09 and C-93/09, *Volker und Markus Schecke GbR and Hartmut Eifert v. Land Hessen* [GC], 9 November 2010, para. 48.
[41] *A.g.e.*, para. 50.
[42] AİHM, S. *and Marper v. the United Kingdom* [GC], Nos. 30562/04 ve 30566/04, 8 Aralık 2008, parag. 67

1.1.1. ve Bölüm 1.1.4.), AB hukuk düzeninin aksine, AİHS, kişisel verilerin korunmasını ayrı bir temel hak olarak kabul etmemektedir. Aksine, kişisel verilerin korunması, özel hayata saygı hakkı altında korunan hakların bir parçasını oluşturmaktadır. Bu nedenle, kişisel verilerin işlenmesini içeren hiçbir işlem, AİHS'in 8. Maddesinin kapsamına girmemektedir. 8. Maddenin tetiklenmesi için öncelikle, özel bir çıkar veya bir kişinin özel hayatının tehlikeye atılıp atılmadığı tespit edilmelidir. AİHM, içtihatlar ile "özel yaşam" kavramını, mesleki yaşamın ve kamu davranışının bile yönlerini kapsayan geniş bir kavram olarak ele almıştır. Ayrıca, kişisel verilerin korunmasının, özel hayata saygı gösterilmesi hakkının önemli bir parçası olduğuna karar vermiştir. Bununla birlikte, özel hayatın geniş yorumlanmasına rağmen her veri işleme türü 8. Maddede korunan haklardan ödün vermeyecektir.

AİHM, söz konusu işlemlerin bireylerin özel hayata saygı gösterilmesi hakkını etkilediğini düşünüldüğünde, müdahalenin haklı olup olmadığını incelemektedir. Özel hayata saygı gösterilmesi hakkı mutlak bir hak değildir, ancak diğer kişilerin (özel çıkarlar) veya bir bütün olarak toplumun (kamu çıkarları) olsun, diğer meşru çıkarlar ve haklarla dengelenmeli ve bunlarla uzlaştırılmalıdır.

Bir müdahalenin haklı olabileceği kümülatif koşullar şunlardır:

Kanuna uygunluk

AİHM içtihadına göre, müdahale, belirli niteliklere sahip bir iç hukuk hükmüne dayanıyorsa kanuna uygun olacaktır. Kanun, "ilgili kişilerce ulaşılabilir olmalı ve etkileri öngörülebilmeli.[43]" Kural, herhangi bir bireye -ihtiyaç duyulması halinde- davranışını düzenlemek için yeterli kesinlik ile düzenlenmişse, öngörülebilir sayılmaktadır[44]. Ayrıca "'yasa' için gereken kesinlik derecesi, konusuna göre değişiklik göstermektedir.[45]"

[43] AİHM, *Amann v. Switzerland* [GC], No. 27798/95, 16 Şubat 2000, para. 50; Ayrıca AİHM, *Kopp v. Switzerland*, No. 23224/94, 25 Mart 1998, para. 55 and AİHM, *Iordachi and Others v. Moldova*, No. 25198/02, 10 Şubat 2009, para. 50

[44] AİHM, *Amann v. Switzerland* [GC], No. 27798/95, 16 Şubat 2000, para. 56; ayrıca bkz. AİHM, *Malone v. the United Kingdom*, No. 8691/79, 2 Ağustos 1984, para. 66; AİHM, *Silver and Others v. the United Kingdom*, Nos. 5947/72, 6205/73, 7052/75, 7061/75, 7107/75, 7113/75, 25 Mart 1983, para. 88.

[45] AİHM, *The Sunday Times v. the United Kingdom*, No. 6538/74, 26 Nisan 1979, para. 49; ayrıca bkz. AİHM, *Silver and Others v. the United Kingdom*, Nos. 5947/72, 6205/73, 7052/75, 7061/75, 7107/75, 7113/75, 25 Mart 1983, para. 88.

Örnekler: *Rotaru v. Romania*[46]'da başvuran, Romanya İstihbarat Servisi'nin kişisel bilgilerini içeren bir dosyayı tutması ve kullanması nedeniyle özel hayata saygı gösterilmesi hakkının ihlal edildiğini iddia etmiştir. AİHM, iç hukukun, ulusal güvenliği etkileyen gizli bilgi dosyalarının toplanmasına, kaydedilmesine ve arşivlenmesine izin verirken, yetkililerin takdirine bağlı olarak kalan bu yetkilerin kullanımına herhangi bir sınır getirmediğini tespit etmiştir. Örneğin, iç hukuk, işlenebilecek bilgi türünü, gözetim önlemlerinin alınabileceği insan kategorilerini, bu önlemlerin alınabileceği koşulları veya izlenecek prosedürleri tanımlamamıştır. Mahkeme bu nedenle, iç hukukun AİHS'in 8. Maddesi uyarınca öngörülebilirlik şartına uymadığı ve bu maddenin ihlal edildiği sonucuna varmıştır.

Taylor-Sabori v. Birleşik Krallık[47]'da başvuran, polis gözetiminin hedefi olmuştur. Polis, başvuranın çağrı cihazının bir "klon"unu kullanarak kendisine gönderilen mesajları arayabilmiştir. Başvuran tutuklanmış ve reçeteli bir ilaç temin etmek için komplo kurmakla suçlanmıştır. Soruşturmanın başvuran aleyhine olan kısmı, polisin yazdığı başvurana ait çağrı mesajlarının yazılı notlarından oluşmaktaydı. Bununla birlikte, başvuranın yargılaması sırasında, özel bir telekomünikasyon sistemi yoluyla iletilen mesajlarının ele geçirilmesini düzenleyen bir hüküm İngiliz hukukunda mevcut değildir. Bu nedenle müdahale "kanuna uygun" olmamıştır. AİHM, bunun AİHS'in 8. Maddesini ihlal ettiği sonucuna varmıştır.

Vukota-Bojic v. İsviçre[48], sigorta şirketi tarafından görevlendirilen özel araştırmacılar tarafından yapılan bir sosyal sigorta talebinin gizli gözetimi ile ilgilidir. AİHM, şikayette belirtilen gözetim önleminin bir özel sigorta şirketi tarafından sipariş edilmiş olmasına karşın, söz konusu şirkete Devlet tarafından zorunlu sağlık sigortasından kaynaklanan yararları sağlama ve sigorta primlerini tahsil etme hakkının tanındığını belirtmiştir. Devlet, yükümlülüklerini özel birimlere veya kişilere devrederek, sözleşmedeki sorumluluğunu ortadan kaldıramamaktadır. İç hukuk, AİHS'in 8. Maddesi uyarınca "kanuna uygun" şekilde haklara müdahale edilmesi karşısında yeterli korumayı sağlamakla yükümlüdür. Davada AİHM, iç hukukun sigorta ihtilaflarında kamu gözetim makamı olarak faaliyet gösteren sigorta şirketlerine verilen takdir yetkisinin, sigortalı kişilerin gizli gözetimini yapmak için kullandığı takdir yetkisinin kapsamını ve uygulama şeklini yeterince açık bir şekilde belirtmemesi sebebiyle AİHS'in 8. Maddesinin ihlal edildiğine karar vermiştir. Özellikle, müdahaleye karşı içermediğine kanaat getirilmiştir.

Meşru bir amaç izlenmesi

Meşru amaç, ya adı konan kamu yararlarından biri ya da başkalarının hak ve özgürlüklerinin korunması olabilmektedir. Bir müdahaleyi haklı çıkarabilecek meşru amaçlar, AİHS'in 8(2). Maddesi uyarınca, ulusal güvenlik, kamu güvenliği veya bir ülkenin ekonomik refahı, düzensizliğin veya suçun önlenmesi, sağlığın veya ahlakın korunması ve diğer kişilerin hak ve özgürlüklerinin korunmasıdır.

Örnek: Peck v. Birleşik Krallık[49]'ta başvuran, CCTV kamerasının kendisini çektiğinin

[46] AİHM, *Rotaru v. Romania* [GC], No. 28341/95, 4 Mayıs 2000, para. 57; ayrıca bkz. AİHM, *Association for European Integration and Human Rights and Ekimdzhiev v. Bulgaria*, No. 62540/00, 28 Haziran 2007; AİHM, *Shimovolos v. Russia*, No. 30194/09, 21 Haziran 2011; and AİHM, *Vetter v. France*, No. 59842/00, 31 Mayıs 2005.
[47] AİHM, *Taylor-Sabori v. the United Kingdom*, No. 47114/99, 22 Ekim 2002.
[48] AİHM, *Vukota-Bojić v. Switzerland*, No. 61838/10, 18 Ekim 2016, para. 77.

[49] AİHM, *Peck v. the United Kingdom*, No. 44647/98, 28 Ocak 2003, para. 85.

farkında olmadan sokakta bileklerini keserek intihar girişiminde bulunmuştur. CCTV kameralarını izleyen polis onu kurtarmış ve artından CCTV görüntülerini başvuranın yüzünü maskelemeden yayınlayan basın kuruluşlarına vermiştir. AİHM, başvuranın rızasını almadan veya kimliğini maskelemeden resmi makamların kamuoyuna doğrudan açıklamasını haklı çıkarak herhangi bir geçerli veya yeterli sebep bulunmadığını tespit etmiştir. Mahkeme, AİHS'in 8. Maddesinin ihlal edildiğine karar vermiştir.

Demokratik toplum için gereklilik

AİHM, "gereklilik nosyonunun, müdahalenin acil bir sosyal ihtiyaca karşılık geldiğini ve özellikle de amaçlanan meşru amaç ile orantılı olduğunu belirtmiştir."[50] AİHM, acil bir sosyal ihityacı ele almak için bir önlem gerekip gerekmediğini değerlendirirken, izlenen amaç ile ilgili olarak ilgi ve uygunluğu incelemektedir. Bu amaçla, müdahalenin ele alınmadığı takdirde toplum üzerimde zararlı bir etkiye neden olabilecek bir sorunu ele almaya çalışıp çalışmadığı, müdahalenin bu tür zararlı etkileri azaltabileceğine dair kanıt olup olmadığı ve bu konuda toplumun genel görüşlerinin ne olduğu dikkate alınabilir.[51] Örneğin, terörist hareketlerle bağlantısı olduğu tespit edilen belirli kişilerin kişisel verilerinin güvenlik hizmetleri tarafından toplanması ve saklanması, bireylerin özel hayata saygı duyma haklarına müdahaleye yol açacaktır, ancak ciddi, acil bir sosyal ihtiyaca hizmet eden bir müdahale olacaktır: ulusal güvenlik ve terörle mücadele. Gereklilik testini karşılamak için, girişimin orantılı da olması gerekmektedir. AİHM içtihadında, orantılılık, gereklilik kavramının altında ele alınmaktadır. Orantılılık, AİHS'de korunan haklara yapılan müdahalenin, izlenen meşru amacı yerine getirmek için gerekenden daha fazla ilerlememesini gerektirmektedir. Orantılılık testi yapılırken göz önünde bulundurulması gereken önemli faktörler, müdahalenin kapsamı, özellikle etkilenen kişilerin sayısı ve bireylerin haklarına, müdahalenin kapsamını veya zararlı etkilerini sınırlandırmak için uygulanan tedbirler veya uyarılardır[52].

Örnek: *Khelili v. İsviçre*[53]'de bir polis kontrolü sırasında polis, başvuranın üzerinde "Güzel, hoş kadın, otuzlu yaşlarının sonunda birlikte bir şeyler içmek ya da zaman zaman dışarı çıkmak için bir erkekle tanışmak istiyor. Tel. no […]" yazılı kartvizitler ele geçirmiştir. Başvuran, polisin bu olayın ardından polisin kendisini sürekli olarak inkar etmesine rağmen hayat kadını olarak kaydettiğini iddia etmektedir. Başvuran 'hayat kadını' ibaresinin polisin bilgisayar kayıtlarından silinmesini talep etmiştir. AİHM, bir bireyin başka bir suç işleyebileceği ihtimalinin söz konusu olduğu durumlarda polisin bu kişinin kişisel verilerini tutmanın orantılı olabileceğini kabul etmektedir. Bununla birlikte, başvuranın davasında, yasadışı fuhuş iddiası çok belirsiz ve genel olarak ortaya çıkmıştır, kişi daha önceden yasadışı fuhuştan mahkum edilmemiş olduğundan bunun devlet için AİHS'in 8. Maddesi anlamına 'acil bir sosyal ihtiyacı' karşıladığı düşünülememektedir. Yetkili makamların başvuru sahibi hakkındaki bilginin doğruluğunu ispat edememeleri ve başvuranın hakkına müdahalenin ciddiyeti göz önünde bulundurulduğunda, Mahkeme 'hayat kadını' ibaresinin polis kayıtlarında yıllarca tutulmasının demokratik toplum için gerekli olmadığına karar vermiştir. Mahkeme, AİHS'in 8. Maddesi'nin ihlal edildiğine karar vermiştir.

[50] AİHM, *Leander v. Sweden*, No. 9248/81, 26 March 1987, para. 58.
[51] Veri Koruma Çalışma Grubu Madde 29 (Çalışma Grubu Madde 29) (2014), Kolluk sektöründe gereklilik ve orantılılık kavramlarının ve veri korumanın uygulanmasına ilişkin Görüş, WP211, Bürksel, 27 Şubat 2014, syf 7-8.
[52] *A.g.e.*, pp. 9–11.
[53] AİHM, *Khelili v. Switzerland*, No. 16188/07, 18 Ekim 2011.

Örnek: *S. ve Marper v. Birleşik Krallık*[54]'ta, iki başvuran tutuklanmış ve ceza gerektiren suçlardan mahkum edilmiştir. Polis, Polis ve Ceza Kanıtı Yasası kapsamında öngörüldüğü üzere başvuranların parmak izlerini ve DNA örneklerini almıştır. Başvuranlar, daha önce hiçbir suçtan mahkum edilmemiştir: biri mahkemede beraat etmiş, ikinci başvuran aleyhindeki cezai kovuşturmalara ise devam edilmemiştir. Bununla birlikte, başvuranların parmak izleri, DNA profilleri ve doku numuneleri polis tarafından bir veri tabanında tutulmuş ve saklanmış ve ulusal mevzuat da geçerli bir zaman sınırı olmadan tutulmalarına izin vermiştir. Birleşik Krallık, verilerin tutulmasının gelecekteki suçların belirlenmesine yardımcı olduğunu ve böylece suçun önlenmesi ve tespit edilmesinin meşru amacını izlediğini savunurken, AİHM, başvuranların özel hayata saygı gösterilmesi haklarının ihlal edildiğini ileri sürmüştür. Veri korumanın temel ilkelerinin, kişisel verilerin elde edilmesinin toplama amacı ile orantılı olmasını gerektirdiği ve saklama sürelerinin sınırlı olması gerektiği hatırlatılmıştır. Mahkeme, veri tabanının yalnızca hükümlü kişilerin değil, aynı zamanda şüpheli olan ancak mahkum olmayan kişilerin de DNA profillerini içerecek şekilde genişletilmesinin Birleşik Krallık'ta suçun tespit edilmesine ve önlenmesine katkıda bulunabileceğini kabul etmiştir. Ancak.[55]

Doku örneklerinde yer alan genetik ve sağlık bilgi hazinesi göz önüne alındığında, başvuranların özel hayatın gizliliği hakkına müdahale teşkil etmektedir. Tutuklana kişilerin parmak izleri ve örnekleri alınabilir ve suçun niteliği ve ciddiyetine bakılmaksızın ve hatta hapis cezasına çarptırılmayan küçük suçlar için bile polis veri tabanında süresiz olarak tutulabilir. Ayrıca, beraat eden bireylerin verilerinin veri tabanından kaldırılması için olasılıklar sınırlıdır. Son olarak, AİHM, başvuranlardan birinin tutuklandığında on bir yaşında olduğu gerçeğine özel önem vermiştir. Hüküm giymemiş bir küçüğün kişisel verilerini korumak, savunmasızlığı ve topluma entegrasyonlarının önemi göz önünde bulundurulduğunda özellikle zararlı olabilecektir[56]. Mahkeme oybirliğiyle, tutuklamanı demokratik bir toplumda gerekli olmadığını ve özel hayata saygı gösterilmesi hakkına orantısız bir müdahale oluşturduğuna kanaat getirmiştir.

Örnek: In *Leander v. İsveç*[57]'de AİHM, iş başvurusunda bulunan kişilerin, ulusal güvenlik açısından önem taşıyan görevlerde gizli incelemelerinin, demokratik bir toplumda gerekli olma şartının aksine bir durum teşkil etmediğine karar vermiştir. Veri sahiplerinin menfaatlerinin korunması için ulusal mevzuatta öngörülen özel önlemler -örneğin parlamento ve Adalet Bakanı tarafından yapılan kontroller- AİHM'in İşveç personel kontrol sisteminin AİHS'in 8(2). Maddesi'nin gerekliliklerini karşıladığına karar vermesine sebep olmuştur. Geniş takdir marjını dikkate alarak, katılımcı devlet, ulusal güvenlik çıkarlarının bireysel çıkarlardan üstün geldiğini kabul etmeye hak kazanmıştır. Mahkeme, AİHS'in 8. Maddesi'nin ihlal edilmediğine karar vermiştir.

1.2.2 AB Temel Haklar Bildirgesi uyarınca meşru sınırlama için öngörülen koşullar

Bildirge'nin yapısı ve ifadesi AİHS'ten farklıdır. Bildirge, garantili haklara sahip girişim kavramını kullanmamaktadır; ancak Bildirge tarafından tanınan hakların kullanımına ilişkin sınırlandırmaları düzenleyen bir hüküm içermektedir.

[54] AİHM, *S. and Marper v. the United Kingdom* [GC], Nos. 30562/04 ve 30566/04, 4 Aralık 2008.
[55] *A.g.e.*, para. 119.
[56] *A.g.e.*, para. 124.
[57] AİHM, *Leander v. Sweden*, No. 9248/81, 26 March 1987, paras. 59 and 67.

Madde 52 (1) uyarınca, Bildirge tarafından kabul edilen hakların kullanılmasına ve dolayısıyla kişisel verilerin korunmasına ilişkin hakkın kullanılmasına ilişkin sınırlamalar ancak aşağıdaki durumlarda mümkündür:

- Kanunda belirtilmiş olma; ve
- Veri koruma hakkının özüne saygı duyma;ve
- Orantılılık ilkesine tabi olma ve gerekli olma[58]; ve
- Birlik tarafından tanınan genel menfaatleri karşılamaları veya başkalarının hak ve özgürlüklerini koruma ihtiyacı.

Kişisel verilerin korunması, Bildirge'nin 8. Maddesi uyarınca korunan AB hukuk düzeninde ayrı ve tek başına temel bir hak olduğu için, kişisel verilerin işlenmesi başlı başına bu hakka müdahale teşkil etmektedir. Söz konusu kişisel verilerin bir bireyin özel hayatı ile ilgili olup olmaması, hassas olması veya veri sahiplerini herhangi bir şekilde rahatsız edip etmemesi bundan bağımsızdır. Meşru olması için, müdahalenin Bildirge'nin 52 (1). Maddesinde belirtilen koşulları sağlaması gerekmektedir.

Kanunda belirtilmiş olma

Kişisel verilerin korunması hakkına ilişkin sınırlamaların kanunen öngörülmesi gerekmektedir. Bu gereklilik, sınırlamaların, bireylerin yükümlülüklerini anlamalarını ve davranışlarını düzenlemelerini sağlamak için yeterince erişilebilir ve öngörülebilir ve yeterli hassasiyetle formüle edilmiş yasal bir temele dayanma gerekliliğini belirtmektedir. Hukuki dayanak, bireyleri keyfi müdahaleye karşı korumak için yetkili makamlarca yetkilerin kullanılmasının kapsamını ve şeklini açıkça tanımlamalıdır. Bu yorum, AİHM içtihatları[59] uyarınca "hukuka aykırı müdahale" koşullarını andırmakta ve Bildirge'de kullanılan "kanunda belirtilmiş olma" ifadesinin anlamının, AİHS hükmüyle bağlantılı olması gerektiği iddia edilmektedir[60]. AİHM içtihat hukuku ve özellikle yıllar boyunca geliştirdiği "kanunun niteliği" kavramı, Bildirge'nin 52 (1). Maddesinin kapsamını yorumlarken ABAD tarafından göz önünde bulundurulması gereken bir husustur[61].

Hakkın özüne saygı duyma

AB hukuk düzeninde, bu Bildirge kapsamında korunan temel haklar üzerindeki herhangi bir sınırlama, bu hakların özüne saygı göstermelidir. Bu, temel haklardan yoksun bırakılacak kadar geniş ve müdahaleci olan sınırlamaların haklı çıkamayacağı anlamına gelmektedir. Hakkın özüne uyulması durumunda, genel çıkar hedefine hizmet edip etmediğini ve gereklilik ve orantılılık kriterlerini yerine getirip getirmediğini daha fazla değerlendirmek zorunda kalmadan, sınırlama yasadışı olarak kabul edilecektir.

[58] Kişisel verilerin korunmasına ilişkin temel hakkı sınırlayan önlemlerin gerekliliğinin değerlendirilmesinde: EDPS (2017), *Necessity Toolkit*, Brüksel, 11 Nisan 2017.
[59] EDPS (2017), *Necessity Toolkit*, Brüksel, 11 Nisan 2017, p.4; ayrıca bakınız ABAD, Mahkemenin 1/15 sayılı Görüşü (Yüce Divan), 26 Temmuz 2017.
[60] ABAD, Birleştirilmiş davalar C-203/15 ve C-698/15, *Tele2 Sverige AB v. Post- och telestyrelsen* ve *Secretary of State for the Home Department v. Tom Watson, Peter Brice, Geoffrey Lewis, Opinion of Advocate General Saugmandsgaard Øe*, 19 Temmuz 2016, para. 140.
[61] ABAD, C-70/10, *Scarlet Extended SA v. Société belge des auteurs compositeurs et éditeurs (SABAM), Opinion of Advocate General Cruz Villalón*, 14 Nisan 2011, para. 100.

Örnek: *Schrems*[62] davası, bireylerin kişisel verilerinin üçüncü ülkelere aktarılması karşısında korunması ile ilgilidir -bu durumda söz konusu üçüncü ülke Birleşik Devletler olacaktır. Birkaç yıl boyunca Facebook kullanıcısı olan bir Avusturya vatandaşı Schrems, kişisel verilerinin Facebook'un İrlanda'daki yan kuruluşundan Facebook Inc.'e ve verilerin işlendiği ABD'deki sunuculara aktarılmasını ihbar etme amacıyla İrlanda veri koruma denetleme makamına şikayette bulunmuştur. Schrems, ABD gözetim servislerinin gözetim faaliyetleri ile ilgili Amerikalı bir casus olan Edward Snowden'in 2013 ifşaları ışığında, ABD yasalarına ve uygulamasına ABD topraklarına aktarılan kişisel verilere yeterli koruma sağlamadığını savunmuştur. Snowden, Ulusal Güvenlik Ajansının doğrudan Facebook gibi firmaların sunucularına girdiğini ve sohbetlerin ve özel mesajların içeriğini okuyabildiğini ortaya çıkarmıştı.

ABD'ye veri aktarımı, 2000'de kabul edilen ve AB'ye aktarılan kişisel verileri koruyacaklarını ve "Güvenli Liman İlkelerine" uyduklarını onaylayan ve ABD şirketlerine yapılan transferlere izin veren bir Komisyon yeterlilik kararına dayanmaktaydı. Dava, ABAD önüne çıkarıldığında, Komisyon kararının geçerliliği, Bildirge ışığında incelenmiştir. AB'deki temel hakların korunmasının, ABAD, bu hakların yalnızca tam olarak gerekli olduğu ölçüde uygulanabilmesi için istisnalar ve sınırlamalar gerektirdiğini hatırlatmıştır. ABAD, kamu makamlarının genel olarak, elektronik haberleşmenin içeriğine müdahale ettiği yasa için "Bildirge'nin 7. Maddesinde belirtilen şekilde, özel hayata saygı gösterilmesine ilişkin temel hakkın özünü tehlikeye atan" değerlendirmesi yapmıştır. ABD kamu otoritelerine ilgili ulusal güvenlik veya suç önleme konusundaki somut kaygılara dayanan herhangi bir nesnel gerekçe olmadan ve ilgili gözetim uygulamalarına uygun güvenlik önlemleri alınmadan iletişimlere rahat bir şekilde erişme yetkisi verildiyse, bu hak anlamsız olacaktır.

Ayrıca, ABAD, "bireyin kendisiyle ilgili kişisel verilere erişim sağlamak veya bu tür verilerin düzeltilmesini veya silinmesini sağlamak için yasal yollara başvurma imkanı sağlamayan yasanın" adil yargılanma temel hakkı ile uyumlu olmadığı gözlemlenmiştir (Bildirge Madde 47). Bu nedenle, Güvenli Liman Kararı, ABD'de temel hakların korunmasına ilişkin Bildirge'ye tabi AB içinde sağlanan seviyede seviyesinde etkin bir koruma sağlayamamıştır. Sonuç olarak ABAD bu kararı geçersiz kılmıştır[63].

Örnek: *Digital Rights İrlanda*[64]'da ABAd, 2006/24/EC sayılı Direktif'in (Veri Saklama Direktifi) Bildirge'nin 7. ve 8. Maddeleri ile uyumluluğunu incelemiştir. Direktif, elektronik iletişim servis sağlayıcılarını, trafik ve konum verilerini en az altı ay ve 24 aya kadar tutmak ve yetkili ulusal makamların bu suçlara suçu önleme, soruşturma, tespit etme ve kovuşturma amacıyla erişmesine izin vermekle yükümlü tutmuştur. Direktif, elektronik içeriğin saklanmasına izin vermemiştir. ABAD, sağlayıcıların bir iletişim kaynağını ve hedefini, bir iletişimin tarihini, saatini ve süresini, arayan numarayı, aranan numaraları ve IP adreslerini izlemek ve tanımlamak için gerekli olan yönetmeliğe uygun olarak saklamak zorunda

[62] ABAD, C-362/14, *Maximillian Schrems v. Data Protection Commissioner* [GC], 6 Ekim 2015

[63] ABAD'ın 520/2000/EC sayılı Komisyon kararını geçersiz kılma kararı ayrıca bu el kitabında sonraki bölümlerde açıklanacak olan diğer sebeplere dayanmaktadır. ABAD, kararın ulusal veri koruma denetleme kurumlarının yetkilerini kanuna aykırı şekilde kısıtladığına kanaat getirmiştir. Ayrıca, Güvenli Liman rejimi kapsamında, kendileri ile ilgili kişisel verilere erişmek ve/veya düzeltme veya slime işlemlerini elde etmek istemeleri durumunda, bireyler için yargı yolu öngörülmemiştir. Böylece, Bildirge'nin 47. Maddesinde yer alan adil yargılanma hakkının özü de tehlikeye atılmıştır.

[64] ABAD, birleştirilmiş davalar C-293/12 ve C-594/12, *Digital Rights Ireland Ltd v. Minister for Communications, Marine and Natural Resources and Others* ve *Kärntner Landesregierung and Others* [GC], 8 Nisan 2014.

olduklarına dikkat çekmiştir. Bu veriler "bir bütün olarak, verileri saklanan kişilerin günlük yaşamlarındaki alışkanlıkları, sürekli veya geçici ikamet yerleri, günlük veya diğer hareketler, yapılan faaliyetler, bu kişilerin sosyal ilişkileri ve uğrak sosyal çevreleri gibi özel hayatlarına ilişkin oldukça kesin sonuçlar ortaya çıkarmaktadır."

Bu nedenle, kişisel verilerin saklanması Direktif uyarınca gizlilik ve kişisel verilerin korunması hakkına ciddi bir müdahale teşkil etmektedir. Bununla birlikte, ABAD, müdahalenin bu hakların özünü olumsuz yönde etkilemediğine karar vermiştir. Gizlilik hakkı ile ilgili olarak, hakların özü, elektronik iletişim içeriğinin içeriği hakkında bilgi edinilmesine izin vermediğinden, özünde hakta taviz verilmemiştir. Benzer şekilde, Direktif elektronik telekomünikasyon hizmet sağlayıcılarının belirli veri koruma ve veri güvenliği ilkelerine uymalarını ve uygun teknik ve organizasyonel önlemler almalarını öngördüğünden kişisel verilerin korunması hakkının özünden ödün verilmemiştir.

Gereklilik ve orantılılık

Bildirge'nin 52 (1). Maddesi, orantılılık ilkesine bağlı olarak, Bildirge tarafından tanınan temel hak ve özgürlüklerin kullanımına ilişkin kısıtlamaların ancak gerekli olmaları halinde yapılabilmesini öngörmektedir.

İzlenen kamu yararı hedefine yönelik önlemlerin benimsenmesi durumunda bir sınırlama **gerekli** olabilmektedir -ancak ABAD tarafından yorumlandığı üzere, alınan önlem, aynı ama ulaşmak için alınacak diğer önlemlere kıyasla daha az müdahaleci olmalıdır. Özel hayata saygı gösterilmesi ve kişisel verilerin korunmasına ilişkin haklarla ilgili sınırlamalar için ABAD "istisnalar ve sınırlamaların yalnızca kesinlikle gerekli olduğu ölçüde uygulanması gerektiğini" içeren katı bir gereklilik testi uygulamaktadır. Bir sınırlamanın kesinlikle gerekli olarak kabul edildiği durumlarda bu sınırlamanın aynı zamanda orantılı olup olmadığı da değerlendirilmelidir.

Orantılılık, sınırlamadan kaynaklanan avantajların, söz konusu temel hakların kullanılmasında dezavantajlardan ağır basması gerektiği anlamına gelmektedir[65]. Gizlilik ve veri koruma haklarından yararlanmadaki dezavantajları ve riskleri azaltmak için, sınırlamaların uygun korumaları içermesi önem taşımaktadır.

Örnek: *Volker und Markus Schenke*[66]'de ABAD, belirli tarım fonlarından yararlanan her gerçek kişi için bu kişilerin hangi sürelerle bu yardımı aldığı, yardımın sıklığı veya miktarı gibi bir kriterlere dayanarak ayrım yapmadan bu kişilere ilişkin kişisel verilerin paylaşılması yükümlülüğünün öngörülmesi ile Konsey'in ve Komisyon'un orantılılık ilkesinin sınırlarını aştığına hükmetmiştir.

Böylece, ABAD, 1290/2005 sayılı Konsey Yönetmeliği (EC)'in bazı hükümlerinin ve 259/2008 sayılı Yönetmeliğin tamamının geçersizliğine karar vermiştir[67].

[65] EDPS (2017), *Necessity Toolkit*, p. 5.

[66] ABAD, birleştirilmiş davalar C-92/09 ve C-93/09, *Volker und Markus Schecke GbR and Hartmut Eifert v. Land Hessen* [GC], 9 Kasım 2010, parag. 89 ve 86.

[67] Ortak tarım finansmanı politikası hakkında 1290/2005 sayılı 21 Jaziran 295 tarihli Konsey Yönetmeliği (EC) , OJ 2005 L 209; 1290/200; Avrupa Tarımsal Garanti Fonu'ndan türeyen fonların yararlanıcılarına ilişkin bilgilerin yayınlanmasına ilişkin 1290/205 sayılı Konsey Yönetmeliği'nin uygulanmasına ilişkin ayrıntılı kurallar içeren 18 Mart 2008 tarih ve 259/2008/EC sayılı Komisyon Yönetmeiği, OJ 2008 L 76.

Örnek: Digital Rights Ireland[68]'da ABAD, Veri Saklama Yönetmeliği'nin neden olduğu gizlilik hakkına olan müdahale ile, elektronik iletişimin içeriğinin saklanmasının yasaklanması sebebiyle bu hakkın özünden taviz verilmediğini belirtmiştir. Ancak Direktifin, Bildirgenin 7. Ve 8. Maddeleriyle uyumlu olmadığı sonucuna varılmış ve bu nedenle geçersiz olduğu belirtilmiştir. Toplanan ve bir bütün olarak ele alınan trafik ve konum verileri, analiz edilebildiği ve bireylerin özel yaşamlarının ayrıntılı bir resmini gösterebildiği için, bu haklara ciddi bir müdahale teşkil etmektedir. ABAD, Direktifin sabit telefon, mobil telefon, internet erişimi, internet e-postası ve internet telefonu gibi insanların günlük yaşamlarında kullanımı çok yaygın olan tüm iletişim araçları ile ilgili tüm meta verilerinin tutulmasını öngördüğünü dikkate almıştır. Pratikte bu, tüm Avrupa popülasyonunu etkileyen bir müdahale teşkil etmektedir. Bu müdahalenin kapsamı ve ciddiyeti göz önüne alındığında, trafik ve konum verilerinin saklanması ABAD'a göre yalnızca ciddi suçlarla mücadele amacıyla haklı görülebilecektir. Ayrıca, direktif, yetkili ulusal makamların tutulan verilere erişiminin kesinlikle gerekli olanlarla sınırlı olmasını sağlayacak objektif kriterleri belirlememiştir. Ayrıca direktif, bir mahkeme veya başka bir bağımsız kuruluş tarafından önceki bir incelemeye bağlı olmayan ve tutulan verilere ulusal makamlar tarafından erişilmesini ve kullanılmasını düzenleyen önemli ve sürece ilişkin koşullar içermemiştir.

ABAD birleştirilmiş davalar *Tele2 Sverige AB v. Post- och telestryrelsen* and *Secretary of State for the Home Department v. Tom Watson and Others*[69]'da da benzer bir sonuca varmıştır. Bunlar, "tüm abonelerin ve kayıtlı kullanıcıların ve tüm elektronik iletişim araçlarının yanı sıra meta verinin" trafik ve konum verilerinin "izlenen amaca göre farklılaşma, sınırlama ya da istisna[70]" olmadan tutulmasına ilişkindir. Bu durumda, bir kişinin doğrudan ya da dolaylı olarak ciddi ceza suçlarıyla bağlantısı olup olmadığı ya da iletişiminin ulusal güvenlik ile ilgili olup olmadığı, verilerin tutulmasının bir şartı değildir. Elde tutulan veriler ile kamu güvenliği ya da zaman aralığı veya coğrafi alan kısıtlamaları tehdidi arasında gerekli bağlantının bulunmadığına bakılacak olursa, ABAD, ulusal mevzuatın suça karşı ciddi bir şekilde mücadele etmek için kesinlikle gerekli olanın sınırlarını aştığı sonucuna varmıştır[71].

Gereklilik için benzer bir yöntem Avrupa Veri Koruma Denetçisi tarafından *Necessity Toolkit*[72]'te ele alınmıştır. Bu ara., önerilen önlemlerin veri koruma konusundaki AB yasalarına uygunluğunun değerlendirilmesine yardımcı olmayı hedeflemektedir. Bu araç, kişisel verilerin işlenmesini içeren önlemlerin hazırlanmasından veya incelenmesinden sorumlu olan AB politika yapıcılarını ve yasa koyucuları daha iyi donatmak ve kişisel verilerin işlenmesini dahil etmek ve kişisel verilerin korunması hakkını sınırlamak ve Bildirge'de yer alan diğer hak ve özgürlükler için geliştirilmiştir.

Genel menfaatin hedefleri

Gerekçelendirilmesi için, Bildirgenin kabul ettiği hakların kullanılmasına ilişkin herhangi bir

[68] ABAD, birleştirilmiş davalar C-293/12 ve C-594/12, *Digital Rights Ireland Ltd v. Minister for Communications, Marine and Natural Resources and Others* and *Kärntner Landesregierung and Others* [GC], 8 Nisan 2014, para. 39.
[69] ABAD, birleştirilmiş davalar C-203/15 ve C-698/15, *Tele2 Sverige AB v. Post- och telestryrelsen* ve *Secretary of State for the Home Department v. Tom Watson and Others* [GC], 21 Aralık 2016, para. 105–106.
[70] *A.g.e.*, para. 105.

[71] *A.g.e.*, para. 107.
[72] EDPS (2017), *Necessity Toolkit*, Brussels, 11 Nisan 2017

sınırlamanın, Birlik tarafından tanınan genel menfaat amaçlarını veya diğer kişilerin hak ve özgürlüklerini koruma ihtiyacını gerçekten karşılaması gerekmektedir. Başkalarının hak ve özgürlüklerini koruma ihtiyacına ilişkin olarak, kişisel verilerin korunması hakkı genellikle diğer temel haklarla etkileşime girmektedir. Bölüm 1.3 bu tür etkileşimlerin ayrıntılı bir analizini sunmaktadır. Genel menfaat hedeflerine gelince, bunlar AB'nin Avrupa Birliği Antlaşmasının 3. Maddesinde (TEU) onaylanan, barışın teşviki ve halklarının refahı, sosyal adalet ve koruma ve kişilerin serbest dolaşımının sağlanacağı bir özgürlük, güvenlik ve adalet alanının oluşturulması ile birlikte savaş suçlarının önlenmesi için uygun önlemlerin alınması ve bu anlaşmanın belirli hükümleri ile korunan diğer hedefleri içermektedir[73]. Genel Veri Koruma Regülasyonu, bu konuda Bildirge'nin 52 (1). Maddesini ayrıca belirlemektedir: Regülasyonun 23(2). Maddesi, sınırlamanın kişisel verilerin korunması hakkının özüne uyulması ve gerekli ve orantılı olması şartıyla, bireylerin haklarını sınırlamak için meşru olduğu düşünülen bir dizi genel menfaat hedefini listelemektedir. Ulusal güvenlik ve savunma, suçların önlenmesi, AB veya Üye Devletlerin önemli ekonomik ve mali çıkarlarının korunması, kamu sağlığı ve sosyal güvenlik, burada belirtilen genel menfaat hedefleri arasındır.

Sınırlamanın gerekliliği bu arka plana göre değerlendirileceği için, sınırlama tarafından takip edilen genel çıkar hedefini yeterince ayrıntılı olarak tanımlamak ve açıklamak önem taşımaktadır. Sınırlamanın amacının ve önerilen önlemlerin açık ve ayrıntılı bir açıklaması, gerekli olup olmadığına dair değerlendirmeye izin vermek için esastır[74]. İzlenen amaç ve sınırlamanın gerekliliği ve orantılılığı yakından bağlantılıdır.

Örnek: *Schwarz v. Stadt Bochum*[75], Üye Devlet yetkilileri pasaport çıkarırken parmak izi alma ve saklamadan kaynaklanan özel hayata saygı gösterilmesi ve kişisel verilerin korunması hakkıyla ilgili sınırlamalarla ilgilidir[76]. Başvuran, pasaport için Stadt Bochum'a başvurmuş ancak başvuru için parmak izi vermeyi reddetmiştir; bunu takiben Stadt Bochum da başvuranın pasaport başvurusunu reddetmiştir. Daha sonra, parmak izi alınmadan pasaportu çıkartabilmek için bir Alman mahkemesi önünde dava açmıştır. Alman mahkemesi 2252/2004 sayılı Yönetmeliğin 1(2). Maddesinin pasaportlarda ve üye devletler tarafından düzenlenen seyahat belgelerinde güvenlik özellikleri ve biyometrik standartlarıyla ilgili olup olmadığını sorgulayarak konuyu ABAD'a havale etmiştir.

ABAD, parmak izlerinin kişilerle ilgili özgün bilgiler taşıması ve kişilerin tanımlanmasını sağlaması sebebiyle kişisel veri olduğunu belirtmektedir, çünkü nesnel olarak parmak izlerini oluşturulması ve saklanması verilerin işlenmesini teşkil etmektedir. 2252/2004 sayılı Yönetmeliğin 1(2). Maddesi ile yöneltilen sonraki işleme, özel hayata ve kişisel verilerin korunması haklarına yönelik bir tehdit oluşturmaktadır[77]. Bununla birlikte, Bildirge'nin 52 (1). Maddesi bu hakların kullanımına ilişkin sınırlamalara izin vermektedir, bu sınırlamalar yasalarca sağlandığı sürece, bu hakların özüne saygı göstermektedir ve orantılılık ilkesine uygun olarak Birlik tarafından tanınan genel menfaat hedeflerini veya başkalarının hak ve özgürlüklerini koruma ihtiyacını gerçekten karşılamaktadır.

Mevcut davada ABAD, ilk önce pasaport verirken parmak izlerinin alınması ve saklanmasından kaynaklanan sınırlamanın, 2252/2004 sayılı Yönetmeliğin 1(2). Maddesinde öngörüldüğü için, yasalarca öngörülmüş olması gerektiğini belirtmiştir. İkinci olarak, son

[73] Temel Haklar Bildirgesi (2007/C303/02)'ne ilişkin açıklamalar, OJ 2007 No. C303, syf. 17-35
[74] EDPS (2017), *Necessity Toolkit*, Brüksel, 11 Nisan 2017, syf. 4.
[75] ABAD, C-291/12, *Michael Schwarz v. Stadt Bochum*, 17 Ekim 2013.
[76] *A.g.e.*, paras. 33–36.
[77] *A.g.e.*, parag. 27–30.

düzenleme pasaportların sahteciliği ve hileli kullanımlarını önlemek için tasarlanmıştır. Bu nedenle, Madde 1(2), diğerleri arasında AB'ye yasadışı giriş yapılmasını önlemek için yürürlüktedir ve bu nedenle Birlik tarafından tanınan bir genel menfaat hedefini takip etmektedir. Üçüncü olarak, ABAD'a sunulan kanıtlardan açıkça görülmemiştir ve bu davada hakların kullanımına uygulanan sınırlamaların bu hakların özüne saygı göstermediği iddia edilmemiştir. Dördüncü olarak, parmak izlerinin bu hüküm tarafından sağlanan yüksek güvenlikli bir depolama ortamında saklanması, karmaşık bir teknoloji gerektirmektedir. Bu tür bir depolamanın pasaportların tahrif edilme riskini azaltması ve AB sınırlarında pasaportların doğruluğunu kontrol etmekten sorumlu makamların çalışmalarını kolaylaştırması muhtemeldir. Yöntemin tamamen güvenilir olmadığı gerçeği şüphesiz değildir. Her ne kadar yöntem yetkisiz kişilerin kabul edilmesini engellemese de, böyle bir kabul olasılığını önemli ölçüde azaltması yeterlidir. Yukarıda belirtilenler ışığında, ABAD 2252/2004 sayılı Yönetmeliğin 1(2). Maddesinde belirtilen parmak izlerinin alınması ve saklanmasının, söz konusu düzenleme ile öngörülen amaçlara ulaşmak için ve AB'ye hukuka aykırı girişin engellenmesi hedefi için uygun olduğuna karar vermiştir[78].

ABAD daha sonra, söz konusu işlemlin **gerekli** olup olmadığını değerlendirmiştir; söz konusu eylemin genellikle başkaları tarafından görülebilen iki parmağın izinin alınmasından daha fazlasını içermediğine dikkat çekerek, bunun doğası gereği mahrem bir işlem olmaması gerektiğini belirtmiştir. Ayrıca etkilenen kişiye, yüzünün görüntüsünün çekilmesinden daha fazla fiziksel veya zihinsel bir rahatsızlık vermemektedir. Ayrıca, ABAD'ın önündeki işlemler sırasında ileri sürüklen, parmak izinin alınmasının tek gerçek alternatifinin iris (göz) taraması olduğu belirtilmelidir. ABAD'a sunulan dava dosyasındaki hiçbir şey, bu prosedürün, Bildiri'nin 7. Ve 8. Maddelerinde tanınan haklara parmak izi almaktan daha az müdahale edebileceğini önermemiştir. Ayrıca, bu iki yöntemin etkinliği ile ilgili olarak, iris tanıma teknolojisinin henüz parmak izi tanıma teknolojisi kadar gelişmiş olmadığı, şu anda parmak izlerini karşılaştırma prosedüründen önemli ölçüde daha pahalı olduğu ve bu nedenle genel kullanım için daha az uygun olduğu kabul edilmektedir. Buna göre, ABAD, pasaportların hileli kullanımına karşı korunma amacına ulaşılmasında ve Bildirge'nin7. Ve 8. Maddelerinde tanınan haklara yönelik bir tehdit için parmak izi yönteminden daha azının sağlanmasında etkili olacak önlemlerden haberdar olmamıştır[79].

ABAD, 2252/2004 sayılı Yönetmeliğin 4 (3). Maddesinin açıkça, parmak izlerinin ancak bir pasaportun veya sahibinin kimlik doğrulaması için kullanılabileceğini, Yönetmeliğin 1 (2). Maddesinin parmak izlerinin yalnızca sahibine ait olan pasaport haricinde depolanmasına izin vermediğini belirtmiştir. Bu nedenle, düzenleme burada toplanan verilerin merkezi olarak depolanması için veya bu tür verilerin AB'ye yasadışı girişi engellemekten başka amaçlarla kullanılması için yasal bir temel oluşturmamıştır[80]. Yukarıdaki tüm düşünceler ışığında ABAD, söz konusu incelemesinin 2252/2004 sayılı Yönetmeliğin 1 (2). Maddesinin geçerliliğini etkileyebilecek hiçbir etkisi olmadığı sonucuna varmıştır.

Bildirge ve AİHS arasındaki ilişki

Farklı ifadeler içermesine rağmen, Bildirgenin 52 (1). Maddesindeki haklara ilişkin yasal sınırlama koşulları, özel hayata saygı gösterilmesi hakkına ilişkin AİHS'in 8 (2). Maddesini hatırlatmaktadır. İçtihat hukukunda, ABAD ve AİHM, genellikle iki mahkeme arasındaki veri

[78] *A.g.e.*, paras. 35–45.
[79] ABAD, C-291/12, *Michael Schwarz v. Stadt Bochum*, 17 Ekim 2013, parag. 46–53.

[80] *A.g.e.*, parag. 56–61.

koruma kurallarına ilişkin uyumlu bir yorum yapmak amacıyla sürekli birbirlerinin kararlarına atıfta bulunmaktadır. Bildirge'nin 52 (3). Maddesi, "Bildirge'nin, İnsan Hakları ve Temel Özgürlüklerin Korunması Sözleşmesi'nin güvence altına aldığı haklara tekabül eden hakları, bu hakların anlamı ve kapsamı ile aynı olacaktır" şeklinde belirtmiştir. Bununla birlikte, Bildirge'nin 8. Maddesi AİHS'de tam karşılığı bulunmamaktadır[81]. Bildirge'nin 52 (3). Maddesi, sınırlandırma koşullarından ziyade, her bir yasal düzen tarafından korunan hakların içeriği ve kapsamıyla ilgilidir. Bununla birlikte, iki mahkemenin arasındaki diyalog ve iş birliğinin daha geniş bağlamı göz önünde alındığında, ABAD, AİHM'in yorumladığı gibi, AİHS'in 8. Maddesi uyarınca belirtilen yasal sınırlama kriterlerini dikkate alabilir. AİHM'in bu Bildirge uyarınca yasal sınırlama koşullarına atıfta bulunabileceği karşı senaryo da mümkündür. Her durumda, AİHS'in 8. Maddesinin, kişisel verilerin korunmasına ve özellikle de veri sahibinin haklarına, işlem için meşru gereklere ilişkin mükemmel bir eşdeğeri olmadığı göz önünde bulundurulmalıdır. Her durumda, Bildirge'nin 8. Maddesinin AİHS'te kişisel verilerin korunması, veri sahiplerinin hakları, veri işleme için meşru gerekçeler ve bağımsız bir otorite tarafından denetim hükümlerine ilişkin tam bir karşılığı bulunmamaktadır. Bildirge'nin 8. Maddesinin bazı bileşenleri AİHS'in 8. Maddesi uyarınca geliştirilen ve Sözleşme 108'le ilgili olan AİHM içtihat hukukunda bulunabilmektedir[82]. Bu bağlantı, veri koruma ile ilgili konularda ABAD ile AİHM arasında karşılıklı ilhan almayı sağlamaktadır.

1.3 . Diğer haklar ve diğer hukuki menfaatlerle etkileşimler

Kilit noktalar

- Veri koruma hakkı çoğu zaman ifade özgürlüğü ve bilgi alma ve verme hakkı gibi diğer haklarla etkileşime girmektedir.
- Bu etkileşim genellikle değişkendir: kişisel veri koruma hakkının belirli bir hakla gergin olduğu durumlar olmasına rağmen, kişisel veri koruma hakkının aynı özel haklara saygı duyulmasını sağladığı durumlar da vardır. Örneğin, profesyonel gizliliğin özel hayata saygı hakkının bir bileşeni olduğu göz önüne alındığında, ifade özgürlüğü söz konusudur.
- Başkalarının hak ve özgürlüklerini koruma ihtiyacı, kişisel veri koruma hakkının yasal olarak sınırlandırılmasının değerlendirilmesine kullanılan kriterlerden biridir.
- Farklı haklar söz konusu olduğunda, mahkemeler bunları uyumlaştırmak için farklı denge mekanizmaları oluşturmalıdır.
- Genel Veri Koruma Regülasyonu, Üye Devletlerin kişisel veri koruma hakkını ifade ve bilgi özgürlüğü ile bağdaştırmasını öngörmektir.
- Üye Devletler ayrıca, kişisel veri koruma hakkını resmi belgelere ve mesleki gizlilik yükümlülüklerine kamu erişimi ile uzlaştırmak için ulusal hukukta özel kurallar da kullanabilmektedir.

Kişisel veri koruma hakkı mutlak bir hak değildir; bu hakkın yasal olarak sınırlandırılmasına ilişkin koşullar yukarıda detaylı olarak verilmiştir. Hem Avrupa Konseyi hem de AB hukuku kapsamında tanınan haklarla ilgili yasal kısıtlama kriterlerinden biri, başkalarının hak ve özgürlüklerinin korunması için veri korumayla müdahalenin gerekli olduğudur. Veri korumanın diğer haklarla etkileşime girdiği hallerde, AİHM ve ABAD, AİHS'in 8. Maddesini ve Regülasyonun 8. Maddesini uygularken ve yorumlarken, diğer haklarla dengeleme

[81] EDPS (2017), *Necessity Toolkit*, Brussels, 11 Nisan 2017, syf. 6.
[82] Avrupa İnsan Hakları Bildirgesine ilişkin açıklamalar (2007/C 303/02), md. 8.

uygulamasının gerekli olduğunu belirtmiştir[83]. Birkaç önemli örnek bu dengeye nasıl ulaşıldığını gösterecektir.

Bu mahkemelerin yürüttüğü dengeleme uygulamasına ek olarak, devletler gerektiğinde kişisel bilgilerin korunma hakkını diğer haklarla uzlaştırmak için mevzuat kabul edebilecektir. Bu nedenle, Genel Veri Koruma Regülasyonu bir dizi ulusal ihlal alanı sunmaktadır.

İfade özgürlüğü ile ilgili olarak, GDPR Üye Devletlerin yasalara göre, "Bu Yönetmeliğe uygun olarak kişisel verileri korunması hakkını, gazetecilik amaçlı işlemler ve amaçlı dahil olmak üzere, ifade ve bilgi alma hakkı ile uzlaştırmasını şart koşar akademik, sanatsal veya edebi ifadeyi ifade etmektedir[84]." Üye Devletler ayrıca, veri korumasını, resmi belgelere kamu erişimiyle ve özel hayata saygı gösterilmesi hakkı olarak korunan mesleki gizlilik yükümlülüklerini uzlaştırmak için yasalar kabul edebilir[85].

1.3.1 İfade Özgürlüğü

Veri koruma hakkıyla en fazla etkileşime giren haklardan biri ifade özgürlüğü hakkıdır. İfade özgürlüğü, Bildirge'nin 11. Maddesi ile korunmaktadır ('İfade ve bilgi özgürlüğü'). Bu hak, "kamu makamı tarafından ve sınırlar gözetilmeksizin, kamuoyunun müdahalesine maruz kalmadan fikir sahibi olma ve bilgi ve fikir alma ve verme özgürlüğünü" içermektedir. Bilgi özgürlüğü, hem Bildirge'nin 11. Maddesi hem de AİHS'in 10. Maddesine göre, yalnızca bilgi verme değil aynı zamanda bilgi *alma* hakkını da korumaktadır.

İfade özgürlüğü konusundaki sınırlamalar, yukarıda belirtilen Bildirge'nin 52 (1). Maddesinde belirtilen kriterlere uymalıdır. Ek olarak, 11. Madde AİHS'in 10. Maddesine karşılık gelmektedir. Bildirge'nin 52 (3). Maddesi uyarınca, AİHS tarafından güvence altına alınan haklara karşılık gelen hakları içerdiği sürece, "bu hakların anlamı ve kapsamı, söz konusu Sözleşme tarafından belirtilenlerle aynı olacaktır." Bildirge'nin 11. Maddesi ile güvence altına alınan haklara yasal olarak uygulanabilecek sınırlamalar, bu nedenle AİHS'in 10 (2). Maddesinde öngörülen sınırlamaları aşmamalıdır -bu, sınırlamaların kanunlarda öngörülmesi, demokratik toplum içinde "diğer kişilerin itibarı veya haklarının korunması" için gerekli olması anlamına gelmektedir. Bu haklar, özellikle özel hayata saygı gösterilmesi ve kişisel verilerin korunması hakkını kapsamaktadır.

Kişisel verilerin korunması ile ifade özgürlüğü arasındaki ilişki, "Veri işleme ve bilgi ve ifade özgürlüğü" başlıklı Genel Veri Koruma Regülasyonu'nun 85. Maddesi ile düzenlenmektedir. Bu maddeye göre, Üye Devletler, kişisel verilerin korunması hakkını, ifade ve bilgi özgürlüğü hakkı ile uzlaştırmaktadır. Özellikle, Genel Veri Koruma Yönetmeliği'nin belirli bölümlerinden muafiyetler ve istisnalar, gazetecilik amacıyla veya akademik, sanatsal veya edebi ifade amacıyla, ifade ve bilgi özgürlüğü ile kişisel verilerin korunması hakkını uzlaştırmak için gerekli olduğu sürece yapılmaktadır.

---

[83] AİHM, *Von Hannover v. Germany (No. 2)* [GC], Nos. 40660/08 and 60641/08, 7 Şubat 2012; AİHM, Birleştirilmiş davalar C-468/10 and C-469/10, *Asociación Nacional de Establecimientos Financieros de Crédito (ASNEF) and Federación de Comercio Electrónico y Marketing Directo (FECEMD) v. Administración del Estado*, 24 Kasım 2011, parag. 48; ABAD, C-275/06, *Productores de Música de España (Promusicae) v. Telefónica de España SAU* [GC], 29 Ocak 2008, parag. 68.

[84] Genel Veri Koruma Regülasyonu, Md. 85.

[85] *A.g.e.*, Madde 86 ve 90.

Örnek: *Tietosuojavaltuutettu v. Satakunnan Markkinapörssi Oy and Satamedia Oy*[86]'da ABAd'dan veri koruma ile basin özgürlüğü arasındaki ilişkiyi tanımlaması istenmiştir[87]. ABAD'ın, bir şirketin SMS dağıtımını kullanarak Finlandiya vergi makamlarından yasal olarak elde edilen 1,2 milyon gerçek kişiye ait vergileri elde etmesini incelemesi gerekmekteydi. Fin veri koruma denetleme otoritesi, şirketin bu verilerin yayılmasını durdurmasını gerektiren bir karar vermiştir. Şirket bu karara, ulusal mahkemede, Veri Koruma Direktifi'nin yorumlanması konusunda ABAD'dan açıklık talep eden bir itirazda bulunmuştur. Özellikle ABAD, cep telefonu kullanıcılarının diğer gerçek kişilerle ilgili gerçek kişilerle ilgili vergi verilerini almasına izin vermek için sağlanan vergi otoritelerinin kişisel verilerin işlenmesinin yalnızca gazetecilik amaçlı bir faaliyet olarak değerlendirilmesinin gerekip gerekmediğini doğrulamak zorundaydı. ABAD şirket faaliyetlerinin Veri Koruma Direktifi'nin 3 (1). Maddesi kapsamında "kişisel verilerin işlenmesi" olduğu sonucuna vardıktan sonra, ABAD Direktifin 9. Maddesini (kişisel verilerin işlenmesi ve ifade özgürlüğü hakkında) analiz etmiştir. Öncelikle her demokratik toplumda ifade özgürlüğü hakkının önemine dikkat çekmiş ve gazetecilik gibi bu özgürlükle ilgili kavramların geniş yorumlanması gerektiğini belirtmiştir. Daha sonra, iki temel hak arasında bir denge sağlamak için, veri koruma hakkındaki istisnaların ve kısıtlamaların, yalnızca gerekli olduğu sürece uygulanması gerektiğini gözlemlemiştir. Bu gibi durumlarda, ABAD, kamuoyunda bulunan ve kamu mevzuatında yer alan belgelere ait verilerle ilgili olarak söz konusu şirketler tarafından yürütülen faaliyetler gibi faaliyetlerin, amaçlarının kamuya açıklanması halinde bilgi, fikir veya onları aktarmak için kullanılan araç ne olursa olsun bunların 'gazetecilik faaliyeti' olarak sınıflandırılabileceğini belirtmiştir. Ayrıca, bu faaliyetin medya kuruluşları ile sınırlı olmadığına ve kar amacı gütme amaçlı olabileceğine karar vermiştir. Bununla birlikte, ABAD bunun, bu davanın unsurları olup olmadığının belirlenmesini ulusal mahkemeye bırakmıştır.

Aynı dava, AİHM tarafından, ulusal mahkemenin karar vermesinden sonra, ABAD'dan alınan rehbere dayanarak, denetim otoritesinin tüm vergi bilgilerinin yayınlanmasını durdurma emrinin, şirketin ifade özgürlüğüne haklı bir müdahale olduğunu da incelemiştir. AİHM bu yaklaşımı onaylamıştır[88]. AİHM, şirketlerin bilgi verme hakkına müdahale olmasına rağmen, müdahalenin yasaya uygun olduğunu, meşru bir amaç edindiğini ve demokratik bir toplumda gerekli olduğunu tespit etmiştir.

Mahkeme, ifade özgürlüğü ile özel hayata saygı gösterilmesi hakkını dengelerken, ulusal makamlara ve AİHM'in kendisine yol göstermesi gereken içtihat kriterlerini hatırlatmıştır. Siyasi konuşmanın veya halkın ilgisini çeken bir tartışmanın söz konusu olduğu durumlarda, halkın bilgi edinme hakkı olduğu için bilgi alma ve verme hakkının kısıtlanması için çok az bir alan vardır, "ve bu demokratik bir toplumda temel bir haktır.[89]" Ancak, yalnızca belirli bir okuyucunun, bir kişinin özel hayatının ayrıntılarıyla ilgili merakını gidermeyi amaçlayan basın makaleleri, halkın ilgilisini çeken bir tartışmaya katkıda bulunmamaktadır. Gazetecilik amaçlı veri koruma kurallarından çıkan istisna, gazetecilerin gazetecilik faaliyetlerini yerine getirebilmeleri için verilere erişmesine, verilerin toplanmasına ve işlenmesine izin vermeyi

[86] ABAD, C-73/07, *Tietosuojavaltuutettu v. Satakunnan Markkinapörssi Oy and Satamedia Oy* [GC], 16 Aralık 2008, parag. 56, 61 ve 62.
[87] Dava, "Üye Devletler, yalnızca gazetecilik amaçlı veya sanatsal amaçlarla yapılan kişisel verilerin işlenmesi için yalnızca gizlilik hakkı ve ifade özgürlüğü kurallarını uzlaştırmak amacıyla bu Bölüm, Bölüm IV ve Bölüm VI'daki hükümlerden muafiyet ve istisna sağlayacaklardır" diyen Veri Koruma Direktifi Madde 9'un, -şimdi Genel Veri Koruma Regülasyonu'nun 85. Maddesiyle değiştirilmiştir- yorumlanmasına ilişkindir.
[88] AİHM, *Satakunnan Markkinapörssi Oy and Satamedia Oy v. Finland*, No. 931/13, 27 Haziran 2017.
[89] *A.g.e.*, parag. 169.

amaçlamaktadır. Bu nedenle, başvuran şirketlerin söz konusu yüksek miktara vergi verilerini toplamalarına ve işlemelerine izin verme ve bunlara erişim sağlama konusunda kamu yararı bulunmaktadır. Buna karşılık, Mahkeme, bu ham verilerin gazeteler tarafından toplu olarak dağıtılmasında, kamuoyunda herhangi bir değişiklik yapılmadan ve analitik bir girdi olmadan, kamu yararı olmadığını tespit etmiştir. Vergilendirme hakkındaki bilgiler, halkın meraklı üyelerinin, bireyleri ekonomik durumlarına göre kategorize etmelerini ve halkın başkalarının özel hayatlarıyla ilgili bilgi almak için susuzluklarını tatmin etmelerini sağlamış olabilir. Bu, kamu menfaatine yönelik bir tartışmaya katkı olarak kabul edilemez.

Örnek: *Google İspanya*[90]'da ABAD, Google'ın başvuranın mali zorluklarıyla ilgili eski bilgileri arama listesi sonuçlarından silmek zorunda olup olmadığını değerlendirmiştir. Başvuranın ismini kullanarak Google arama motorunda bir arama yapıldığında, aramanın sonuçları, iflas işlemleri ile bağlantısını açıklayan eski gazete makalelerine bağlantı sağlamaktadır. Başvuran bunun, özel hayata saygı gösterme ve kişisel verilerin korunmasına ilişkin haklarını ihlal etiğini, işlemlerin yıllar önce sonuçlandığı ve bu gibi referansları alakasız hale geldiğini iddia etmiştir.

ABAD ilk önce internet arama motorlarının ve kişisel veri sağlayan arama sonuçlarının bir bireyin detaylı bir profilini oluşturabildiğini açıklığa kavuşturmuştur. Giderek artan bir şekilde sayısallaştırılmış bir toplumun ışığında, kişisel verilerin doğru olması ve yayınlanması için gerekenin ötesine geçmemesi yani hala bilgi sağlama gereksinimi, bireylere yüksek düzeyde veri koruması sağlamak için esastır. "Bu veri işlemeye ilişkin sorumlu, sorumlulukları, yetki ve yeteneklerini çerçevesinde, işlemenin AB hukukunun şartlarını yerine getirmesini sağlamalıdır" ki mevcut yasal garantiler tam etkili olsun. Bu, işlem artık geçerli olmadığında veya eski olduğunda bir kişinin kişisel verilerinin silinme hakkının, yalnızca veri işleyenleri değil, veri sorumlusu olarak bulunan arama motorlarını da kapsadığı anlamına gelmektedir (2.3.1. bölüme bakınız).

Google'ın başvuru sahibi ile ilgili bağlantıları kaldırması gerekip gerekmediğini inceleyen ABAD, belirli koşullar altında bireylerin kişisel verilerini bir internet arama motorunun arama sonuçlarından silme hakkına sahip olduğunu belirtmiştir. Bu hak, bir bireye ilişkin bilgilerin veri işleme amaçları için yanlış, yetersiz, ilgisiz veya aşırı olduğu durumlarda kullanılabilmektedir. ABAD, bu hakkın mutlak olmadığını kabul etmiştir; diğer haklarla özellikle de kamuoyunun bilgiye erişimdeki menfaatleri ve hakları ile dengelenmesi gerekmektedir. Her bir silme talebinde, bir yandan kişisel verilerin korunmasına ilişkin temel haklarla bir yandan veri sahiplerinin özel hayatı ile diğer taraftan tüm internet kullanıcılarının meşru çıkarları arasında bir denge aramak için durum bazında bir değerlendirme yapılması gerekmektedir. ABAD, dengeleme çalışması sırasında göz önünde bulundurulması gereken faktörler hakkında rehberlik sağlamıştır. Söz konusu bilgilerin niteliği, özellikle önemli bir faktördür. Bilgi, bireyin özel hayatına duyarlıysa ve bilgilerin mevcudiyeti için herhangi bir kamu menfaati yoksa, veri koruma ve gizlilik kamunun bilgiye erişme hakkından üstün gelecektir. Ancak, veri sahibi kamuya mal olmuş bir kişi olması veya bilgilerin genel kamuya bu bilgilere erişim sağlamayı haklı gösterecek şekilde ortaya çıkması durumunda, verilerin korunması ve gizliliğe ilişkin temel haklara müdahale edilmesi üstün gelmektedir.

Kararı müteakip, Çalışma Grubu Madde 29, ABAD kararının uygulanmasına ilişkin yönergeleri kabul etmiştir. Yönergeler, denetleme makamları tarafından, kişilerin verilerinin

[90] ABAD, C-131/12, *Google Spain SL, Google Inc. v. Agencia Española de Protección de Datos (AEPD), Mario Costeja González* [GC], 13 Mayıs 2014, parag. 81–83.

silinmesi talepleriyle ilgili şikayetlerini ele alırken ve bu haklara ilişkin dengeleme mekanizmasını uygularken kullanılacak olan ortak kriterlerin bir listesini içermektedir[91].

AİHM, veri koruma hakkının ifade özgürlüğü hakkı ile uzlaştırılması ile ilgili olarak birçok önemli karar vermiştir.

Örnek: *Axel Springer AG v. Almanya*[92]'da AİHM, başvuran şirketin, tanınmış bir aktörün tutuklanması ve mahkum edilmesiyle ilgili AİHS'in 10. Maddesinin ihlal edildiği yönünde bir makale yayınlanmasını engelleyen bir tazminatı ele almıştır. AİHM, içtihat hukukunda belirtildiği gibi, ifade özgürlüğü hakkını özel hayata saygı gösterilmesi hakkına karşı dengelemek için göz önünde bulundurulması gereken kriterleri yinelemiştir:

- Yayınlanan makalenin kamu menfaatini ilgilendirip ilgilendirmediği;
- İlgili kişinin kamuya mal olmuş bir kişi olup olmadığı; ve
- Bilginin nasıl elde edildiği ve güvenilir olup olmadığı.

AİHM, aktörün tutuklanması ve mahkum edilmesinin kamusal bir adli gerçek olduğunu ve bu nedenle kamu yararına olduğunu; oyuncunun kamuya mal olmuş bir figür olarak nitelenebilecek kadar iyi tanınması; ve bilginin cumhuriyet savcılığı tarafından sağlandığı ve doğruluğunun taraflarca tartışılmadığını tespit etmiştir. Bu nedenle, şirkete uygulanan yayın kısıtlamaları, başvuranın özel hayatını korumak için meşru bir amaç ve makul derecede orantılı olmamıştır. Mahkeme AİHS'in 10. Maddesinin ihlal edilmediğine karar vermiştir.

Örnek: *Coudec and Hachette Filipacchi Associes v. France*[93]'de Monako Prensi Albert'in çocuğunun babası olduğunu iddia eden Bayan Coste ile yapılan röportajın haftalık Fransız dergisi tarafından yayınlanmasıyla ilgilidir. Röportaj ayrıca, Bayan Coste'nin prens ile olan ilişkisini ve çocuğunun doğumuna nasıl tepki verdiğini fotoğraflarla birlikte içermektedir. Prens Albert, özel hayatın korunması hakkını ihlal ettiği gerekçesiyle yayıncılık şirketine dava açmıştır. Fransız mahkemeleri, röportajın yayınlanmasının Prens Albert'e geri dönüşü olmayan bir zarara yol açtığını ve yayıncının tazminat ödemesini ve mahkeme kararının detaylarıyla birlikte derginin kapağında yayınlanmasına hükmetmiştir. Derginin yayıncıları, Fransız mahkemelerinin kararlarının haksız yere ifade özgürlüğü haklarına müdahale ettiğini iddia ederek AİHM önünde dava açmışlardır. AİHM, Prens Albert'in özel yaşama saygı gösterilmesi hakkı, yayıncının ifade hakkı ve kamuoyunun bilgi alma hakkı arasında denge kurmuştur. Bayan Coste'nin öyküsünü kamuoyu ile paylaşma hakkı ve çocuğun babası ile hukuki bağının kurulması yönündeki menfaati de önemli değerlendirme kriterleriydi.

AİHM, röportajın yayınlanmasının, Prens'in özel hayatına müdahale oluşturduğunu belirterek müdahalenin gerekli olup olmadığını incelemeye geçmiştir. Monako vatandaşlarının, kalıtımsal monarşinin geleceğinin "soyundan geleceklerle bağlantılı" olması sebebiyle prenslerinin bir çocuğunun varlığını bilmek konusunda menfaatleri olduğuna değinilmiştir[94]. Mahkeme ayrıca, makalenin Bayan Coste ve çocuğunun ifade özgürlüğü

[91] Çalışma Grubu Madde 29 (2014), *"Google Spain and Inc v. Agencia Española de Protección de Datos (AEPD) and Mario Costeja González" C-131/12'in uygulanmasına ilişkin ABAD yönergeleri*, WP 225, Brüksel, 26 Kasım 2014.
[92] ABAD, *Axel Springer AG v. Germany* [GC], No. 39954/08, 7 Şubat 2012, parag. 90 ve 91.
[93] AHİM, *Coudec and Hachette Filipacchi Associés v. France* [GC], No. 40454/07, 10 Kasım 2015.

[94] *Ibid*., parag. 104–116.

haklarını kullanmalarına izin verdiğini belirtmiştir. Yerel mahkemeler, özel hayata saygı gösterilmesi ve ifade özgürlüğü hakkının dengelenmesi için AİHM içtihat kanunu ile geliştirilen ilke ve kriterleri dikkate almamışlardır. Mahkeme, Fransa'nın AİHS'in ifade özgürlüğü konusundaki 10. Maddesini ihlal ettiği sonucuna varmıştır.

AİHM içtihat hukukunda, bu hakların dengelenmesi ile ilgili önemli kriterlerden biri, söz konusu ifadenin genel kamu menfaati tartışmasına katkıda bulunup bulunmadığıdır.

Örnek: *Mosley v. Birleşik Krallık*[95]'ta ulusal haftalık bir gazete, tanınmış bir kişinin mahrem fotoğraflarını yayınlamıştır, daha sonra başvuran başarılı bir şekilde yayıncı aleyhine dava açan ve tazminata hak kazanmıştır. Başvuran, maddi tazminatın ödenmesine rağmen söz konusu fotoğrafların yayınlanmasından önce bildirimde bulunulması yönünde herhangi bir yasal zorunluluk bulunmamasından dolayı, fotoğraflara ilişkin bir tedbir kararı aldırılamamış olmasından ötürü hala mağdur olduğunu iddia etmektedir.

AİHM, bu tür materyallerin yayımlanmasının genellikle eğitimden ziyade eğlence amaçlı olmasına rağmen bilginin gizli ve mahrem doğası gereği yayımlanmasında kamu menfaati olmamasına ilişkin AİHS'in 8. Maddesindeki gereklilikleri sağlamasından ötürü AİHS'in 10. Maddesi'nin korumasından hiç kuşkusuz faydalandığını belirtmiştir. Ancak, yayınlanmadan önce bir sansür olarak işleyebilecek kısıtlamalar da incelenmelidir. AİHM, ön bildirim gerekliliğinin ortaya çıkmasının yaratabileceği gerginliği ve etkililiği konusundaki şüpheleri ve bu konuda ortaya çıkabilecek geniş takdir yetkisini göz önünde bulundurarak AİHS'in 8. Maddesi uyarınca bağlayıcı bir ön bildirimin gerekli olmadığına karar vermiştir. Bu doğrultuda Mahkeme, Madde 8'in ihlal edilmediğine karar vermiştir.

Örnek: *Bohlen v. Almanya*[96] tanınmış bir şarkıcı ve sanat yapımcısı olan başvuran, otobiyografik bir kitap yayınlamış ve daha sonra mahkeme kararlarını takiben kitabın bazı bölümlerini kaldırmak zorunda kalmıştır. Hikaye, ulusal medyada geniş çapta ele alınmış ve bir tütün şirketi, başvuranın ilk adını rızası olmadan kullanarak bu olayla ilgili mizahi bir reklam kampanyası başlatmıştır. Başvuran, AİHS'in 8. Maddesi uyarınca haklarının ihlal edildiğini iddia ederek, reklam şirketinden başarısız bir tazminat talebinde bulunmuştur. AİHM, özel hayata saygı gösterilmesi hakkı ile ifade özgürlüğü arasındaki dengeyi gösteren kriterleri yinelemiş ve 8. Maddenin ihlal edilmediğine karar vermiştir. Başvuran, kamuya mal olmuş bir kişiydi ve reklam özel hayatının ayrıntılarına değinmemiş yalnızca medya tarafından kapsanan ve bir kamuoyu tartışmasının bir parçası olan halka açık bir olaya atıfta bulunmuştur. Ayrıca, reklam mizahi bir yapıya sahiptir ve başvuru sahibi ile ilgili aşağılayıcı veya olumsuz hiçbir şey içermemektedir.

Örnek: *Biriuk v. Litvanya*[97]'da başvuran, AİHM önünde, büyük bir gazete tarafından gizliliğinin ihlal edilmesi sonucunda yerel mahkemeler tarafından gülünç bir miktarda tazminata hükmedilmesi sebebiyle Litvanya'nın özel hayatın gizliliği hakkına saygı duyma konusundaki güvencesini yerine getirme yükümlülüğünü yerine getirmediğini ileri sürmüştür. Manevi tazminata hükmedilmesi sırasında, ulusal mahkemeler, bir kişinin özel hayatına ilişkin bilgilerin medyaya dağıtılması sebebiyle hükmedilecek manevi tazminat için

[95] AİHM, *Mosley v. the United Kingdom*, No. 48009/08, 10 Mayıs 2011, parag. 129 ve 130.
[96] AİHM, *Bohlen v. Germany*, No. 53495/09, 19 Şubat 2015, parag. 45–60.

[97] AİHM, *Biriuk v. Lithuania*, No. 23373/03, 25 Kasım 2008.

düşük bir tavan öngören kamunun bilgilendirilmesine ilişkin ulusal yasa hükümlerinden faydalanmışlardır. Dava, Litvanya'nın en büyük gazetesinin, başvuranın HIV pozitif olduğunu bildiren bir ön sayfa makalesi yayınlamasından kaynaklanmıştır. Makale ayrıca başvuranın davranışlarını eleştirmiş ve ahlaki standartlarını sorgulamıştır.

AİHM, kişisel verilerin korunmasının, yalnızca tıbbi verilerin değil, AİHS kapsamındaki özel hayata saygı gösterilmesi hakkı için temel öneme sahip olduğunu hatırlatmıştır. Sağlık verilerinin gizliliği özellikle önemlidir, çünkü tıbbi verilerin ifşa edilmesi (bu durumda başvuranın HIV durumu), bir kişinin özel ve aile yaşamını, istihdam durumunu ve topluma dahil edilmesini önemli ölçüde etkilemektedir. Mahkeme, gazetedeki rapora göre, hastanenin sağlık personelinin, başvuranın HIV durumu hakkında tıbbi gizlilik yükümlülüğünün ihlal edilmesi olduğunun altını çizmektedir. Dolayısıyla, başvuranın özel yaşam hakkına meşru bir müdahale söz konusu değildir.

Makale basın tarafından yayınlanmıştır ve ifade özgürlüğü de AİHS uyarınca temel haklardan biridir. Ancak Mahkeme, bir kamu menfaatinin varlığının başvuru sahibi hakkındaki bu tür bilgilerin yayınlanmasını haklı gösterip göstermediğini incelerken, yayının asıl amacının okur merakını sağlayarak gazetenin satışını artırmak olduğunu tespit etmiştir. Böyle bir amaç, genel kamu menfaati tartışmasına konu edilemez. Bu, "basın özgürlüğünün aşırı bir şekilde kötüye kullanılmasını" oluşturduğu için, ulusal mevzuat uyarınca verilen zararın telafi edilmesi üzerindeki kısıtlamalar ve düşük tazminat oranları, Litvanya'nın başvuranın haklarını koruma konusundaki pozitif yükümlülüğünü yerine getirmediği anlamına gelmektedir. AİHM, AİHS'in 8. Maddesinin ihlal edildiğine karar vermiştir.

İfade özgürlüğü ve kişisel verilerin korunması hakkı her zaman çatışma içerisinde değildir. Kişisel verilerin etkin bir şekilde korunmasının ifade özgürlüğünü garanti ettiği durumlar mevcuttur.

Örnek: *Tele2 Sverige*'de ABAD, 2006/4 sayılı Direktifin (Veri Saklama Direktifi), Bildirge'nin 7. Ve 8. Maddelerinde belirtilen temel haklara oluşturduğu müdahalenin "geniş kapsamlı olduğunu ve özellikle ciddi olarak dikkate alınmalıdır. Ayrıca, verilerin saklanması ve daha sonra abone veya kayıtlı kullanıcıyı bilgilendirmeden kullanılmasının, ilgili kişilerin kafasında, özel hayatlarının sürekli gözetim altında olduğu hissi yaratması muhtemeldir" demiştir. ABAD ayrıca, trafik ve konum verilerinin genel olarak tutulmasının, elektronik iletişimin kullanımı ve "sonuç olarak Bildirge'nin 11. Maddesinde güvence altına alınmış olan ifade özgürlüğünün kullanıcıları tarafından kullanılması" üzerinde etkili olabileceğini tespit etmiştir[98]. Bu anlamda, veri saklamanın genel bir şekilde gerçekleştirilmemesi için katı güvenceler talep ederek, veri koruma kuralları nihayetinde ifade özgürlüğünün kullanılmasına katkıda bulunmaktadır.

İfade özgürlüğünün bir parçasını da oluşturan bilgi alma hakkı ile ilgili olarak, demokratik bir toplumun işleyişinde devlet şeffaflığının önemi giderek artmaktadır. Şeffaflık, Bölüm 1.2'de açıklandığı üzere, gerektiğinde ve orantılı olarak veri koruma hakkına bir müdahaleyi haklı gösterebilecek bir genel menfaat hedefidir. Son yirmi yılda, sonuç olarak, kamu makamları tarafından tutulan belgelere erişim hakkı, her AB vatandaşının ve bir Üye Devlet'te ikamet eden herhangi bir gerçek veya tüzel bir kişinin önemli bir hakkı olarak kabul edilmiştir.

[98] ABAD, birleştirilmiş davalar C-203/15 ve C-698/15, *Tele2 Sverige AB v. Post- och telestyrelsen* and *Secretary of State for the Home Department v. Tom Watson and Others* [GC], 21 Aralık 2016, parag. 37 ve 101; ABAD, Birleştirilmiş davalar C-293/12 ve C-594/12, *Digital Rights Ireland Ltd v. Minister for Communications, Marine and Natural Resources and Others* and *Kärntner Landesregierung and Others* [GC], 8 Nisan 2014, parag. 28.

Avrupa Konseyi hukuku uyarınca, Resmi Belgelere Erişim Sözleşmesi'ne (Sözleşme 205) yazarlarına ilham veren Öneri ilkelerine atıfta bulunulabilir[99].

AB hukuku uyarınca, Avrupa Parlamentosu, Konsey ve Komisyon belgelerine halka erişim konusunda 1049/2002 sayılı Tüzük ile belgelere erişim hakkı güvence altına alınmıştır (Belgelere Erişim Yönetmeliği)[100]. Yönetmeliğin 42. Maddesi ve TFEU'nun 15 (3). Maddesi bu erişim hakkını "şekli ne olursa olsun Birliğin kurumlarının, organlarının, ofislerinin ve acentelerinin belgelerine" genişletilmiştir.

Bir belgeye erişim, başkalarının kişisel verilerini açığa çıkarırsa, bu hak veri koruma hakkıyla çakışabilmektedir. Genel Veri Koruma Regülasyonu'nun 86. Maddesi, kamu yetkilileri ve organları tarafından tutulan ve resmi belgelerdeki kişisel verilerin, resmi belgelere halkın erişim hakkını uzlaştırmak amacıyla Birlik[101] veya Üye Devlet yasalarına uygun olarak ilgili makam ya da kuruluş tarafından ifşa edilebileceğini açıkça belirtmektedir.

Bu nedenle, kamu makamları tarafından tutuşan belgelere veya bilgilere erişim talepler, verileri istenen belgelerde bulunan kişilerin veri koruma hakkıyla dengelenmeye ihtiyaç duyabilir.

Örnek: *Volker und Markus Schecke and Hartmut Eifert v. Land Hessen*[102] ABAD, AB tarım sübvansiyonlarının yararlanıcılarının adı ve kazandıkları miktarların orantılılığını değerlendirmiştir. Yayın şeffaflığı artırmayı ve kamu fonlarının idare tarafından uygun kullanımının kamu kontrolüne katkıda bulunmayı amaçlamıştır. Birkaç yararlanıcı bu yayının orantılılığına itiraz etmiştir.

Kişisel verilerin korunması hakkının mutlak olmadığında dikkat çeken ABAD, iki AB tarımsal yardım fonunun yararlanıcılarını ve alınan kesin miktarların bir internet sitesinde yayınlanmasının, özellikle kişisel verilerin korunması olmak üzere özel hayata müdahale oluşturduğuna karar vermiştir.

ABAD, Bildirge'nin 7. Ve 8. Maddelerinde, yapılan bu müdahalenin kanunen öngörüşmüş olduğunu ve AB tarafından tanınan genel menfaat hedefiyle uyumlu olduğuna -yani topluluk fonlarının kullanımının şeffaflığı arttırdığına- karar vermiştir. Bununla birlikte, ABAD, AB tarımsal yardımdan faydalanan gerçek kişilerin adlarının ve aldıkları yardım miktarlarının yayınlanmasının orantısız bir tedbir olduğuna ve Bildirge'nin 52 (1). Maddesi uyarınca meşru müdahale sayılmadığına karar vermiştir. ABAD, demokratik bir toplumda vergi mükelleflerinin kamu fonlarının kullanımı konusunda bilgilendirmelerinin önemini belirtmiştir. Bununla birlikte, "kişisel verilerin korunmasında şeffaflık hedefine otomatik bir öncelik verilemeyeceğinden", AB kurumları Birliğin şeffaflık konusundaki çıkarlarını yayınlama sonucunda zarar görecek kişilerin gizlilik ve veri koruma haklarının kullanılmasındaki sınırlama ile dengelemek zorunda kalmışlardır.

[99] Avrupa Konseyi, Bakanlar Komitesi (2002), Recommendation Rec (81) 19 and Recommendation Rec (2002) 2 to member states on access to official documents, 21 Şubat 2002; Avrupa Konseyi, Resmi Belgelere Erişim Sözleşmesi, CETS No. 205, 18 Haziran 2009. Sözleşme henüz yürürlüğe girmemiştir.
[100] Avrupa Parlamentosu ve Konseyi ve Komisyon belgelerine halkın erişimi hakkında Avrupa Parlamentosu ve Konseyinin 1049/2001 sayılı, 20 Mayıs 2001 tarihli Yönetmeliği OJ 2001 L 145.
[101] Bildirge'nin 42. maddesi, TFEU'nun 15 (3). Maddesi ve 1049/2009 sayılı Yönetmelik
[102] ABAD, Birleştirilmiş davalar C-92/09 ve C-93/09, *Volker und Markus Schecke GbR and Hartmut Eifert v. Land Hessen* [GC], 9 Kasım 2010, parag. 47–52, 58, 66–67, 75, 86 ve 92.

ABAD, AB kurumlarının bu dengeleme çalışmasını gerektiği gibi yapmadıklarını, zira bireylerin temel haklarını daha az olumsuz etkileyebilecek tedbirlerin öngörülmesinin mümkün olduğunu, bununla birlikte yayının takip ettiği şeffaflık hedefine etkili bir şekilde katkıda bulunduğunu değerlendirmiştir. Örneğin, tüm faydalanıcıları etkileyen, isimlerini ve her birinin aldığı kesin miktarları veren genel bir yayın yerine, bu kişilerin yardım aldığı süre, ve yardım alma sıklığı, yardımın miktarı ve niteliği gibi ilgili kriterlere dayanarak bir ayrım yapılabilecektir. Bu nedenle ABAD, Avrupa tarım fonlarından yararlananlarla ilgili bilgilerin yayınlanmasını düzenleyen AB mevzuatını kısmen geçersiz ilan etmiştir.

Örnek: *Rechnungshof v. Österreichischer Rundfunk ve Diğerleri*[103] davasında ABAD, Avusturya mevzuatının bir kısmının AB veri koruma hukuku ile uyumluluğunu gözden geçirmiştir. Mevzuat, bir kamu kurumundan, kamuya sunulan yıllık bir raporda çeşitli kamu kuruluşlarının çalışanlarının adlarını ve gelirlerini yayınlamak amacıyla, gelir hakkında veri toplamasını ve bunu iletmesini gerektirmiştir. Bazı kişiler, veri koruma dayanağıyla verilerini iletmeyi reddetmişlerdir.

ABAD, görüşünde, temel haklara - AB hukukunun genel prensipleri - ve o zamanlar Bildirge'nin bağlayıcı olmadığını hatırlatarak AİHS'nin 8. maddesine dayanmıştır. Mahkeme, kişinin mesleki gelirine ilişkin veri toplanmasının ve özellikle de bunun üçüncü kişilere iletiminin, özel hayata saygı hakkı kapsamında olduğuna ve bu hakkın ihlal edildiğine karar vermiştir. Müdahalenin; yasaya uygun olsaydı, meşru bir amaç izleseydi ve bu amaca ulaşmak için demokratik bir toplumda gerekli olsaydı haklı olabileceğini söylemiştir. ABAD, Avusturya mevzuatının, – ülkenin ekonomik refahı ile ilgili bir değerlendirmede olmak üzere – kamu çalışanlarının maaşlarını makul sınırlar içinde tutmak olarak meşru bir amaç izlediğini belirtmiştir. Ancak, Avusturya'nın kamu fonlarının en iyi şekilde kullanılmasını sağlamaktaki menfaati, ilgili kişilerin özel hayatlarına saygı gösterilmesi haklarına müdahalenin ciddiyetine karşı dengelenmek zorunda kalmıştır.

Kişilerin gelirine ilişkin verilerin yayınlanmasının gerekli ve mevzuatın ulaşmak istediği amaç ile orantılı olup olmadığına karar vermek ulusal mahkemeye bırakılırken; ABAD, ulusal mahkemeyi, böyle bir amaca ulaşmanın eşit etkililikteki daha az müdahaleci araçlarla mümkün olup olmadığını incelemeye çağırmıştır. Kişisel verilerin kamuya değil yalnızca gözlemci kamu kurumlarına iletilmesi, buna örnektir.

Daha sonraki davalarda, veri koruma ile belgelere erişim arasındaki dengenin, ayrıntılı ve durum özelinde bir analiz gerektirdiği ortaya çıkmıştır. Her iki hak da diğerini otomatik olarak geçersiz kılamaz. ABAD, kişisel verileri içeren belgelere erişim hakkını iki davada yorumlama fırsatı bulmuştur.

Örnek: *Avrupa Komisyonu v. Bavyera Lager*[104] davasında ABAD, AB kurumlarının belgelerine erişim bağlamında kişisel veri koruma kapsamını ve 1049/2001 sayılı Yönetmelik (Belgelere Erişim Yönetmeliği) ile 45/2001 sayılı Yönetmelik (AB Kurumları Veri Koruma Yönetmeliği) arasındaki ilişkiyi tanımlamıştır. 1992 yılında kurulan Bavarian Lager, esas olarak birahaneler ve barlar için şişelenmiş Alman birasını Birleşik Krallık'a ithal etmektedir. Ancak, İngiliz mevzuatı *fiilen* ulusal üreticilerin lehine olduğu için zorluklarla

[103] ABAD, C-465/00, C-138/01 ve C-139/09, *Rechnungshof/Österreichischer Rundfunk ve Diğerleri ve Christa Neukomm ve Jospeh Lauermann/Österreichischer Rundfunk*, 20 Mayıs 2003.
[104] ABAD, C-28/08 P, *Avrupa Komisyonu/The Bavarian Lager Co. Ltd.* [GC], 29 Haziran 2010.

karşılaşmaktadır. Bavarian Lager'ın şikayetine yanıt olarak, Avrupa Komisyonu, yükümlülüklerini yerine getirmediği için Birleşik Krallık aleyhinde dava açmış ve bu durum, tartışmalı hükümlerin AB mevzuatına uyacak şekilde değiştirilmesine yol açmıştır. Daha sonra Bavarian Lager, Komisyon'dan, diğer belgelerin yanı sıra, Komisyon temsilcilerinin, İngiliz yetkililerin ve *Confédération des Brasseurs du Marché Commun* (CBMC)'nin katıldığı toplantı tutanağının bir kopyasını istemiştir. Komisyon, toplantı ile ilgili bazı belgeleri ifşa etmeyi kabul etmiştir ancak tutanaklarda beliren beş ismi silmiştir – bunlar, kimliklerinin ifşa edilmesine açıkça itiraz eden iki kişi ve Komisyon'un bağlantıya geçemediği üç kişidir. Komisyon, 18 Mart 2004 tarihli kararıyla, AB Kurumları Veri Koruma Yönetmeliği'nde güvence altına alındığı şekliyle ve özellikle bu kişilerin özel hayatlarının korunmasını gerekçe göstererek, toplantının tam tutanağının alınmasını içeren Bavyera Lager'in yeni başvurusunu reddetmiştir.

Bu durumdan memnun olmayan Bavarian Lager, İlk Derece Mahkemesi'nde bir dava açmıştır. Bu mahkeme, Komisyon kararını, 8 Kasım 2007 tarihli kararıyla (dava T-194/04, *The Bavarian Lager Co. Ltd/Avrupa Toplulukları Komisyonu*), temsil ettikleri kuruluşlar adına bir toplantıya katılan kişiler listesindeki söz konusu kişilerin yalnızca isimlerinin yazılmasının, özel hayata zarar vermediğini ve bu kişilerin özel hayatlarını herhangi bir tehlikeye sokmadığını söyleyerek hükümsüz kılmıştır.

Komisyon'un temyiz başvurusu üzerine, ABAD, İlk Derece Mahkemesi'nin kararını hükümsüz kılmıştır. ABAD, Belgelere Erişim Yönetmeliği'nin "kişisel verilerinin bazı durumlarda kamuya açıklanabileceği bir kişiyi koruyacak özel ve güçlendirilmiş bir sistem" oluşturduğuna karar vermiştir. ABAD'a göre, Belgelere Erişim Yönetmeliği'ne dayanan bir talebin kişisel verileri içeren belgelere erişmeye çalışması halinde, AB Kurumları Veri Koruma Yönetmeliği hükümleri bütünüyle uygulama bulacaktır. ABAD, daha sonra, Komisyon'un Ekim 1996 toplantısının tam tutanağına erişim başvurusunu reddetmede haklı olduğu sonucuna varmıştır. Bu toplantıya katılan beş katılımcının rızası eksik olduğu için, Komisyon, söz konusu belgenin bu kişilerin isimlerinin boş bırakıldığı bir versiyonunu vererek, aleniyet görevine yeterince uymuştur.

Ayrıca, ABAD'a göre, "Bavarian Lager, bu kişisel verilerin aktarılması gerekliliğini göstermek için herhangi bir açık ve meşru gerekçe veya ikna edici bir argüman sunmadığından, Komisyon, ilgili tarafların çeşitli menfaatlerini birbiriyle tartamamıştır". Komisyon, AB Kurumları Veri Koruma Yönetmeliği gereğince "veri sahiplerinin meşru menfaatlerinin taraflı olabileceğini" varsaymak için herhangi bir neden olup olmadığını da doğrulayamamıştır.

Örnek: *Client Earth ve PAN Europe v. EFSA*[105] davasında ABAD, Avrupa Gıda ve Güvenlik Kurumu'nun (EFSA), başvuranların belgelere tam erişimini reddetmesi kararının, belgelerde atıf yapılan kişilerin gizlilik ve veri koruma haklarını korumak için gerekli olup olmadığını incelemiştir. Belgeler, EFSA çalışma grubu tarafından harici uzmanlarla iş birliği içinde hazırlanan ve bitki koruma ürünlerinin piyasaya sunulması hakkında hazırlanan bir taslak rehber rapor ile ilgilidir. EFSA başlangıçta başvuru sahiplerine taslak rehber raporun bazı çalışma sürümlerine erişimi reddeden kısmi erişim izni vermiştir. Daha sonra, harici uzmanların bireysel yorumlarını içeren taslak versiyona erişim sağlamıştır. Ancak, 45/2001 sayılı Yönetmelik'in kişisel verilerin AB kurumları ve organları tarafından işlenmesine ilişkin 4 (1) (b) maddesi uyarınca ve harici uzmanların gizliliğinin korunması gerektiğinden,

[105] ABAD, C-615/13P, *Client Earth, Pesticide Action Network Europe (PAN Europe)/European Food Safety Authority (EFSA), Avrupa Komisyonu*, 16 Temmuz 2015.

uzmanların adlarını anonimleştirmiştir. Birinci derecede, AB Genel Mahkemesi EFSA'nın kararını onamıştır.

Başvuru sahipleri tarafından yapılan temyiz başvurusunda ABAD, ilk derece kararını tersine çevirmiştir. Mahkeme, bu durumda kişisel verilerin aktarılmasının, harici uzmanların her birinin bilim insanı olarak görevlerini yerine getirmedeki tarafsızlığını tespit etmek ve EFSA'daki karar alma sürecinin şeffaf kalmasını sağlamak için gerekli olduğu sonucuna varmıştır. ABAD'a göre, EFSA, taslak rehber rapor hakkında belirli yorumlar yapan harici uzmanların adlarının açıklanmasının uzmanların meşru menfaatlerine nasıl zarar vereceğini belirtmemiştir. Açıklama yapılmasının muhtemelen gizliliği zedeleyeceğine ilişkin genel bir argüman, her bir olaya özgü kanıtlarla desteklenmiyorsa yeterli olmayacaktır.

Bu kararlara göre, belgelere erişim bağlamında veri koruma hakkına müdahale edilmesi için belirli ve haklı bir nedene ihtiyaç vardır. Belgelere erişim hakkı, veri koruma hakkını otomatik olarak geçersiz kılamaz.[106]

Bu yaklaşım, aşağıdaki kararın gösterdiği üzere, gizlilik ve belgelere erişim konusunda AİHM'ninkine benzerdir. *Magyar Helsinki* kararında, AİHM, 10. maddenin bireye bir kamu otoritesi tarafından tutulan bilgilere erişim hakkı vermediğini veya hükümeti bireye bu tür bilgileri vermeye mecbur kılmadığını belirtmiştir. Ancak, böyle bir hak veya yükümlülük; ilk olarak, bilgilerin açıklanmasının kesinleşmiş veya icra edilebilir bir mahkeme kararına dayandığı ve ikinci olarak, bilgiye erişimin, bireyin ifade özgürlüğü – özellikle de bilgi alma ve verme özgürlüğü – hakkını kullanması için önemli olduğu ve hakkın inkâr edilmesinin bu haklara müdahale teşkil edeceği durumlarda ortaya çıkabilir[107]. Bilgiye erişimin kısıtlanmasının, başvuru sahibinin ifade özgürlüğüne müdahale teşkil edip etmediği ve hangi ölçüde müdahale teşkil ettiği her bir durum özelinde ve aşağıdakiler de dahil olmak üzere kendine has koşulları ışığında değerlendirilmesi gerekir: (i) bilgi talebinin amacı; (ii) aranan bilgilerin niteliği; (iii) başvuru sahibinin rolü; ve (iv) bilginin hazır ve ulaşılabilir olup olmadığı.

Örnek: *Magyar Helsinki Bizottság v. Macaristan*[108] davasında, bir insan hakları STK'sı olan başvuru sahibi, polislerden, Macaristan'daki kamu avukatı sisteminin işleyişiyle ilgili bir çalışmayı tamamlamak için baro tarafından atanan savunma avukatının çalışmaları ile ilgili olarak bilgi talebinde bulunmuştur. Polis, bu bilgilerin açıklanmaması gereken kişisel veri ihtiva ettiğini ileri sürerek bilgi vermeyi reddetmiştir. AİHM, yukarıdaki kriterleri uygulayarak, 10. madde ile korunan bir hakka müdahalede bulunulduğu sonucuna varmıştır. Açıklamak gerekirse, başvuru sahibi, kamu yararının olduğu bir konuda bilgi edinme hakkını kullanmak istemiş, bu amaçla bilgiye ulaşmaya çalışmıştır ve bilgi, başvuru sahibinin ifade özgürlüğü hakkını kullanması için gereklidir. Kamu avukatlarının atanmasına ilişkin bilgiler bakımından kamu yararı vardır. Söz konusu anketin, başvuru sahibinin halka sunmayı taahhüt ettiği bilgileri içerdiği ve halkın bu anketi öğrenme hakkına sahip olduğu konularında şüphe etmek için hiçbir sebep yoktur. Dolayısıyla, Mahkeme, başvuru sahibinin araştırmasını tamamlaması için istenen bilgilere erişiminin gerekli olduğu konusunda tatmin olmuştur. Son olarak, bilgi hazır ve mevcuttur.

AİHM, bu durumda bilgiye erişimin engellenmesinin bilgi alma özgürlüğünün özünü

[106] Bununla birlikte, bkz. EDPS'deki ayrıntılı görüşmeler (2011), *Bavyera Lager kararından sonra kişisel verileri içeren belgelere kamu erişimi*, Brüksel, 24 Mart 2011.
[107] AİHM, *Magyar Helsinki Bizottság/Macaristan*[GC], No. 18030/11, 8 Kasım 2016, para. 148.
[108] *A.g.e.*, para. 181, 187–200.

zayıflattığı sonucuna varmıştır. Mahkeme bu sonuca varırken, özellikle, talep edilen bilginin amacını ve önemli bir kamusal tartışmaya katkısını, aranan bilginin niteliğini ve kamu yararı olup olmadığını ve davada başvuranın toplumda oynadığı rolü incelemiştir.

Mahkeme, gerekçesinde, STK tarafından yürütülen çalışmanın AİHS'de büyük önem taşıyan bir hak olan adil yargılanma hakkı ile ve adaletin işletilmesi ile ilgili olduğunu belirtmiştir. Talep edilen bilgiler kamuya ilişkin olmayan verileri içermediğinden, başvuru sahibine polis tarafından bilgilere erişim izni verilmesinin, ilgili veri sahiplerinin (baro tarafından atanan kamu avukatları) gizlilik haklarını tehlikeye atmayacağı söylenmiştir. Başvuru sahibinin talep ettiği bilgi, baro tarafından atanan avukatların cezai kovuşturmalarda sanıkları temsil etmek için atanma sayılarına ilişkin istatiksel nitelikte bir bilgidir.

Mahkeme, çalışmanın genel çıkarlar konusunda önemli bir tartışmaya katkıda bulunmayı amaçladığı düşünüldüğünde, STK'nın planladığı yayın hakkındaki herhangi bir kısıtlamanın en üst düzeyde incelemeye tabi tutulması gerektiğini belirtmiştir. Söz konusu bilgi kamu yararınadır, çünkü kamu yararı "önemli tartışmalara yol açabilecek, önemli bir sosyal meseleyi ilgilendiren ya da halkın hakkında bilgi sahibi olmakla ilgileneceği bir sorunu içeren konular"ı kapsamaktadır[109]. Bu nedenle, başvuru sahibinin çalışmasının konusu olan adalet ve adil yargılanmaya ilişkin bir tartışmayı kesinlikle kapsayacaktır. Söz konusu birbirinden farklı hakların dengelenmesi ve orantılılık ilkesinin uygulanması uyarınca AİHM, AİHS'nin 10. maddesi uyarınca başvuru sahibinin haklarının haksız yere ihlal edildiğine karar vermiştir.

1.3.2. Mesleki Sır

Ulusal kanunlara göre, bazı iletişimler mesleki sır yükümlülüğüne tabi olabilir. Mesleki sır, inanç ve güvene dayanan ve belirli meslek ve işlerin doğası gereğince yasal bir zorunluluk olarak karşılaşılan özel bir etik görev olarak anlaşılabilir. Bu işlevleri yerine getiren kişi ve kurumlar, görevlerini yerine getirirken aldıkları gizli bilgileri ifşa etmemekle yükümlüdür. Mesleki sır en çok tıp sektöründe ve avukat-müvekkil gizliliğinde uygulanır, ayrıca birçok yargı alanında finans sektörüne ilişkin mesleki sır yükümlülüğü de tanınır. Mesleki sır bir temel hak değildir, ancak özel hayatın gizliliği hakkının bir şekli olarak korunur. Örneğin, ABAD, belirli durumlarda "AİHS'in 8. maddesi ve Avrupa Birliği Temel Haklar Bildirgesi'nin 7. maddesinde yer alan özel ve aile hayatına saygı gösterme temel hakkını korumak için gizli olarak sınıflandırılan belirli bilgilerin açıklanmasının yasaklanması gerekebileceğine" karar vermiştir[110]. AİHM, mesleki sırra getirilen kısıtlamaların, vurgulanan örneklerde gösterildiği gibi, AİHS'nin 8. maddesinin ihlalini teşkil edip etmediğine karar vermeye çağrılmıştır.

Örnek: *Pruteanu v. Romanya*[111] davasında, başvuru sahibi, dolandırıcılık suçlamalarını takiben banka işlemleri yapmaktan men edilen bir ticari şirketin avukatı olarak görev yapmıştır. Davanın soruşturması sırasında, Romen mahkemeleri, kovuşturma makamlarına belirli bir süre boyunca bir şirket ortağının telefon görüşmelerini dinleme ve kaydetme yetkisi vermiştir. Kayıtlar ve dinlemeler, şirket ortağının avukatıyla olan iletişimini içermektedir.

Bay Pruteanu, bu durumun kendisinin özel hayatına ve haberleşmesine saygı duyulması

[109] *A.g.e.*, para. 156.
[110] ABAD, Dava T-462/12 R, *Pilkington Group Ltd/Avrupa Komisyonu*, Genel Mahkeme Başkanı'nın Kararı, 11 Mart 2013, para. 44.
[111] AİHM, *Pruteanu/Romanya*, No. 30181/05, 3 Şubat 2015.

hakkına müdahale teşkil ettiğini iddia etmiştir. AİHM, kararında, bir avukatın müvekkili ile olan ilişkisinin durumunu ve önemini vurgulamıştır. Bir avukatın müvekkiliyle yaptığı görüşmelerin dinlenmesi, şüphesiz ki, bu iki kişi arasındaki ilişkinin temeli olan mesleki sır prensibini ihlal etmektedir. Böyle bir durumda avukat, özel hayatına ve haberleşmesine saygı gösterilmesi hakkına müdahale edilmesinden de şikâyet edebilir. ABAD, AİHS'nin 8. maddesinin ihlal edildiğine karar vermiştir.

Örnek: *Brito Ferrinho Bexiga Villa-Nova v.Portekiz*[112] davasında, başvuru sahibi olan avukat, mesleki sır ve bankacılık sırrı gerekçesiyle kişisel banka hesap özetlerini vergi makamlarına açıklamayı reddetmiştir. Savcılık, vergi dolandırıcılığı için soruşturma başlatmıştır ve mesleki sırrın askıya alınması için yetki verilmesini talep etmiştir. Ulusal mahkemeler, kamu yararının başvuru sahibinin bireysel menfaatlerinden üstün olduğu gerekçesiyle gizliliğin ve bankacılık sırrı kurallarının askıya alınmasına karar vermiştir.

Dava AİHM'nin önüne geldiğinde AİHM, başvuru sahibinin banka hesap özetlerine erişimin, özel hayat kapsamına giren mesleki sırra saygı duyma hakkına müdahale ettiği sonucuna varmıştır. Müdahalenin, ceza muhakemesi usulü kanununa dayanması sebebiyle, yasal bir dayanağı vardır ve müdahale meşru bir amaç izlemektedir. Bununla birlikte, müdahalenin gerekliliği ve orantılığını inceleyen AİHM, gizliliğin kaldırılması işlemlerinin başvuru sahibinin katılımı veya bilgisi olmadan gerçekleştiğini vurgulamıştır. Başvuru sahibi bu nedenle iddialarını sunamamıştır. Ayrıca, her ne kadar iç hukukta bu tür işlemler için baroya danışılması gerekse de somut olayda baroya danışılmamıştır. Son olarak, başvuru sahibinin, gizliliğin kaldırılmasına karşı etkili bir şekilde mücadele etme seçeneği ya da alınan tedbire itiraz etmek için herhangi bir imkanı yoktur. AİHM, gizlilik yükümlülüğünü askıya alan tedbir konusunda usule ilişkin teminatların verilmemesi ve etkin adli kontrolün bulunmaması nedeniyle, AİHS'nin 8. maddesinin ihlal edildiğine karar vermiştir.

Mesleki sır ve veri koruma arasındaki etkileşim çoğu zaman ikirciklidir. Bir yandan, mevzuatta yer alan veri koruma kuralları ve güvenceler, mesleki sırrın sağlanmasına yardımcı olmaktadır. Örneğin, veri sorumlularının ve veri işleyenlerin sağlam veri güvenliği önlemleri uygulamasını emreden kurallar, diğer şeylerin yanı sıra, mesleki sır uyarınca korunan kişisel verilerin gizliliğinin kaybını önlemeye çalışmaktadır. Ek olarak, AB Genel Veri Koruma Regülasyonu, daha güçlü koruma gerektiren özel nitelikli bir kişisel veri kategorisi olan sağlık verilerinin işlenmesini mümkün kılmaktadır, ancak veri sahiplerinin haklarının özellikle mesleki sır kapsamında korunması için bu imkanı uygun ve özel tedbirlerin varlığına tabi tutmaktadır[113].

Öte yandan, belirli kişisel veriler açısından veri sorumlularına ve veri işleyenlere uygulanan mesleki sır yükümlülükleri, veri sahiplerinin haklarını, özellikle de bilgi alma hakkını sınırlayabilir. Genel Veri Koruma Regülasyonu, prensip olarak, kişisel verilerinin kendisinden temin edilmediği hallerde veri sahiplerine verilmesi gereken bilgileri içeren kapsamlı bir liste içermesine rağmen, bu açıklama yükümü, ulusal ya da AB hukuku uyarınca mesleki sır yükümlülüğü nedeniyle kişisel verilerin gizli kalması gereken yerlerde geçerli değildir[114].

Genel Veri Koruma Regülasyonu (GDPR), Üye Devletler'in, kanunen, mesleki veya diğer eşdeğer sır yükümlülüklerini güvence altına almak ve kişisel verilerin gizliliği hakkını mesleki sır yükümlülüğü ile uyumlu hale getirmek için özel kurallar benimsemelerini sağlamaktadır[115].

---

[112] AİHM, *Brito Ferrinho Bexiga Villa-Nova/Portekiz*, No. 69436/10, 1 Aralık 2015.
[113] Avrupa Birliği Genel Veri Koruma Regülasyonu, Madde 9(2)(h) ve 9 (3).
[114] *A.g.e.*, Madde 14 (5) (d).
[115] *A.g.e.*, Başlangıç hükmü 164 ve Madde 90.

GDPR, Üye Devletler'in, denetim otoritelerinin yetkileri hakkında, mesleki sır yükümlülüğüne tabi olan veri sorumluları veya veri işleyenlerle ilgili özel kurallar benimsemelerini sağlamaktadır. Bu özel kurallar, bir veri sorumlusunun veya veri işleyenin tesislerine, onun veri işleme ekipmanına ve kişisel verilerin gizliliği yükümlülüğü kapsamındaki bir faaliyet sırasında elde edilen kişisel verilere erişim sağlama gücü ile ilgilidir. Bu nedenle, veri koruması ile görevlendirilen denetim otoriteleri, veri sorumlularını ve veri işleyenleri bağlayan mesleki sır yükümlülüklerine uymakla mükelleftir. Ayrıca, denetim otoritelerinin kendileri de görev süreleri sırasında ve sonrasında mesleki sır yükümlülüğü altındadır. Denetim otoritelerinin üyeleri ve personeli, görevlerini yerine getirdikleri sırada gizli bilgilere haiz olabilirler. Regülasyonun 54(2) maddesi bu kişilerin bu tür gizli bilgiler konusunda mesleki sır yükümlülüğü altında olduğunu açıkça göstermektedir.

GDPR uyarınca Üye Devletler'in, veri korumasının ve mevzuatlarında yer alan mesleki sır yükümlülüğü ile ilgili ilkelerin uyumlaştırılması için kabul ettikleri kuralları Komisyon'a bildirmeleri gerekmektedir.

1.3.3. Din ve İnanç Özgürlüğü

Din ve inanç özgürlüğü, AİHS'nin 9. maddesi (düşünce, vicdan ve din özgürlüğü) ve AB Temel Haklar Bildirgesi'nin 10. maddesi kapsamında korunmaktadır. Dini veya felsefi inançları ortaya çıkaran kişisel veriler hem AB hem de Avrupa Komisyonu hukukuna göre "özel nitelikli veri" olarak kabul edilmektedir ve bunların işlenmesi ve kullanılması daha fazla korumaya tabidir.

Örnek: *Sinan Işık v. Türkiye*[116] davasında başvuru sahibi, Tasavvuf ve diğer İslam öncesi inançlardan etkilenen, bazı alimler tarafından ayrı bir din olarak ve bazı alimler tarafından İslam dininin bir parçası olarak kabul edilen Alevi dini cemaatin bir üyesidir. Başvuru sahibi, kendi isteğine karşı olarak, kimlik kartının, dinini "Alevi" yerine "İslam" olarak gösteren bir kutu içerdiğinden şikayetçi olmuştur. Yerel mahkemeler, bu kelimenin ayrı bir dini değil, İslam dininin bir alt grubunu belirttiği gerekçesiyle kimlik kartının ilgili hanesinin "Alevi" olarak değiştirilmesi talebini reddetmiştir. Işık, daha sonra AİHM'e başvurmuş ve rızası olmadığı halde inancını açıklamakla yükümlü tutulduğunu çünkü kişinin kimlik kartında dininin belirtilmesinin zorunlu olduğunu, bu durumun – özellikle kimlik kartında dininin yanlış bir biçimde "İslam" olarak gösterilmesi sebebiyle – din ve vicdan özgürlüğü hakkını ihlal ettiğini söylemiştir.

AİHM, din özgürlüğünün, bir insanın dinini bir topluluk içinde başkalarıyla birlikte, kamuoyunda ve aynı inancı paylaşan insanların içinde, ancak aynı zamanda tek başına ve özel olarak ortaya koyma özgürlüğü olduğunu yinelemiştir. O zaman geçerli olan yerel kanunlar, bireyleri, herhangi bir kamu otoritesinin veya özel teşebbüsün talebi üzerine gösterilmesi gereken ve kişilerin dinlerini gösteren bir belge olan kimlik kartı taşımakla yükümlü kılmıştır. Bu zorunluluk, bir kişinin dinini açıklama hakkının bunun tam tersini de yani bir kişinin inançlarını açıklamak zorunda kalmama hakkını da içerdiğini ortaya koymak hususunun tanınmasında başarısız olmaktadır. Hükümet, her ne kadar ulusal mevzuatın kişilerin kimlik kartlarındaki din kutusunun boş bırakılmasını talep edebilecekleri şekilde değiştirildiğini söylese de Mahkeme'nin görüşüne göre, dinin silinmesi için başvurmak zorunda olmak, kişinin dine karşı tutumu hakkındaki bilgilerin açıklanması anlamına

[116] AİHM, *Sinan Işık/Türkiye*, No. 21924/05, 2 Şubat 2010.

gelmektedir. Ek olarak, kimlik kartlarında bir din kutusu bulunması ve bunun boş bırakılması özel bir çağrışıma sahiptir, çünkü din hanesinin boş bırakıldığı kimlik kartlarının sahipleri, inançlarını belirten bir karta sahip olanlardan ayrıştırılacaktır. AİHM, yerel mevzuatın AİHS'nin 9. maddesini ihlal ettiği sonucuna varmıştır.

Bununla birlikte, kiliselerin ve dini derneklerin veya toplulukların işleyişi, cemaat içindeki faaliyetlerin iletişimini ve organizasyonunu mümkün kılmak için üyelerin kişisel bilgilerinin işlenmesini gerektirebilir. Bu nedenle, kiliseler ve dini dernekler, genellikle, kişisel verilerin işlenmesiyle ilgili kurallar uygulamışlardır. Genel Veri Koruma Regülasyonunun 91. maddesine göre, bu tür kurallar, kapsamlı oldukları hallerde ve tüzük hükümleriyle uyumlu hale getirilmeleri şartıyla, geçerli olmaya devam edebilirler. Bu tür kurallara sahip kiliseler ve dini dernekler, bu tür otoriteler için Genel Veri Koruma Regülasyonu'nde öngörülen koşulları yerine getirmeleri kaydıyla kendilerine özel olabilecek, bağımsız bir denetim otoritesinin denetimine tabi tutulmalıdır[117].

Dini kuruluşlar kişisel verilerin işlenmesini cemaatleriyle temaslarını sürdürmek veya dini veya hayır etkinlikleri ve düzenlenen festivaller hakkında bilgi iletmek gibi çeşitli nedenlerle üstlenebilirler. Bazı ülkelerde, kiliselerin, üyelerinin kaydını vergi sebebiyle tutmaları gerekmektedir; çünkü dini kuruluşlara üyelik, bireyler tarafından ödenecek vergileri etkileyebilmektedir. Her durumda, Avrupa hukuku uyarınca, dini inançları açığa çıkaran veriler özel nitelikli veridir ve kiliseler – özellikle, dini kuruluşlar tarafından işlenen bilgilerin çoğunlukla çocukları, yaşlıları veya toplumun diğer savunmasız üyelerini ilgilendirmesi sebebiyle – bu verilerin idaresi ve işlenmesinden sorumlu tutulmalıdır.

1.3.4. Bilim ve Sanat Özgürlüğü

Özel hayata saygı ve veri koruma haklarına karşı denge sağlamada bir diğer hak, AB Temel Haklar Bildirgesi'nin 13. maddesi kapsamında açıkça korunan bilim ve sanat özgürlüğüdür. Bu hak, esas olarak, düşünce ve ifade özgürlüğü hakkından çıkarılmaktadır ve Bildirge'nin 1. maddesi (insanlık onuru) göz önüne alınarak uygulanmaktadır. AİHM, sanat özgürlüğünün AİHS'nin 10. maddesi uyarınca korunduğunu düşünmektedir[118]. Bildirge'nin 13. maddesi ile güvence altına alınan hak, aynı zamanda, AİHS'nin 10(2). maddesi ışığında yorumlanabilecek olan Bildirge'nin 52(1). maddesine göre sınırlamalara da tabi olabilmektedir[119].

Örnek: *Vereinigung bildender Künstler v. Avusturya*[120] davasında, Avusturya mahkemesi, başvuru sahibi derneğin, çeşitli kamu figürlerinin kafalarının fotoğraflarını çeşitli cinsel pozisyonlarda gösteren bir tabloyu sergilemesini yasaklamıştır. Tabloda resmi kullanılmış olan bir Avusturyalı parlamento üyesi, resmin sergilenmesini yasaklayan bir tedbir kararı almak amacıyla başvuru sahibi dernek aleyhine dava açmıştır. Yerel mahkeme bir tedbir kararı vermiştir. AİHM, AİHS'nin 10. maddesinin devleti veya nüfusun herhangi bir bölümünü gücendiren, dehşete düşüren veya rahatsız eden fikirlerin iletilmesi hususunu da kapsadığını yinelemiştir. Sanat eserlerini yaratan, icra eden, dağıtan veya sergileyen kişiler fikir ve görüş alışverişine katkıda bulunmaktadır ve devlet, ifade özgürlüğüne haksız yere müdahale etmemekle yükümlüdür. Tablonun bir kolaj olduğu, insanların sadece kafalarının fotoğraflarını kullandığı, bedenlerinin gerçeği yansıtmayı ve hatta ima etmeyi

[117] Genel Veri Koruma Regülasyonu, Madde 91(2).
[118] AİHM, *Müller ve Diğerleri/İsviçre*, No. 10737/84, 24 Mayıs 1988.
[119] Temel Haklar Bildirgesine İlişkin Açıklamalar, OJ 2007 C 303.
[120] AİHM, *Vereinigung bildender Künstler/Avusturya*, No. 68345/01, 25 Ocak 2007, para. 26 ve 34.

amaçlamayacak biçimde gerçekçi olmayan ve abartılı bir şekilde çizildiği göz önüne alındığında, AİHM, "tabloda, [resmedilenlerin] özel hayatının ayrıntılarının ele alındığının anlaşılmasının zor olduğu, bunun daha ziyade [resmedilenlerin] bir politikacı olarak kamuoyu duruşları ile ilgili olduğu" ve "[resmedilenin] eleştirilere daha geniş bir tolerans sergilemek zorunda olduğu" sonucuna varmıştır. AİHM, söz konusu farklı menfaatleri birbiriyle tartarak, resmin daha fazla sergilenmesine karşı süresiz yasağın orantısız olduğunu tespit etmiştir. Mahkeme, AİHS'nin 10. maddesinin ihlal edildiğine karar vermiştir.

Avrupa veri koruma kanunu ayrıca bilimin topluma kattığı özel değeri kabul etmektedir. Genel Veri Koruma Regülasyonu ve Modernize Edilmiş Sözleşme 108, kişisel verilerin yalnızca bilimsel veya tarihi araştırma amacıyla işleneceği sürece daha uzun süre tutulmasına izin vermektedir. Ayrıca ve belirli bir işleme faaliyetinin asıl amacından bağımsız olarak, bilimsel araştırma için kişisel verilerin daha sonra kullanılması, uygunsuz bir amaç olarak kabul edilemez[121]. Aynı zamanda, veri sahiplerinin haklarının ve özgürlüklerinin korunması için, bu tür işlemeler bakımından uygun önlemler alınmalıdır. AB veya Üye Devlet kanunları, veri sahiplerinin örneğin erişim hakkı, düzeltme hakkı, işleme kısıtlaması hakkı ve kişisel verilerinin bilimsel araştırma, tarihsel veya istatistiksel amaçlar için işlenmesi söz konusu olduğunda itiraz etme hakkı gibi haklarından istisna tutulmasını sağlayabilmektedir (ayrıca bkz. Bölüm 6.1 ve Bölüm 9.4).

1.3.5. Fikri Mülkiyetin Korunması

Mülkiyetin korunmasına ilişkin hak, AİHS'nin Birinci Protokol'ünün 1. maddesinde ve ayrıca AB Temel Haklar Bildirgesi'nin 17(1) maddesinde belirtilmiştir. Mülkiyet hakkının, özellikle veri koruma ile ilgili olan önemli bir yönü, Bildirge'nin 17(2) maddesinde açıkça belirtilen fikri mülkiyetin korunmasıdır. AB hukuk düzenindeki bazı direktifler fikri mülkiyeti, özellikle telif haklarını, etkin bir şekilde korumayı amaçlamaktadır. Fikri mülkiyet yalnızca edebi ve sanatsal mülkiyeti değil aynı zamanda patent, ticari marka ve ilgili hakları da kapsamaktadır.

ABAD'ın içtihat hukukunun açıkça ortaya koyduğu üzere; bir temel hak olan mülkiyet hakkının korunması, diğer temel hakların, özellikle de veri koruma hakkının korunmasına karşı dengelenmelidir[122]. Telif hakkı koruma kurumlarının internet erişim sağlayıcılarından internet dosya paylaşım platformları kullanıcılarının kimliğini açıklamasını talep ettiği durumlar olmuştur. Bu tür platformlar, genellikle, telif haklarıyla korunmalarına rağmen, müzik parçalarının internet kullanıcıları tarafından ücretsiz olarak indirmelerini mümkün kılmaktadır.

Örnek: *Promusicae v. Telefónica de España*[123] davası, İspanyol internet erişim sağlayıcısı Telefónica'nın internet erişim hizmetleri sunduğu bazı kişilerin kişisel verilerini müzik üreticilerinin ve müzik ve görsel-işitsel kayıtların yayıncılarının kâr amacı gütmeyen organizasyonu Promusicae'ye açıklamasını reddedilmesiyle ilgilidir. Promusicae, kullanım hakları Promusicae üyelerine ait olan fonogramlara erişim sağlayan bir dosya değişim programı kullandıklarını söylediği kişilere karşı hukuki sürecin başlatılabilmesi için bu bilgilerin açıklanmasını istemiştir.

İspanya mahkemesi konuyu ABAD'a havale ederek, bu tür kişisel bilgilerin, topluluk hukuku

[121] Genel Veri Koruma Regülasyonu, Madde 5 (1) (b) ve Modernize Edilmiş Sözleşme 108, Madde 5 (4) (b).
[122] ABAD, C-275/06, *Productores de Música de España (Promusicae)/Telefónica de España SAU* [GC], 29 Ocak 2008, para. 62–68.
[123] *A.g.e.*, para. 54 ve 60.

uyarınca, özel hukuk bağlamında, telif haklarının etkili bir şekilde korunmasını sağlamak için paylaşılması gerekip gerekmediğini sormuştur. Mahkeme, Bildirge'nin 17. ve 47. maddeleri ışığında da okunan 2000/31, 2001/29 ve 2004/48 sayılı Direktiflere atıfta bulunmuştur. ABAD, bu üç direktifin ve bunların yanı sıra e-Gizlilik Direktifi'nin (2002/58 sayılı Direktif), Üye Devletlerin etkin telif hakkı koruması sağlayan hukuki süreç bağlamında kişisel verileri açıklama yükümlülüğü koymalarını engellemediği sonucuna varmıştır.

ABAD, bu nedenle davanın, farklı temel hakların korunmasına ilişkin şartların – yani özel hayata saygı hakkı karşısında mülkiyeti koruma ve etkin bir hukuk yoluna sahip olma haklarının – uyumlaştırmaya ihtiyacı olup olmadığı sorusunu gündeme getirdiğine dikkat çekmiştir.

Divan, şu sonuca varmıştır: "Üye Devletler, yukarıda belirtilen direktiflerin aktarılması sırasında, bu direktiflerin Topluluk yasal düzeni tarafından korunan çeşitli temel haklar arasında adilane bir dengenin sağlanmasına izin veren bir şekilde yorumlanmasına özen göstermelidir. Ayrıca, bu direktiflere ilişkin önlemler yürürlüğe konurken, Üye Devletler'in otoriteleri ve mahkemeleri, ulusal kanunlarını yalnızca bu direktiflerle tutarlı bir şekilde yorumlamakla kalmamalı, aynı zamanda bu yorumların diğer temel haklarla veya Topluluk hukukunun orantılılık ilkesi gibi diğer genel ilkeleri ile çatışmamasına dikkat etmelidir[124].

Örnek: *Bonnier Audio AB ve Diğerleri v. Perfect Communication Sweden AB*[125] davası, fikri mülkiyet hakları ile kişisel verilerin korunması arasındaki dengeyi ele almıştır. Başvuru sahipleri – 27 sesli kitapta telif hakkı bulunan beş yayıncılık şirketi – İsveç mahkemesi nezdinde, bu telif haklarının bir FTP sunucusu (internet üzerinden dosya paylaşımı ve veri aktarımına izin veren bir dosya aktarım protokolü) ile ihlal edildiğini iddia ederek dava açmıştır. Başvuru sahipleri, internet hizmet sağlayıcısından (İHS), dosyaların gönderildiği IP adresini kullanan kişinin adını ve adresini açıklamasını istemiştir. İHS, ePhone, 2006/24 sayılı Direktifi (Veri Saklama Direktifi – 2014 yılında uygulamadan kaldırılmıştır) ihlal ettiği iddiasıyla başvuruya itiraz etmiştir.

İsveç mahkemesi konuyu ABAD'a havale etmiştir ve 2006/24 sayılı Direktifin, 2004/48 sayılı Direktifin (Fikri Mülkiyet Hakları Yürütme Direktifi) 8. maddesine dayanan ve telif hakkı sahiplerine İHS tarafından IP adreslerinin ihlallerde kullanıldığını iddia edilen aboneler hakkındaki bilgilerin verilmesini kapsayan bir tedbir kararı verilmesini öngören bir ulusal hükmün uygulanmasını engelleyip engellemediğini sormuştur. Soru, başvuru sahibinin belirli bir telif hakkının ihlal edildiğine dair net kanıtlar getirdiği ve önlemin orantılı olduğu varsayımına dayandırılmıştır.

ABAD, 2006/24 sayılı Direktifin, münhasıran, ciddi suçların soruşturulması, tespit edilmesi ve kovuşturulması ve yetkili ulusal makamlara iletilmesi amacıyla elektronik iletişim hizmet sağlayıcıları tarafından elde edilen verilerin idaresi ve saklanması ile ilgili olduğunu belirtmiştir. Bu nedenle, Fikri Mülkiyet Hakları Yürütme Direktifini uygulamaya koyan bir ulusal hüküm, 2006/24 sayılı Direktifin kapsamı dışındadır ve bu nedenle bu Direktif ile engellenmemiştir[126].

Başvuru sahipleri tarafından talep edilen adın ve adresin iletilmesi ile ilgili olarak, ABAD,

---

[124] *A.g.e.*, para. 65 ve 68; ayrıca bkz. ABAD, C-360/10, *Belgische Vereniging van Auteurs, Componisten en Uitgevers CVBA (SABAM)/Netlog NV*, 16 Şubat 2012.
[125] ABAD, C-461/10, *Bonnier Audio AB, Earbooks AB, Norstedts Förlagsgrupp AB, Piratförlaget AB, Storyside AB/Perfect Communication Sweden AB*, 19 Nisan 2012.
[126] *A.g.e.*, para. 40–41.

bu eylemin kişisel verilerin işlenmesi olduğunu ve 2002/58 sayılı Direktif (e-Gizlilik Direktifi) kapsamına girdiğini belirtmiştir. Ayrıca, bu verilerin iletilmesinin, bir telif hakkı sahibinin telif haklarının etkili bir şekilde korunmasını sağlamak için hukuk yargılamalarında gerekli olduğunu ve bu nedenle de 2004/48 sayılı Direktif kapsamında kaldığını belirtmiştir[127].

ABAD, 2002/58 ve 2004/48 sayılı Direktiflerin, ana yargılamada söz konusu olduğu üzere, ulusal mevzuatı engellemeyecek şekilde yorumlanması gerektiğine karar vermiştir ancak bunun sınırlarını şöyle çizmiştir: mevzuat, kişisel verilerin açıklanmasına ilişkin bir başvuru söz konusu olduğunda, yerel mahkemeleri karşı karşıya gelen menfaatleri her durumun kendine has özelliklerine dayanacak ve orantılılık ilkesinin gereklerini dikkate alacak şekilde olmalıdır.

1.3.6. Veri Koruma ve Ekonomik Menfaatler

Dijital veri ya da büyük veri çağında veri, yenilik ve yaratıcılığı arttırmada ekonominin "yeni petrolü" olarak tanımlanmaktadır[128]. Birçok şirket, veri işleme konusunda sağlam iş modelleri kurmuştur ve bu tür işlemler genellikle kişisel verileri içermektedir. Bazı şirketler kişisel verilerin korunmasına ilişkin özel kuralların pratikte ekonomik çıkarlarını etkileyebilecek ölçüde zorlayıcı yükümlülüklerle sonuçlanabileceğine inanabilir. Bu nedenle, veri sorumlularının ve veri işleyenlerin veya kamunun ekonomik çıkarlarının veri koruma hakkının sınırlandırılmasını haklı çıkarıp çıkarmayacağına dair bir soru ortaya çıkmaktadır.

Örnek: *Google İspanya*[129] davasında ABAD, belirli şartların bulunması durumunda kişilerin, arama motorlarından, arama sonuçlarını arama endekslerinden çıkarmalarını talep etme hakkına sahip olduğunu belirtmiştir. Sebep olarak, ABAD, arama motorlarının ve listelenen arama sonuçlarının kullanımının bir bireyin detaylı bir profilini oluşturabildiğine işaret etmiştir. Bu bilgiler, bireyin özel hayatının çok geniş bir kısmıyla ilgili olabilir ve bir arama motoru olmadan kolayca bulunamayabilir veya birbiriyle ilişkilendirilemeyebilir. Dolayısıyla, bu durum, veri sahibinin kişisel verilerin gizliliği ve korunmasına ilişkin temel haklarına potansiyel olarak ciddi bir müdahale oluşturmaktadır.

ABAD daha sonra müdahalenin meşru olup olmadığını incelemiştir. Arama motoru şirketinin işlemeyi gerçekleştirme konusundaki ekonomik menfaati ile ilgili olarak ABAD, "[müdahalenin] sadece böyle bir motorun operatörünün o işlemedeki ekonomik menfaatine dayanılarak meşrulaştırılamayacağı açıktır" demiştir ve Bildirge'nin 7. ve 8. maddelerinde gösterilen temel hakların, "kural olarak", bu ekonomik çıkardan ve kamuoyunun veri sahibinin ismiyle ilgili bir araştırmada bulacağı bilgiyle elde edeceği menfaatten üstün olduğunu belirtmiştir[130].

Avrupa veri koruma kanununun kilit noktalarından biri, bireylere kişisel verileri üzerinde daha fazla kontrol sağlamasıdır. Özellikle dijital çağda, çok büyük miktarda kişisel veriye erişimi olan ve bunları işleyen işletmelerin gücü ile bu kişisel verilerin sahibi olan kişilerin gücü

[127] *A.g.e.*, para. 52–54. Ayrıca bkz. ABAD, C-275/06, *Productores de Música de España (Promusicae)/Telefónica de España SAU* [GC], 29 Ocak 2008, para. 58.
[128] Örneğin bkz., Financial Times (2016), "Veri yeni petrol… ona kim sahip olacak?", 16 Kasım 2016.
[129] ABAD, C-131/12, *Google Spain SL, Google Inc./Agencia Española de Protección de Datos (AEPD), Mario Costeja González* [GC], 13 Mayıs 2014.
[130] *A.g.e.*, para. 81 ve 97.

arasında, bu bilgilerin kontrol edilmesi bakımından bir dengesizlik vardır. ABAD, anonim ve limited şirketler karşısında üçüncü kişilerin menfaatlerine ilişkin *Manni* kararında da belirttiği gibi, verilerin koruması ile ekonomik menfaatleri dengelerken olay bazında bir yaklaşım izlemektedir.

Örnek: *Manni* davası[131], bir bireyin kişisel verilerinin bir kamu ticaret siciline dahil edilmesiyle ilgilidir. Bay Manni, potansiyel müşterilerin sicile baktıklarında on yıldan daha fazla bir süre önce iflas ilan eden bir şirketin yöneticisi olduğunu görebilecek olmaları sebebiyle, Lecce Ticaret Odası'ndan, kişisel verilerinin bu sicilden silinmesini talep etmiştir. Bu bilgi potansiyel müşterilerini önyargılı hale getirmektedir ve bu bilginin Bay Manni'nin ticari menfaatleri üzerinde olumsuz bir etkisi olması mümkündür.

ABAD, AB hukukunun bu durumda silme hakkını kabul edip etmediğini tespit etmeye çağrılmıştır. Sonuca varırken mahkeme, AB veri koruma kurallarını ve Bay Manni'nin eski şirketinin iflasıyla ilgili bilgilerin kaldırılmasındaki ticari menfaatini, kamuoyunun bu bilgiye erişmedeki menfaati ile karşılaştırmıştır. Mahkeme bunu yaparken, şirketlerin kamu sicilindeki ifşaatlarının kanunen ve özellikle de şirket bilgilerine üçüncü şahıslar tarafından daha kolay erişilmesini amaçlayan bir AB Direktifi ile öngörüldüğünü dikkate almıştır. İfşaat, belirli bir şirketle iş yapmak isteyebilecek üçüncü kişilerin menfaatlerini korumak için önemlidir, çünkü anonim şirketler ve limited şirketlerin üçüncü kişilere sunduğu tek güvence, mal varlıklarıdır. Bu nedenle, "ilgili şirketin temel belgeleri, üçüncü kişilerin, bu belgelerin içeriklerini ve özellikle de şirketi temsile yetkisi olan kişilerin tespiti olmak üzere şirket hakkındaki diğer bilgileri açıklanmalıdır"[132].

Sicil tarafından takip edilen meşru amacın önemi göz önüne alındığında, ABAD, üçüncü kişilerin anonim ve limited şirketlerdeki menfaatlerinin korunması ve kanuni kesinliğin, adil ticaretin ve dolayısıyla iç pazarın düzgün işleyişinin sağlanması hususlarının Bay Manni'nin veri koruma mevzuatı kapsamındaki haklarından öncelik olduğuna ve dolayısıyla Bay Manni'nin kişisel verilerinin silinmesi hakkına sahip olmadığına karar vermiştir. Bu özellikle böyledir çünkü bir anonim veya limited şirket aracılığıyla ticarete atılmayı seçen bireyler, kimlikleri ve görevleri ile ilgili bilgileri açıklamaları gerektiğinin farkındadırlar.

Bu davada silinmeyi sağlayacak hiçbir neden bulunmadığına karar veren ABAD, işlemeye tabi tutulmaya itiraz etme hakkının var olduğunu şu şekilde belirtmiştir: "Sicile işlenen kişisel verilere, yeterli uzunlukta bir sürenin geçmesiyle bu verileri öğrenmede özel menfaatleri olan üçüncü kişiler tarafından erişilmesinin kısıtlanmasını haklı kılacak kişiye mahsus özel durumların mevcut olabileceği yadsınamaz."[133]

ABAD, her bir durumun ve bireyle ilgili tüm koşullar göz önüne alınarak üçüncü şahısların şirketler sicilindeki kişisel verilere erişiminin kısıtlanmasını istisnai olarak haklı çıkaracak meşru ve geçersiz kılma nedenlerinin olup olmadığını değerlendirmenin ulusal mahkemelerce yapılacağını belirmiştir. Bununla birlikte, Bay Manni'nin durumunda, kişisel verilerinin sicilde açıklanmasının müşteri çevresini etkilediği iddiasının meşru ve geçerli bir neden olarak kabul edilemeyeceği açıktır. Bay Manni'nin potansiyel müşterilerinin, Bay Manni'nin önceki şirketinin iflasıyla ilgili bilgileri öğrenmede meşru menfaati vardır.

---

[131] ABAD, C-398/15, *Camera di Commercio, Industria, Artigianato e Agricoltura di Lecce/Salvatore Manni*, 9 Mart 2017.
[132] *A.g.e.*, para. 49.
[133] *A.g.e.*, para. 60.

Bildirge'nin 7. ve 8. maddeleri ile güvence altına alınan özel hayata saygı ve kişisel verilerin korunmasına karşın, Bay Manni ve sicile kayıtlı diğer kişilerin temel haklarına müdahalede bulunulması kamu menfaatine hizmet etmektedir ve gerekli ve orantılıdır.

Bu nedenle ABAD, *Manni*'de, veri koruma ve gizlilik haklarının, üçüncü tarafların anonim şirketlerle ve limited şirketlerle ilgili olarak şirketler sicilindeki bilgilere erişime ilişkin menfaatlerinin sağlanmasına üstün gelmediğine karar vermiştir.

2. Veri Koruma Terminolojisi

AB	Ele alınan konular	Avrupa Konseyi
Veri işleme		
Genel Veri Koruma Regülasyonu, Madde 4 (2) ABAD, C-212/13, František Ryneš/Úřad pro ochranu osobních údajů, 2014 ABAD, C-398/15, *Camera di Commercio, Industria, Artigianato e Agricoltura di Lecce/Salvatore Manni*, 2017 ABAD, C-101/01, *Bodil Lindqvist hakkında cezai süreç*, 2003 ABAD, C-131/12, *Google Spain SL, Google Inc./Agencia Española de Protección de Datos (AEPD), Mario Costeja González* [GC], 2014	Tanımlar	Modernize Edilmiş Sözleşme 108, Madde 2 (b) ve (c)
Veri kullanıcıları		
Genel Veri Koruma Regülasyonu, Madde 4 (7) ABAD, C-212/13, *František Ryneš/Úřad pro ochranu osobních údajů*, 2014 ABAD, C-1318/12, *Google Spain SL, Google Inc./Agencia Española de Protección de Datos (AEPD), Mario Costeja González* [GC], 2014	Veri sorumlusu	Modernize Edilmiş Sözleşme 108, Madde 2 (d) Profilleme Tavsiyesi, Madde 1 (g)*
Genel Veri Koruma Regülasyonu, Madde 4 (8)	Veri işleyen	Modernize Edilmiş Sözleşme 108,

		Madde 2 (f) Profilleme Tavsiyesi, Madde 1 (h)
Genel Veri Koruma Regülasyonu, Madde 4 (9)	Alıcı	Modernize Edilmiş Sözleşme 108, Madde 2 (e)
Genel Veri Koruma Regülasyonu, Madde 4 (10)	Üçüncü kişi	
Rıza		
Genel Veri Koruma Regülasyonu, Madde 4 (11) ve 7 ABAD, C-543/09, Deutsche Telekom AG/Bundesrepublik Deutschland, 2011 ABAD, C-536/15, Tele2 (Hollanda) BV ve Diğerleri/Autoriteit Consument en Markt (AMC), 2017	Geçerli rızanın tanımı ve gereklilikleri	Modernize Edilmiş Sözleşme 108, Madde 5 (2) Tıbbi Veri Tavsiyesi, Madde 6, ve başka ilgili tavsiyeler AİHM, Elberte/Letonya, No.61243/08, 2015

*Not: *Avrupa Konseyi, Bakanlar Komitesi (2010), Profil oluşturma bağlamında kişisel verilerin otomatik olarak işlenmesi konusunda kişilerin korunmasına ilişkin üye devletler Bakanlar Komitesi (Profil Önerisi), Tavsiye CM/Rec (2010)13, 23 Kasım 2010.*

2.1. Kişisel Veri

Kilit Noktalar

• Veri, belirli veya belirlenebilir bir kişiye ilişkinse ("veri sahibi") kişisel veridir.

• Bir gerçek kişinin belirlenebilir olup olmadığını tespit etmek için, veri sorumlusu ya da başkaca bir kişinin, bu gerçek kişinin doğrudan ya da dolaylı olarak belirlenmesinde kullanılması muhtemel olan bütün makul araçları – seçip ayırmak gibi – dikkate alması gerekir.

• Kimlik doğrulama, belirli bir kişinin belirli bir kimliğe sahip olduğunu ve/veya belirli faaliyetleri yürütmeye yetkili olduğunu ispat etmek anlamına gelmektedir.

• Modernize Edilmiş Sözleşme 108'de ve AB Veri Koruma hukukunda listelenen, daha fazla koruma gerektiren ve bu nedenle de özel bir yasal rejime tabi olan, hassas veri olarak adlandırılan özel nitelikli kişisel veri kategorileri mevcuttur.

• Veri, belirli ya da belirlenebilir bir kişi ile ilişkilendirilemediği takdirde, anonimleştirilmiştir.

• Maskeleme, kişisel verilerin bunlardan ayrı tutulan ek bilgiler olmadan veri sahibine atfedilememesini sağlayan bir önlemdir. Veri sahiplerinin yeniden belirlenmesini sağlayan 'anahtar', ayrı ve güvenli şekilde tutulmalıdır. Maskeleme sürecinden geçen veri, kişisel veri olarak kalmaktadır. AB hukuku kapsamında maskelenmiş veri kavramı bulunmamaktadır.

• Veri koruma prensipleri ve kuralları, anonimleştirilmiş bilgiler için geçerli değildir. Ancak, bu prensipler ve kurallar, maskelenmiş veriler için geçerlidir.

2.1.1. Kişisel Veri Konseptinin Ana Hatları

AB hukuku ve **Avrupa Konseyi hukuku** uyarınca, "kişisel veri", belirli veya belirlenebilir bir gerçek kişiyle ilgili bilgiler olarak tanımlanır[134]. Kişisel veri, kimliği açık bir şekilde açık olan veya başka bilgilerden oluşturulabilecek olan bir kişi hakkındaki bilgiler ile ilgilidir. Bir kişinin belirlenebilir olup olmadığını tespit etmek için, veri sorumlusu ya da başkaca bir kişinin, bu gerçek kişinin doğrudan ya da dolaylı olarak belirlenmesinde kullanılması muhtemel olan bütün makul araçları – bir kişiye diğerinden farklı davranmayı mümkün kılan seçip ayırmak gibi – dikkate alması gerekir.[135]

Böyle bir kişi hakkındaki veriler işleniyorsa, bu kişiye "veri sahibi" denir.

Veri sahibi

AB hukuku uyarınca, veri koruma kurallarının tek faydalanıcısı gerçek kişilerdir[136] ve yalnızca canlı varlıklar Avrupa veri koruma kanunu kapsamında korunmaktadır.[137] Genel Veri Koruma Regülasyonu (GDPR), kişisel veriyi, belirli veya belirlenebilir bir gerçek kişiyle ilgili herhangi bir bilgi olarak tanımlamaktadır.

Avrupa Konseyi hukuku, Özellikle Modernize Edilmiş Sözleşme 108, aynı zamanda, kişisel verilerinin işlenmesiyle ilgili bireylerin korunmasına da atıfta bulunur. Ayrıca kişisel veri, belirli veya belirlenebilir bir bireye ilişkin herhangi bir bilgi anlamına gelmektedir. Bu gerçek kişi veya birey, GDPR ve Modernize Edilmiş Sözleşme 108'de sırasıyla bahsedildiği üzere,

---

[134] Genel Veri Koruma Regülasyonu, Madde 4 (1); Modernize Edilmiş Sözleşme 108, Madde 2 (a).
[135] Genel Veri Koruma Regülasyonu, Başlangıç hükmü 26.
[136] *A.g.e.*, Madde 1.
[137] *A.g.e.*, Başlangıç hükmü 27. Ayrıca bkz. Madde 29 Çalışma Grubu (2007), Kişisel veri kavramı hakkında 4/2007 sayılı Görüş, WP 136, 20 Haziran 2007, p. 22.

veri koruma kanununda veri sahibi olarak bilinmektedir.

Tüzel kişilerin de bazı korumaları vardır. AİHM içtihat hukuku, tüzel kişilerin, AİHS'nin 8. maddesi uyarınca verilerinin kullanımına karşı korunma haklarının ihlal edildiğine ilişkin iddialarla ilgili olarak yargılamada bulunmaktadır. AİHS'nin 8. maddesi hem özel hayata ve aile hayatına saygı duyma, hem de konut ve yazışma haklarını kapsamaktadır. Mahkeme, bu nedenle, davaları özel hayat başlığından ziyade ikincisinin altında inceleyebilir.

Örnek: *Bernh Larsen Holding AS ve Diğerleri v. Norveç*[138] kararı, üç Norveçli şirketin, müştereken kullandıkları bir bilgisayar sunucusunda tutulan tüm verilerin bir kopyasını vergi denetçilerine sunmalarını emreden bir vergi makamı kararı hakkında şikâyette bulunmaları hakkındadır.

AİHM, başvuru sahibi şirketler üzerindeki böyle bir yükümlülüğün AİHS'nin 8. maddesi uyarınca "konuta" ve "yazışmaya" saygı haklarına müdahale ettiği sonucuna varmıştır. Ancak Mahkeme, vergi makamlarının kötüye kullanıma karşı etkili ve yeterli güvenceye sahip olduğunu tespit etmiştir: Başvuru sahibi şirketlere makul bir süre önceden bildirim yapılmıştır; bu şirketler yerinde inceleme sırasında hazır bulunmaktadır ve ibraz yapabilecek durumdadır ve ilgili belgeler vergi incelemesi tamamlandıktan sonra imha edilecektir. Bu gibi durumlarda, başvuru sahibi şirketlerin "konutuna" ve "yazışmalarına" saygı gösterilmesi hakları ve kendileri için çalışan kişilerin mahremiyetinin korunmasındaki menfaatleri ile vergi tahakkuk ettirmek amacıyla yapılan denetimlerin garanti altına alınmasındaki kamu menfaati arasında adil bir denge sağlanmıştır. Diğer taraftan vergi değerlendirme amaçları için etkin denetim. Mahkeme, bu nedenle, 8. maddenin ihlal edilmediğine karar vermiştir.

Modernize Edilmiş Sözleşme 108'e göre, veri koruma, öncelikle, gerçek kişilerin korunması ile ilgilidir; ancak, Sözleşme Tarafları, veri korumasını iç hukuklarında işletmeler ve dernekler gibi tüzel kişilere de genişletebilirler. Modernize Edilmiş Sözleşmeye İlişkin Açıklayıcı Rapor, ulusal hukukun, sözleşmenin kapsamını tüzel kişilere genişleterek bu tür aktörlerin menfaatlerinin korunabileceğini belirtmektedir.[139] **AB veri koruma kanunu**, tüzel kişileri ilgilendiren veri işlemelerini kapsamaz; ve özellikle tüzel kişinin adı, şekli ve iletişim bilgileri de dahil olmak üzere tüzel kişilik olarak kurulan teşebbüslerle ilgilenmez.[140] Ancak, e-gizlilik Direktifi, tüzel kişilerin, abonelere ve kullanıcılara ilişkin verilerin otomatik olarak depolanması ve işlenmesi için artan kapasiteye ilişkin iletişimlerinin gizliliğini ve meşru menfaatlerini korumaktadır.[141] Benzer şekilde, e-Gizlilik Yönetmeliği taslağı, korumayı tüzel kişilere genişletmektedir.

Örnek: *Volker und Markus Schecke ve Hartmut Eifert vLand Hessen*[142] davasında, ABAD, tarım desteğinden faydalananların kişisel verilerinin yayınlanmasına atıfta bulunarak şöyle demiştir: "Tüzel kişilerin böyle belirlenmesi durumunda Bildirge'nin 7 ve 8. maddeleri kapsamında korunma talebinde bulunabilmesi, tüzel kişinin resmi unvanının bir veya daha fazla gerçek kişiyi belirlediği sürece mümkündür. Bildirge'nin 7 ve 8. maddelerinde tanınan

[138] AİHM, *Bernh Larsen Holding AS ve Diğerleri/Norveç*, No. 24117/08, 14 Mart 2013. Ancak, ayrıca bkz. AİHM, *Liberty ve Diğerleri/Birleşik Krallık*, No. 58243/00, 1 Temmuz 2008.
[139] Modernize Edilmiş Sözleşme 108'e İlişkin Açıklayıcı Rapor, para. 30.
[140] Genel Veri Koruma Regülasyonu, Başlangıç hükmü 14.
[141] E-Gizlilik Direktifi, Başlangıç hükmü 7 ve Madde 1 (2).
[142] ABAD, Birleşik davalar C-92/09 ve C-93/09, *Volker und Markus Schecke GbR ve Hartmut Eifert/Land Hessen* [GC], 9 Kasım 2010, para. 53.

kişisel verilerin işlenmesiyle ilgili olarak özel hayata saygı gösterme hakkı, belirli veya belirlenebilir bir bireye ilişkin herhangi bir bilgi ile ilgilidir […] ".[143]

ABAD; bir yandan AB'nin desteklerin dağıtımında şeffaflığı sağlamadaki menfaatini bir yandan da destekten yararlanan kişilerin gizlilik ve verilerin korunmasına ilişkin temel haklarını dengeleyerek, bu temel haklara yapılan müdahalenin orantısız olduğuna karar vermiştir. Mahkeme, şeffaflık hedefine, ilgili kişilerin haklarına daha az müdahalede bulunacak önlemler ile etkili bir şekilde ulaşılabileceğini düşünmektedir. Ancak, destek alan tüzel kişilere ilişkin bilgi yayınlama oranı incelendiğinde, ABAD farklı bir sonuca varmış, bu tür yayınların orantılılık ilkesinin sınırlarının ötesine geçmediğine karar vermiştir. Mahkeme şöyle demiştir: "Kişisel verilerin korunması hakkının ihlalindeki ağırlık, bir yandan tüzel kişiler ve diğer yandan gerçek kişiler için farklı şekillerde kendini gösterir."[144] Tüzel kişiler, bilgilerin yayınlanması ile ilgili olarak daha külfetli şartlara tabidir. ABAD, ulusal makamlara, her bir faydalanıcı tüzel kişiliğin verilerinin veriler yayınlanmadan önce ve bu verilerin ilişkili herhangi bir gerçek kişiyi belirleyip belirlemediği bakımından inceleme yükümlülüğü getirilmesinin, o makamlara makul olmayan bir idari yük getireceğini söylemiştir. Bu nedenle, tüzel kişilere ilişkin genel bir veri yayını gerektiren mevzuat, söz konusu yarışan menfaatler arasında adil bir denge sağlamıştır.

Verinin doğası

Belirli veya belirlenebilir bir kişiyle ilgili olması koşuluyla her türlü bilgi, kişisel veri olabilir.

Örnek: Bir amirin, çalışanın personel dosyasında saklanan, çalışanın iş performansını değerlendirmesi, çalışan hakkındaki kişisel verilerdendir. Bu durum, her ne kadar kısmen veya tamamen amirin kişisel görüşünü yansıtıyor olsa da – örneğin "çalışan kendini işine adamış değil" – ve sabit gerçekleri yansıtmıyor olsa da – örneğin "çalışan son altı ayın beş haftasında devamsızlık yapmıştır" – böyledir.

Kişisel veri, bir kişinin mesleki faaliyetlerine ilişkin bilgileri de içeren özel hayatına ilişkin bilgileri ve aynı zamanda kamu hayatına ilişkin bilgileri içerir.

Amann davasında[145] AİHM, "kişisel veri" teriminin bir bireyin özel alanına ilişkin meselelerle sınırlı olmadığını söylemiştir. "Kişisel veri" teriminin bu anlamı, GDPR için de böyledir.

Örnek: *Volker und Markus Schecke ve Hartmut Eifert v.Land Hessen*[146] davasında ABAD şöyle demiştir: "Yayınlanan bu bilgilerin profesyonel nitelikteki faaliyetlerle ilgili olmasının bir önemi yoktur […]. Avrupa İnsan Hakları Mahkemesi, bu noktada, Sözleşme 108'in 8. maddesinin yorumuna atıfta bulunarak, 'özel hayat' teriminin, kısıtlayıcı bir şekilde yorumlanmaması gerektiğini ve profesyonel [...] nitelikteki faaliyetleri özel hayat kavramının doğasından ayırmayı haklı çıkaracak bir prensip olmadığını söylemiştir."

[143] *A.g.e.*, para. 52–53.
[144] *A.g.e.*, para. 87.
[145] Bkz. AİHM, *Amann/Switzerland*, No. 27798/95, 16 Şubat 2000, para. 65.
[146] ABAD, Birleşik davalar C-92/09 ve C-93/09, *Volker und Markus Schecke GbR ve Hartmut Eifert/Land Hessen* [GC], 9 Kasım 2010, para. 59.

Örnek: *YS/Minister voor Immigratie, Integratie en Asiel* ve *Minister voor Immigratie, Integratie en Asiel v. M and S*[147] birleştirilmiş davalarında, ABAD, Göçmenlik ve Vatandaşlığa Kabul Hizmetleri'nin oturma izni başvurularıyla ilgili taslak kararında yer alan yasal analizin, bazı kişisel bilgileri içerse bile, kendi başına kişisel veri teşkil etmediğini söylemiştir.

AİHM'nin AİHS'nin 8. maddesine ilişkin içtihat hukuku, özel hayata ve mesleki hayata ilişkin hususların tamamen ayrılmasının zor olabileceğini teyit etmektedir[148].

Örnek: *Bărbulescu v. Romanya*[149] davasında başvuru sahibi, iç düzenlemelere aykırı olarak çalışma saatleri içinde işvereninin internetini kullanmaktan dolayı işten çıkarılmıştır. İşveren, çalışanının iletişimlerini izlemiştir ve iç hukuk sürecinde tamamen özel nitelikteki mesajları gösteren kayıtlar üretilmiştir. 8. maddenin uygulanabilir olduğunu bulurken, AİHM, işverenin kısıtlayıcı düzenlemelerinin başvuru sahibinde makul bir gizlilik beklentisi yaratıp yaratmadığı sorusunu yanıtsız bırakmıştır, ancak her halükârda işverenin talimatlarının işyerindeki özel sosyal hayatı sıfıra indiremeyeceğini tespit etmiştir. Esasa ilişkin olarak, Akit Devletlere, bir işverenin, çalışanlarının işyerindeki – elektronik veya diğer biçimlerdeki – mesleki olmayan iletişimlerini düzenleyebileceği koşullara ilişkin yasal çerçeve oluşturma ihtiyacını değerlendirmede geniş bir takdir payı tanınması gerekmektedir. Bununla birlikte, yerel makamlar, kapsamı ve süresine bakılmaksızın yazışmaların ve diğer iletişimlerin izlenmesi için bir işverenin alacağı önlemlerin, kötüye kullanıma karşı uygun ve yeterli güvenceler eşliğinde kullanılmasını sağlamak zorundadır. Keyfiliğe karşı orantılılık ve usulü garantiler esastır ve AİHM, şartlarla ilgili bir dizi değişken belirlemiştir. Bu değişkenler arasında, örneğin, işverenin çalışanları izlemesinin kapsamı ve çalışanın mahremiyetine girme derecesi, çalışan için sonuçları ve uygun güvencenin sağlanıp sağlanmadığı yer almaktadır. Buna ek olarak, yerel makamlar, iletişimleri izlenen bir çalışanın, en azından özünde, belirtilen kriterlerin nasıl uygulandığını ve alınan tedbirlerin yasal olup olmadığını belirlemek için yargı alanındaki bir yargı organı önünde çareye erişebilmesini sağlamak zorundadır. Bu durumda AİHM, 8. maddenin ihlal edildiğine karar vermiştir, çünkü yerel makamlar, başvuru sahibinin özel hayatına ve yazışmalarına saygı gösterme hakkının uygun bir şekilde korunmasını sağlamamış ve sonuç olarak söz konusu çıkarlar arasında adil bir denge sağlayamamışlardır.

AB hukuku ve **Avrupa Konseyi hukuku** uyarınca, aşağıdaki durumlarda, bilgiler bir kişi hakkında veri içerir:

• Bir kişi bu bilgilere dayanılarak belirlidir veya belirlenebilirdir; veya

• Bir kişi, belirli olmadığı halde, bu bilgiyle, veri sahibinin kim olduğunun daha fazla araştırma yapılarak bulunması mümkün olacak şekilde, ayırt edilebilirdir.

Her iki bilgi türü de Avrupa veri koruma kanunu uyarınca aynı şekilde korunmaktadır. Bireylerin doğrudan ya da dolaylı olarak belirlenebilmesi, "işleme sırasında mevcut teknoloji

[147] ABAD, Birleşik davalar C-141/12 ve C-372/12, *YS/Minister voor Immigratie, Integratie en Asiel ve Minister voor Immigratie, Integratie en Asiel/M and S*, 17 Temmuz 2014, para. 39.
[148] Örneğin bkz., AİHM, *Rotaru/Romania* [GC], No. 28341/95, 4 Mayıs 2000, para. 43; AİHM, *Niemietz/Almanya*, No. 13710/88, 16 Aralık 1992, para. 29.
[149] AİHM, *Bărbulescu/Romania* [GC], No. 61496/08, 5 Eylül 2017, para. 121.

ve teknolojik gelişmeler göz önünde bulundurularak" sürekli değerlendirme gerektirmektedir.[150] AİHM, AİHS'teki "kişisel veri" kavramının, özellikle belirli veya belirlenebilir kişilerin durumları ile ilişkili olarak, Sözleşme 108'deki ile aynı olduğunu tekrar tekrar söylemiştir.[151]

GDPR, bir gerçek kişinin "özellikle ad, kimlik numarası, konum verileri, çevrimiçi bir belirleyici gibi bir belirleyiciye veya o kişinin fiziksel, fizyolojik, genetik, zihinsel, ekonomik, kültürel veya sosyal kimliğine özgü değişkenlerden birine ya da daha fazlasına atıf yapılarak kısmen ya da tamamen belirli olması durumunda" o kişinin belirlenebilir olduğunu belirtmektedir.[152] Bu nedenle, belirleme, bir kişiyi diğer tüm insanlardan ayırt edilebilecek ve kişi olarak teşhis edebilecek şekilde belirleyecek unsurlar gerektirmektedir. Bir kişinin adı, bu belirleme unsurlarının ana örneğidir ve bir kişiyi doğrudan belirleyebilir. Bazı durumlarda, diğer öznitelikler, addakine benzer bir etkiye sahip olabilir ve bu da bir kişiyi dolaylı olarak belirlenebilir kılar. Telefon numarası, sosyal güvenlik numarası ve araç kayıt numarası bir kişiyi belirlenebilir yapan bilgilere örnektir. Ayrıca; davranışlarını ve alışkanlıklarını belirleyerek bireyleri ayırmak için bilgisayarlı dosyalar, çerezler ve web trafiği gözetleme araçları gibi öznitelikleri kullanmak mümkündür. Madde 29 Çalışma Grubu'nun (WP29) görüşünde açıklandığı üzere, "kişinin adını ve adresini sormaksızın, bu kişiyi sosyo-ekonomik, psikolojik, felsefi veya diğer kriterler temelinde sınıflandırmak ve belli kararları bu kişiye atfetmek mümkündür çünkü kişinin (bir bilgisayardaki) irtibat noktası artık kişinin kimliğinin dar anlamda ifşa edilmesini gerektirmemektedir."[153] Hem Avrupa Konseyi hem de AB kapsamında, kişisel verinin tanımı, tüm belirleme olasılıklarını (ve dolayısıyla her türlü belirlenebilme derecelerini) kapsayacak genişliktedir.

Örnek: *Promusicae v. Telefónica de España*[154] davasında, ABAD, "Promusicae tarafından [belirli bir internet dosya paylaşım platformunun] belirli kullanıcılarının adlarının ve adreslerinin kendisine iletilmesi talebinin, kişisel verilerin yani 95/46 sayılı Direktifin 2 (a) maddesindeki (halihazırda GDPR'nin 4 (1) maddesi) tanıma uygun olarak belirli veya belirlenebilir gerçek kişilere ilişkin bilgilerin erişilebilir kılınmasını içerdiği tartışmasızdır. Promusicae'nin sunduğu ve Telefónica'nın itiraz etmediği üzere, iletilen bilgiler Telefónica tarafından saklanmıştır ve bu durum kişisel verilerin işlenmesini oluşturmaktadır".[155]

Örnek: *Scarlet Extended SA v.Société belge des auteurs, compositeurs et éditeurs SCRL (SABAM)*[156] davası, internet hizmet sağlayıcısı Scarlet'in; yazarları, bestecileri ve editörleri temsil eden bir yönetim şirketi olan SABAM tarafından korunan telif haklarını ihlal eden dosya paylaşımını engellemek için dosya paylaşım yazılımı kullanan elektronik haberleşmeleri filtreleyen bir sistem kurmayı reddetmesiyle ilgilidir. ABAD, kullanıcıların IP adreslerinin "kişisel veri olarak korunduğunu çünkü bunların bu kullanıcıların tam olarak belirlenmesine izin verdiğini" belirtmiştir.

---

[150] Genel Veri Koruma Regülasyonu, Başlangıç hükmü 26.
[151] Bkz. AİHM, *Amann/Switzerland* [GC], No. 27798/95, 16 Şubat 2000, para. 65.
[152] Genel Veri Koruma Regülasyonu, Madde 4 (1).
[153] Madde 29 Veri Koruma Çalışma Grubu, *Kişisel veri kavramı hakkında 4/2007 sayılı Görüş*, WP 136, 20 Haziran 2007, p. 15.
[154] ABAD, C-275/06, *Productores de Música de España (Promusicae)/Telefónica de España SAU* [GC], 29 Ocak 2008, para. 45.
[155] Önceki Direktif 95/46, Madde 2 (b), şimdiki Genel Veri Koruma Regülasyonu, Madde 4 (2).
[156] ABAD, C-70/10, *Scarlet Extended SA/Société belge des auteurs, compositeurs et éditeurs SCRL (SABAM)*, 24 Kasım 2011, para. 51.

Pek çok isim benzersiz olmadığı için, bir kişinin kimliğinin belirlenmesi, bir kişinin başkasıyla karıştırılmadığından emin olmak için ek özelliklere ihtiyaç duyabilir. Bazen, bilgilerin ait olduğu kişinin belirlenmesi için doğrudan ve dolaylı niteliklerin birleştirilmesi gerekebilir. Bu anlamda; doğum tarihi ve yeri sıklıkla kullanılmaktadır. Ek olarak, bazı ülkelerde vatandaşlar arasında daha iyi ayrım yapmak için kişiselleştirilmiş numaralar getirilmiştir. Aktarılan vergi verileri[157], oturma iznine ilişkin bir idari belgede bulunan başvuru sahibine ait veriler[158] ve bankacılık ilişkilerine ve güvene dayalı ilişkilere ilişkin belgeler[159] kişisel veri olabilir. Parmak izi, dijital fotoğraf veya iris taraması, konum verileri ve çevrimiçi özellikler gibi biyometrik veriler teknoloji çağında kişileri tanımlamak için giderek daha fazla kullanılmaktadır.

Ancak, Avrupa veri koruma kanununun uygulanabilmesi için, veri sahibinin fiilen belirlenmesi gerekmez; ilgili kişinin belirlenebilir olması yeterlidir. Bir kişinin doğrudan veya dolaylı olarak belirlenebileceği yeterli unsur varsa, o kişi belirlenebilir olarak kabul edilmektedir.[160] GDPR'nin başlangıç hükmü 26'sına göre, kriter, bilginin önceden tahmin edilebilen kullanıcıları tarafından belirleme yapılabilmesi için makul araçların bulunmasının mümkün olup olmadığı ve bunların idare edilip edilmediğidir; bu, üçüncü kişi alıcılar tarafından tutulan bilgileri içermektedir (bkz. Bölüm 2.3.2).

Örnek: Bir yerel makam, yerel sokaklarda hız yapan otomobillerle ilgili veri toplamaya karar verir. Verileri yetkili otoriteye iletmek üzere otomatik olarak zamanı ve yeri kaydederek arabaların fotoğraflarını çeker ki hız sınırlarını ihlal edenleri para cezasına çarptırabilsin. Bir veri sahibi, yerel otoritenin bu tür verileri toplamak için veri koruma kanunu kapsamında yasal bir dayanağı bulunmadığını iddia ederek bir şikâyette bulunur. Yerel otorite kişisel veri toplamadığını savunur. Plakaların isimsiz olduğunu söyler. Yerel otoritenin, araç sahibinin veya sürücünün kimliğini bulmak için genel araç siciline erişmek gibi bir yasal yetkisi yoktur.

Bu temellendirme, GDPR'nin 26 numaralı başlangıç hükmü ile uyumlu değildir. Veri toplamanın amacının açık bir biçimde hız yapan kişilerin belirlenmesi ve cezalandırılması olduğu göz önüne alındığında, bu kişilerin belirlenmesine çalışılacağı öngörülebilirdir. Yerel otoritelerin doğrudan kendilerine sunulan kimlik belirleme araçları bulunmasa da, verileri bu gibi araçlara sahip olan yetkili makama, polise ileteceklerdir. Başlangıç hükmü 26 ayrıca, anlık veri kullanıcısı dışındaki diğer veri alıcılarının kişiyi belirlemeye çalışmasının öngörülebilir olduğu bir senaryoyu da açıkça içermektedir. Başlangıç hükmü 26 ışığında, yerel otoritenin eylemi, belirlenebilir kişiler hakkında veri toplamaya denktir ve bu nedenle, veri koruma kanunu uyarınca yasal bir dayanak gerektirmektedir.

"Gerçek kişiyi belirlemedeki araçların makul bir şekilde kullanılmasının muhtemel olup olmadığına karar vermek için, belirleme için gereken zamana ilişkin masraf ve miktar gibi tüm objektif faktörler, işleme sırasında mevcut teknoloji ve teknolojik gelişmeler göz önünde bulundurularak, dikkate alınmalıdır."[161]

[157] ABAD, C-201/14, *Smaranda Bara ve Diğerleri/Casa Naţională de Asigurări de Sănătate ve Diğerleri*, 1 Ekim 2015.
[158] ABAD, *YS/Minister voor Immigratie, Integratie en Asiel ve Minister voor Immigratie, Integratie en Asiel/M and S*, 17 Temmuz 2014.
[159] AİHM, *M.N. ve Diğerleri/San Marino*, No. 28005/12, 7 Temmuz 2015.
[160] Genel Veri Koruma Regülasyonu, Madde 4 (1).
[161] *A.g.e.*, Başlangıç hükmü 26.

Örnek: *Breyer v. Bundesrepublik Deutschland*[162] davasında ABAD, veri sahiplerinin dolaylı olarak belirlenebilirliği kavramını değerlendirmiştir. Dava, internete her yeni bağlantı yapıldığında değişen, dinamik IP adresleri ile ilgilidir. Federal Alman kurumları tarafından işletilen internet siteleri, siber saldırıları önlemek ve gerektiğinde cezai kovuşturma başlatmak için dinamik IP adreslerini kaydetmiş ve saklamıştır. Yalnızca Bay Breyer'in kullandığı internet hizmet sağlayıcısı, Bay Breyer'i belirlemek için gereken ek bilgilere sahiptir.

ABAD, bir kişinin, bir çevrimiçi medya hizmet sağlayıcısının halka açık hale getirdiği bir internet sitesine erişmesi durumunda bu sağlayıcı tarafından kaydedilen dinamik IP adresinin, yalnızca üçüncü bir tarafın – bu durumda internet hizmet sağlayıcısının –sahip olduğu ve kişiyi belirlemek için gerekli olan ek verilerden olması sebebiyle kişisel verileri oluşturduğunu belirtmiştir[163]. Mahkeme bir verinin kişisel veri teşkil etmesi için "veri sahibinin belirlenmesi için gereken tüm bilgilerin bir kişinin elinde tutulması gerekmediğine" karar verilmiştir. Bir internet hizmet sağlayıcısı tarafından kaydedilen bir dinamik IP adresinin kullanıcıları, belirli durumlarda, örneğin siber saldırılara ilişkin cezai süreç çerçevesinde, diğer kişilerin de yardımıyla belirlenebilir[164]. ABAD'a göre, "internet sağlayıcısının kişi hakkında sahip olduğu ek verilerle veri sahibinin belirlenebilmesi için yasal yollara sahip olması" durumunda, bu, "veri sahibinin belirlenmesi için kullanılması muhtemel bir araç" anlamına gelir. Bu nedenle, bu veriler kişisel veriler olarak kabul edilmektedir.

Avrupa Konseyi hukuku uyarınca, belirlenebilirlik benzer şekilde anlaşılmaktadır. Modernize Edilmiş Sözleşme 108'e İlişkin Açıklayıcı Rapor benzer bir tanım içermektedir: "belirlenebilir" kavramı, yalnızca bireyin medeni veya yasal kimliğini değil aynı zamanda bir kişinin "kişiselleştirilmesini" veya diğerlerinden ayrılmasını ve sonuçta potansiyel olarak diğerlerinden farklı şekilde muamele görmesini ifade eder. Bu 'kişiselleştirme', örneğin kişiye özel olarak atıfta bulunularak veya bir kod numarasına, maskelemeye, biyometrik veya genetik veriye, konum verisine, IP adresine veya başka bir belirleyiciye bağlı bir cihaza veya bir cihaz kombinasyonuna (bilgisayar, cep telefonu, kamera, oyun cihazları vb.) atıfta bulunularak yapılabilir.[165] Bir kişinin belirlenmesi makul olmayan bir zaman, çaba veya kaynak gerektiriyorsa, "belirlenebilir" kabul edilmez. Buna, bir veri sahibinin belirlenmesinin aşırı karmaşık, uzun ve maliyetli işlemler gerektirdiği durum örnektir. Zamanın, çabanın veya kaynakların makul olmaması; işleme işleminin amacı, belirlemenin maliyeti ve faydaları, veri sorumlusunun türü ve kullanılan teknoloji gibi faktörler dikkate alınarak, duruma göre değerlendirilmelidir.[166]

Kişisel verilerin saklandığı veya kullanıldığı şeklin, veri koruma kanununun uygulanabilirliği ile ilgili olmadığını not etmek önemlidir. Yazılı veya sözlü iletişimler, kişisel bilgilerin yanı

[162] ABAD, C-582/14, *Patrick Breyer/Almanya*, 19 Ekim 2016, para. 43.
[163] Avrupa Parlamentosu ve Avrupa Konseyi kişisel verilerin işlenmesi ile ilgili kişilerin korunması ve bu verilerin serbest dolaşımı hakkında 24 Ekim 1995 tarihli ve 95/46/EC sayılı Önceki Direktif, Madde 2 (a).
[164] ABAD, C-70/10, *Scarlet Extended SA/Société belge des auteurs, compositeurs et éditeurs SCRL (SABAM)*, 24 Kasım 2011, para. 47–48.
[165] Modernize Edilmiş Sözleşme 108'e İlişkin Açıklayıcı Rapor, para. 18.
[166] *A.g.e.*, para. 17.

sıra kapalı devre televizyon (CCTV) görüntüleri[167] veya ses[168] dahil görüntüler[169] içerebilmektedir. Elektronik olarak kaydedilen bilgiler ve kağıt üzerindeki bilgiler de kişisel veri olabilir. İnsan dokusuna ilişkin – ve bir kişinin DNA'sını kaydeden – hücre örnekleri bile; veriler bireyin miras aldığı veya edindiği genetik özelliklerle ilgili olduğu, sağlığı ve fizyolojisi hakkında benzersiz bilgiler sağladığı ve bu kişiden gelen biyolojik bir örneğin analizinden kaynaklandığı sürece[170], biyometrik verilerin alınabileceği kaynaklar olabilir[171].

Anonimleştirme

Gerek GDPR gerekse Modernize Edilmiş Sözleşme 108'de (Bölüm 3'te daha ayrıntılı olarak ele alınmıştır) yer alan saklama sınırlaması ilkesine göre, veriler "kişisel verilerin işlendiği amaçlar bakımından gerekli olandan daha uzun bir süre için veri sahiplerinin belirlenmesine izin vermeyecek biçimde" tutulmalıdır.[172] Sonuç olarak, eğer bir veri sorumlusu artık bu verilere ihtiyaç duyulmadığı ve bu verilerin başlangıçtaki amaçlarına hizmet etmediği durumda bu verileri depolamak istemişse, bu verilerin silinmesi veya anonim hale getirilmesi gerekmektedir.

Verilerin anonimleştirilmesi süreci, tüm tanımlayıcı unsurların bir dizi kişisel veriden ayrılması, böylece veri sahibinin artık belirlenebilir olmaması anlamına gelmektedir.[173] Madde 29 Çalışma Grubu (WP29), 05/2014 sayılı Görüş ile, farklı anonimleştirme tekniklerinin etkililiğini ve sınırlarını analiz etmiştir.[174] Madde 29 Çalışma Grubu (WP29), bu tür tekniklerin potansiyel değerini kabul etmektedir ancak bazı tekniklerin mutlaka her durumda işe yaramayacağının altını çizmektedir. Belirli bir durumda en uygun çözümü bulmak için duruma göre uygun bir anonimleştirme işlemine karar verilmelidir. Kullanılan tekniğe bakılmaksızın, belirlemenin geri dönüşü olmayan bir şekilde önlenmesi gerekmektedir. Bu, verilerin anonim hale getirilmesi için, makul bir çaba gösterilerek, bilgilerde ilgili kişiyi ya da kişileri yeniden belirlemeye hizmet edecek hiçbir unsurun kalmayacağı hale getirilmesi anlamına gelmektedir.[175] Yeniden belirleme riski, "verinin niteliği, kullanım bağlamı, mevcut yeniden belirleme teknolojileri ve ilgili maliyetler ışığında ihtiyaç duyulan zaman, çaba veya kaynaklar" hesaba katılarak değerlendirilir.[176]

Veriler başarıyla anonimleştirildiğinde, artık kişisel veri değildir ve bunlara veri koruma mevzuatı uygulanmaz.

GDPR, kişisel veri işlemeyi kontrol eden kişi veya kuruluşun, sırf tüzüğe uymak amacıyla, veri sahibinin belirlenmesi için ek bilgi sağlamak, elde etmek veya işlemek zorunda olmadığını

[167] AİHM, *Peck/Birleşik Krallık*, No. 44647/98, 28 Ocak 2003; AİHM, *Köpke/Almanya* (dec.), No. 420/07, 5 Ekim 2010; EDPS (2010), EDPS video-gözetleme rehberi, 17 Mart 2010.
[168] AİHM, *P.G. ve J.H./Birleşik Krallık*, No. 44787/98, 25 Eylül 2001, para. 59–60; AİHM, *Wisse/Fransa*, No. 71611/01, 20 Aralık 2005 (Fransızca versiyon).
[169] AİHM, *Von Hannover/Almanya*, No. 59320/00, 24 Haziran 2004; AİHM, *Sciacca/İtalya*, No. 50774/99, 11 Ocak 2005; ABAD, C-212/13, *František Ryneš/Úřad pro ochranu osobních údajů*, 11 Aralık 2014.
[170] Genel Veri Koruma Regülasyonu, Madde 4 (13).
[171] Bkz. Madde 29 Çalışma Grubu (2007), *Kişisel veri kavramı hakkında 4/2007 sayılı Görüş*, WP136, 20 Haziran 2007, p. 9; Avrupa Konseyi, İnsan kökenli biyolojik materyallerle ilgili araştırmalar için üye devletler Bakanlar Komitesi'nin Rec (2006) 4 sayılı Tavsiye Kararı, 15 Mart 2006.
[172] *A.g.e.*, Madde 5 (1) (e); Modernize Edilmiş Sözleşme 108, Madde 5 (4) (e).
[173] Genel Veri Koruma Regülasyonu, Başlangıç hükmü 26.
[174] Madde 29 Çalışma Grubu (2014), *Anonimleştirme Tekniklerine İlişkin 05/2014 Sayılı Görüş*, WP216, 10 Nisan 2014.
[175] Genel Veri Koruma Regülasyonu, Başlangıç hükmü 26.
[176] Avrupa Konseyi, Sözleşme Komitesi 108 (2017), Büyük Veri dünyasında kişisel verilerin işlenmesine ilişkin kişilerin korunmasına ilişkin kılavuz, 23 Ocak 2017, para. 6.2.

söylemektedir. Ancak, bu kuralın önemli bir istisnası vardır: ne zaman veri sahibi erişim, imha, silme, işlemenin kısıtlanması ve veri taşınabilirliği haklarını kullanma amacıyla veri sorumlusuna kendisinin belirlenmesini sağlayan ek bilgi sağlarsa, önceden anonimleştirilen veriler sonradan yine kişisel veriler haline gelmektedir.[177]

Maskeleme

Kişisel bilgiler ad, doğum tarihi, cinsiyet, adres veya belirlenmeye yol açabilecek diğer unsurlar gibi özellikler içerir. Kişisel verileri maskeleme işlemi, bu niteliklerin değiştirildiği anlamına gelir.

AB hukuku, "maskeleme" işlemini, "ek bilgilerin ayrı tutulması ve belirli veya belirlenebilir bir gerçek kişiye atfedilmemesini sağlamak için teknik ve örgütsel önlemlerin alınması koşuluyla, kişisel verilerin, artık ek bir bilgi kullanılmadan belirli bir veri sahibine atfedilemeyeceği şekilde işlenmesi" olarak tanımlamaktadır.[178] Anonimleştirilmiş verilerin aksine, maskelenmiş veriler hala kişisel veridir ve bu nedenle veri koruma mevzuatına tabidir. Maskeleme, veri sahipleri için güvenlik risklerini azaltsa da, GDPR kapsamından muaf değildir.

GDPR, çeşitli maskeleme kullanımlarını veri korumasını kuvvetlendirmek için uygun bir teknik önlem olarak kabul etmektedir ve veri işlemelerinin tasarımı ve güvenliği için özellikle belirtmiştir.[179] Maskeleme, aynı zamanda, kişisel verileri başlangıçta toplandıklarından başka amaçlarla işlemek için kullanılabilecek uygun bir korumadır.[180]

Avrupa Konseyi Modernize Edilmiş Sözleşme 108'in yasal tanımında maskeleme açıkça belirtilmemiştir. Ancak, Modernize Edilmiş Sözleşme 108'e İlişkin Açıklayıcı Rapor, açıkça, "maskelemenin veya herhangi bir dijital belirleyicinin/dijital kimliğin kullanılmasının, veri sahibinin hala belirlenebilir ya da kişiselleştirilebilir olması sebebiyle, verilerin anonim hale getirilmesine yol açmadığını" belirtmektedir.[181] Verilerin maskelenmesinin bir yolu, verilerin şifrelenmesidir. Veriler maskelendikten sonra, bir kimliğe olan bağlantı maskeleme ve şifre çözme anahtarı şeklinde var olur. Böyle bir anahtar olmadan, maskelenmiş verileri tespit etmek zordur. Bununla birlikte, şifre çözme anahtarını kullanma yetkisi olanlar için kolayca yeniden belirleme yapmak mümkündür. Şifreleme anahtarlarının yetkisiz kişilerce kullanımı özellikle engellenmelidir. Bu nedenle, Modernize Edilmiş Sözleşme 108 kapsamında "maskelenmiş veri, kişisel veri olarak kabul edilir".[182]

Kimlik Doğrulama

Bir kişinin belirli bir kimliğe sahip olduğunu ve/veya bir güvenlik alanına girme veya bir banka hesabından para çekme gibi bazı şeyleri yapmaya yetkili olduğunu kanıtlayabildiği bir prosedürdür. Örneğin, pasaporttaki fotoğraf ya da parmak izi gibi biyometrik verilerin, kişinin göçmenlik kontrolünde kendisini tanıtırken sunduğu verilerle karşılaştırılmasıyla[183]; kişisel kimlik numarası (PIN) veya şifre gibi yalnızca belirli bir kimliği veya yetkisi olan kişi tarafından bilinmesi gereken bilginin sorulmasıyla veya özel bir çip kartı veya bir bankadaki

[177] Genel Veri Koruma Regülasyonu, Madde 11.
[178] *A.g.e.*, Madde 4 (5).
[179] *A.g.e.*, Madde 25 (1).
[180] *A.g.e.*, Madde 6 (4).
[181] Modernize Edilmiş Sözleşme 108'e İlişkin Açıklayıcı Rapor, para. 18.
[182] *A.g.e.*
[183] *A.g.e.*, para.56–57.

kasanın anahtarı gibi münhasıran belirli bir kimliği veya yetkiyi haiz kişinin bulundurması gereken belirli bir jetonun sunulmasının mecbur kılınmasıyla kimlik doğrulaması yapılabilir. Parolalar veya çip kartlarının yanı sıra – bazen PIN'lerle birlikte olmak üzere – elektronik imzalar elektronik iletişimlerdeki kişiyi belirlemede ve kişinin kimliğini doğrulamada özellikle kullanılan araçlardır.

2.1.2. Özel Nitelikli Kişisel Veri Kategorileri

AB hukuku ve **Avrupa Konseyi hukuku** uyarınca, doğaları gereği, işlendiklerinde veri sahibi için risk oluşturabilecek ve daha fazla korumaya ihtiyaç duyan veriler için özel nitelikli kişisel veri kategorileri vardır. Bu tür veriler bir yasaklama ilkesine tabidir ve bu işlemin yasal olduğu sınırlı sayıda koşul vardır.

Modernize Edilmiş Sözleşme 108 (Madde 6) ve GDPR (Madde 9) çerçevesinde aşağıdaki kategoriler hassas veri olarak kabul edilir:

• ırksal veya etnik kökene işaret eden kişisel veriler;

• felsefi inançlar dahil olmak üzere dini veya diğer inançları, politik görüşleri açığa çıkaran kişisel veriler;

• sendika üyeliğini ortaya koyan kişisel veriler;

• kişiyi tanımlamak amacıyla işlenen genetik veriler ve biyometrik veriler;

• sağlık, cinsel yaşam veya cinsel yönelim ile ilgili kişisel veriler.

Örnek: *Bodil Lindqvist*[184] davası, bir internet sayfasında farklı kişilere isimleriyle veya telefon numaraları ve hobileri hakkındaki bilgiler gibi araçlarla verilen referanslar ile ilgilidir. ABAD, "bir bireyin ayağını incittiğine ve tıbbi gerekçelerle yarı zamanlı çalıştığına ilişkin atfın, sağlıkla ilgili kişisel veri teşkil ettiğini" belirtmiştir.[185]

Ceza Mahkumiyetine ve Suçlarına İlişkin Kişisel Veri

Modernize Edilmiş Sözleşme 108; suçlara, ceza yargılamalarına ve mahkumiyetlere ilişkin kişisel verileri ve özel nitelikli kişisel veri kategorileri listesindeki ilgili güvenlik önlemlerini içermektedir.[186] GDPR kapsamında, ceza mahkumiyetine ve suçlara ilişkin kişisel veriler veya ilgili güvenlik önlemleri, özel nitelikli kişisel veri kategorileri altında belirtilmemiştir, ancak bunlar ayrı bir maddede ele alınmaktadır. GDPR'nin 10. maddesi bu tür verilerin işlenmesinin yalnızca "resmi makamın kontrolü altında veya veri sahiplerinin hak ve özgürlükleri bakımından uygun güvencelerin sağlanması koşuluyla, işlemeye Birlik veya Üye Devlet hukuku tarafından izin verilmiş olmasıyla" yapılmasını öngörmektedir. Öte yandan, ceza mahkumiyeti hakkında bilgi içeren kapsamlı kayıtlar, yalnızca belirli resmi makamların kontrolü altında tutulabilmektedir.[187] AB'de, kişisel verilerin hukuki yaptırımlar bağlamında işlenmesi, belirli bir hukuki enstrüman tarafından yani 2016/680/EU sayılı Direktif[188]

[184] ABAD, C-101/01, *Bodil Lindqvist hakkında cezai süreç*, 6 Kasım 2003, para. 51.
[185] 95/46/EC sayılı Önceki Direktif, Madde 8 (1), şimdiki Genel Veri Koruma Regülasyonu Madde 9 (1).
[186] Modernize Edilmiş Sözleşme 108, Madde 6 (1).
[187] Genel Veri Koruma Regülasyonu, Madde 10.
[188] Avrupa Parlamentosu ve Konseyi'nin suçun önlenmesi, soruşturulması, tespit edilmesi veya kovuşturulması ya da cezaların uygulanması amacıyla yetkili makamlarca kişisel verilerin işlenmesine konu gerçek kişilerin

tarafından yönetilir. Direktif, özellikle suç işlenmesini önlemek, soruşturmak, tespit etmek ve kovuşturmak için kişisel verileri işlediklerinde yetkili makamları bağlayan özel veri koruma kuralları koymaktadır (bkz. Bölüm 8.2.1).

2.2. Veri İşleme

Kilit Noktalar

• "Veri işleme" kişisel veri üzerinde gerçekleştirilen herhangi bir işlemle ilgilidir.

• "İşleme" terimi, otomatik ve otomatik olmayan işlemeyi kapsar.

• AB hukuku uyarınca, "işleme" aynı zamanda yapılandırılmış dosyalama sistemlerinde manuel işlemeyi de ifade eder.

• Avrupa Konseyi hukuku uyarınca, "işleme" teriminin anlamı, manuel işlemeyi içerecek şekilde yerel kanunlarla genişletilebilir.

2.2.1. Veri İşleme Konsepti

Kişisel veri işleme konsepti, hem **AB** hem de **Avrupa Konseyi hukukunda** kapsamlı olarak belirtilmiştir: "kişisel verilerin işlenmesi" [...] kişisel verilerin toplanması, kaydı, düzenlenmesi, yapılandırılması, depolanması, uyarlanması veya değiştirilmesi, geri alınması, danışılması, kullanılması, aktarma veya yayma yoluyla ya da mümkün olan başka bir yolla ifşa edilmesi, sıralanması veya birleştirilmesi, kısıtlanması, silinmesi veya imha edilmesi[189] gibi bütün işlemler" anlamına gelmektedir. Modernize Edilmiş Sözleşme 108, kişisel verilerin muhafaza edilmesini de tanımlamaya eklemektedir.[190]

Örnek: *František Ryneš*[191] davasında, Bay Ryneš, mülkünü korumak için kurduğu ev içi CCTV gözetim sistemi aracılığıyla evindeki pencereleri kıran iki kişinin görüntüsünü kaydetmiştir. ABAD, kişisel verilerin kaydedilmesini ve saklanmasını içeren video görüntülerinin, AB veri koruma kanunu kapsamında olan otomatik veri işlemeyi oluşturduğunu söylemiştir.

Örnek: *Camera di Commercio, Industria, Artigianato e Agricoltura di Lecce/Salvatore Manni*[192] davasında, Bay Manni, kendisini bir emlak şirketinin tasfiyesiyle ilişkilendiren ve bu sebeple itibarını olumsuz etkileyen kişisel verilerinin, ilgili derecelendirme şirketinin sicilinden çıkarılmasını talep etmiştir. ABAD, "bu bilgiyi sicile yazarak, sicilde saklayarak ve uygun olduğu hallerde üçüncü kişilerin talep etmeleri halinde bu kişilere ileterek, bu sicil kayıtlarını tutmaktan sorumlu makamın 'veri sorumlusu' olarak 'kişisel verileri işlediğini'" belirtmiştir.

korunmasına ve bu verilerin serbest dolaşımına ilişkin 27 Nisan 2016 tarih ve (EU) 2016/680 sayılı Direktif ve mülga eden Konsey Çerçeve Kararı 2008/977/JHA, OJ 2016 L 119.

[189] Genel Veri Koruma Regülasyonu, Madde 4 (2). Ayrıca bkz. Modernize Edilmiş Sözleşme 108, Madde 2 (b).

[190] Modernize Edilmiş Sözleşme 108, Madde 2 (b).

[191] ABAD, C-212/13, *František Ryneš/Úřad pro ochranu osobních údajů*, 11 Aralık 2014, para. 25.

[192] ABAD, C-398/15, *Camera di Commercio, Industria, Artigianato e Agricoltura di Lecce/Salvatore Manni*, 9 Mart 2017, para. 35.

Örnek: İşverenler, çalışanları hakkında, maaşlarıyla ilgili bilgiler de dahil olmak üzere veri toplamakta ve işlemektedir. İş sözleşmeleri bunun yapılması için yasal bir zemin oluşturmaktadır.

İşverenler personellerinin maaş verilerini vergi makamlarına iletmekle yükümlü olacaklardır. Bu veri iletimi, aynı zamanda, Modernize Edilmiş Sözleşme 108 ve GDPR anlamında "işleme" teşkil edecektir. Ancak, bu verilerin ifşasının yasal dayanağı iş sözleşmeleri değildir. İşveren tarafından maaş verilerinin vergi makamlarına iletilmesiyle sonuçlanan işleme işlemleri için ek bir yasal dayanak bulunmalıdır. Bu yasal dayanak genellikle ulusal vergi kanunları hükümlerinde bulunmaktadır. Bu tür hükümler olmadan – ve işlemeye yönelik başka bir meşru zemin bulunmadığında – bu kişisel verilerin iletimi yasa dışı işlem teşkil edecektir.

2.2.2. Otomatikleştirilmiş Veri İşleme

Modernize Edilmiş Sözleşme 108 ve GDPR kapsamında veri koruma, otomatik veri işleme için tamamıyla uygulanmaktadır.

AB yasaları uyarınca, otomatik veri işleme, "kişisel veriler üzerinde, tamamen veya kısmen otomatik yollarla" yapılan işlemleri içermektedir.[193] Modernize Edilmiş Sözleşme 108, benzer bir tanım içermektedir.[194] Pratik açıdan, bu, otomatik yollarla, örneğin bir kişisel bilgisayarın, bir mobil cihazın veya bir yönlendiricinin yardımıyla, yapılan herhangi bir kişisel veri işlemenin hem AB hem de Avrupa Konseyi veri koruma kuralları kapsamında olduğu anlamına gelmektedir.

Örnek: *Bodil Lindqvist*[195] davası, bir internet sayfasında farklı kişilere isimleriyle veya telefon numaraları ve hobileri hakkındaki bilgiler gibi araçlarla verilen referanslar ile ilgilidir. ABAD, "bir internet sayfasında, çeşitli kişilere atıfta bulunma ve isimleri yoluyla veya örneğin telefon numaralarını verme veya çalışma koşulları ya da hobileriyle ilgili bilgi verme gibi başka yollarla kişileri belirleme işlemi, 95/46 sayılı Direktif'in 3(1) maddesi anlamında 'kişisel verilerin kısmen veya tamamen otomatik yollarla işlenmesi' teşkil eder" demiştir.[196]

Örnek: *Google Spain SL, Google Inc./Agencia Española Protección de Datos (AEPD), Mario Costeja González*[197] davasında, Bay González, Google arama motorunda kendi adı ile sosyal güvenlik borçlarının tahsiline dair emlak açık artırmasına ilişkin duyurunun yapıldığı iki gazete sayfası arasındaki bağlantının kaldırılmasını veya değiştirilmesini talep etmiştir. ABAD, "internetin otomatik, sürekli ve sistematik olarak, burada yayınlanan bilgilerin aranması anlamında araştırılmasında; arama motorunun işletmecisinin veri 'topladığını' ve bu verileri daha sonra dizinleme programları çerçevesinde 'geri çağırdığını', 'kaydettiğini' ve 'düzenlediğini', sunucularında "depoladığını" ve duruma göre "ifşa ettiğini" ve arama sonuçları listesi şeklinde kullanıcılarının "erişimine sunduğunu" söylemiştir.[198] ABAD, bu tür işlemlerin, "arama motorunun işletmecisinin diğer bilgi türleri bakımından da aynı

[193] Genel Veri Koruma Regülasyonu, Madde 2 (1) ve 4 (2).
[194] Modernize Edilmiş Sözleşme 108, Madde 2 (b) ve (c); Modernize Edilmiş Sözleşme 108'e İlişkin Açıklayıcı Rapor, para. 21.
[195] ABAD, C-101/01, *Bodil Lindqvist hakkında cezai süreç*, 6 Kasım 2003, para. 27.
[196] Genel Veri Koruma Regülasyonu, Madde 2 (1).
[197] ABAD, C-131/12, *Google Spain SL, Google Inc./Agencia Española Protección de Datos (AEPD), Mario Costeja González Costeja González* [GC], 13 Mayıs 2014.
[198] *A.g.e.*, para. 28.

işlemleri yapmasından ve bu ikincisi ile kişisel veriler arasında ayrım yapmamasından bağımsız olarak" "işleme" teşkil ettiği sonucuna varmıştır.

2.2.3. Otomatikleştirilmemiş Veri İşleme

Manuel veri işleme de veri koruması gerektirmektedir.

AB hukukuna göre veri koruma, hiçbir şekilde otomatik veri işleme ile sınırlı değildir. Buna göre, AB hukuku uyarınca, veri koruma, kişisel verilerin manuel dosyalama sisteminde, yani özel olarak yapılandırılmış bir kağıt dosyasında işlenmesi bakımından uygulanmaktadır.[199] Yapılandırılmış dosyalama sistemi, bir dizi kişisel veriyi kategorilere ayırarak belirli kriterlere göre erişilebilir kılan bir dosyalama sistemidir. Örneğin, eğer bir işverenin, çalışanlarının geçen yıl aldığı izinlerin tüm ayrıntılarını içeren ve alfabetik sıraya göre dizilmiş 'çalışan izinleri' adlı bir kağıt dosyası varsa, bu dosya, AB veri koruma kurallarına tabi bir manuel dosyalama sistemi teşkil edecektir. Veri korumanın bu şekilde genişletilmesinin nedeni şudur:

• Kağıt dosyaları, bilgiyi hızlı ve kolay bulmayı sağlayacak şekilde yapılandırılabilir;

• Kişisel verilerin yapılandırılmış kağıt dosyalara kaydedilmesi, otomatik veri işleme için yasaların öngördüğü kısıtlamaları aşmayı kolaylaştırır.[200]

Avrupa Konseyi hukukuna göre, otomatik işleme tanımı, kişisel verilerin manuel kullanımının bazı aşamalarının otomatik işlemeler arasında gerekli olabileceğini kabul etmektedir.[201] Modernize Edilmiş Sözleşme 108'in 2(c) maddesi "otomatik işlemenin kullanılmadığı hallerde, veri işleme, belli kriterlere göre erişilebilen ya da geri çağrılabilen, yapılandırılmış bir veri kümesi içinde bu kişisel veriler üzerinde gerçekleştirilen bir işlem ya da işlem dizisi anlamına gelmektedir" demektedir.

2.3. Kişisel Veri Kullanıcıları

Kilit Noktalar

• Başkalarının kişisel verilerini işlemenin yollarını ve amaçlarını belirleyen kişi, veri koruma kanunu uyarınca bir "veri sorumlusu"dur; eğer bu kararı birkaç kişi birlikte alıyorsa, bunlar "birlikte veri sorumlusu" olabilirler.

• "Veri işleyen", veri sorumlusu adına kişisel verileri işleyen gerçek veya tüzel kişidir.

• Veri işleyen, işlemenin yollarını ve amaçlarını kendisi belirlerse veri sorumlusu olur.

• Kişisel bilgilerin ifşa edildiği herhangi bir kişi, "alıcı"dır.

• "Üçüncü kişi"; veri sahibi, veri sorumlusu, veri işleyen ve veri sorumlusunun veya veri işleyenin doğrudan yetkisi altında kişisel verileri işlemeye yetkili kişiler dışındaki gerçek veya tüzel kişidir.

• Kişisel verilerin işlenmesi için yasal bir temel oluşturan rıza serbestçe verilmeli, aydınlatılmalı, işlemeye yönelik mutabakatı gösteren açık bir onaylayıcı eylem yoluyla

[199] Genel Veri Koruma Regülasyonu, Madde 2 (1).
[200] Genel Veri Koruma Regülasyonu, Başlangıç hükmü 15.
[201] Modernize Edilmiş Sözleşme 108, Madde 2 (b) ve (c).

istenenin spesifik ve açık bir göstergesi olmalıdır.

• Özel nitelikli kişisel veri kategorilerinin rıza temelinde işlenmesi, açık rıza gerektirir.

2.3.1. Veri Sorumluları ve Veri İşleyenler

Veri sorumlusu veya veri işleyen olmanın en önemli sonucu, veri koruma kanunundaki ilgili yükümlülüklere uymaya ilişkin yasal sorumluluktur. Özel sektörde bu genellikle gerçek veya tüzel bir kişidir; kamu sektöründe ise bu genellikle bir yetkili makamdır. Veri sorumlusu ile bir veri işleyen arasında önemli bir ayrım vardır: ilki, işleme amaçlarını ve araçlarını belirleyen gerçek veya tüzel kişi iken; ikincisi, sıkı talimatlara uyarak veri sorumlusu adına verileri işleyen gerçek veya tüzel kişidir. Prensip olarak, işleme üzerinde kontrol sahibi olması gereken ve yasal sorumluluk dahil olmak üzere bunun için sorumluluğu bulunan kişi veri sorumlusudur. Ancak, veri koruma kurallarında yapılan reformla, veri işleyenler artık veri sorumluları için geçerli olan birçok şarta uymakla yükümlüdür. Örneğin, GDPR kapsamında, veri işleyenlerin tüzük kapsamındaki yükümlülüklerine uymuş olmaları için tüm işleme faaliyetleri kategorilerinin kaydını tutmaları gerekmektedir.[202] Veri işleyenler ayrıca işleme güvenliğini sağlamak için uygun teknik ve organizasyonel önlemleri uygulamak[203], bazı durumlarda bir Veri Koruma Görevlisi atamak[204] ve veri ihlallerini veri sorumlusuna bildirmek[205] ile yükümlüdür.

Bir kişinin, işleme amacına ve araçlarına karar verme ve bunları belirleme kapasitesine sahip olup olmaması, olayın somut unsurlarına veya koşullarına bağlı olacaktır. GDPR'deki veri sorumlusu tanımına göre; gerçek kişiler, tüzel kişiler veya diğer herhangi bir kuruluş veri sorumlusu olabilir. Ancak, Madde 29 Çalışma Grubu (WP29), kişilerin haklarını kullanmaları konusunda başvuracakları kişinin daha stabil olmasını sağlamak için "şirket veya organ içindeki belirli bir kişiyi değil şirketi veya organı veri sorumlusu olarak kabul etmenin tercih edilmesi gerektiğini" vurgulamıştır.[206] Örneğin, doktorlara sağlık malzemeleri satan bir şirket, belirli bir bölgedeki tüm doktorların dağıtım listesini derleme ve tutma bakımından veri sorumlusudur, listeyi gerçekten kullanan ve tutan satış müdürü ise veri sorumlusu değildir.

Örnek: Sunshine şirketinin pazarlama bölümü bir pazar araştırması için verileri işlemeyi planladığında, pazarlama bölümü çalışanları değil Sunshine şirketi bu işlemelerin veri sorumlusu olacaktır. Pazarlama bölümü, ayrı bir kimliği olmadığı için veri sorumlusu olamaz.

Gerçek kişiler hem AB hem de Avrupa Konseyi hukukuna göre veri sorumlusu olabilirler. Ancak, tamamen kişisel ya da hane halkına ilişkin bir faaliyetle ilgili olarak başkalarına ilişkin verileri işlerken, özel şahıslar, GDPR ve Modernize Edilmiş Sözleşme 108 kuralları kapsamında kalmazlar ve veri sorumlusu sayılmazlar.[207] Yazışmalarını saklayan veya arkadaşları ve meslektaşları ile yaşadığı olayları ve aile üyelerinin sağlık kayıtlarını tarif ettiği bir kişisel günlük tutan kişi veri koruma kurallarından istisna tutulabilir çünkü bu faaliyetler

[202] Genel Veri Koruma Regülasyonu, Madde 30 (2).
[203] *A.g.e.*, Madde 32.
[204] *A.g.e.*, Madde 37.
[205] *A.g.e.*, Madde 33 (2).
[206] Madde 29 Çalışma Grubu (2010), *"Veri sorumlusu" ve "veri işleyen" kavramları hakkında 1/2010 sayılı Görüş*, WP 169, Brüksel, 16 Şubat 2010.
[207] Genel Veri Koruma Regülasyonu, Başlangıç hükmü 18 ve Madde 2 (2) (c); Modernize Edilmiş Sözleşme 108, Madde 3 (2).

tamamen kişisel veya yalnızca hane halkı ile ilgili faaliyetler olabilir. GDPR ayrıca, kişisel veya hane halkı ile ilgili faaliyetlerin de – bu faaliyetler kapsamında gerçekleştirildiğinde – sosyal ağ oluşturma ve çevrimiçi faaliyetleri içerebileceğini belirtmektedir.[208] Bu halde, veri koruma kuralları, kişisel veya hane halkı ile ilgili faaliyetler için (örneğin, sosyal ağ platformları) kişisel verilerin işlenmesi bakımından araç sağlayan veri sorumluları ve veri işleyenler için tam olarak uygulanır.[209]

Vatandaşların internete erişimi ve kendileri ve diğer kişiler hakkında kişisel bilgileri paylaşmak için e-ticaret platformlarını, sosyal ağları ve blog sitelerini kullanma imkânı, kişisel veri işlemeyi kişisel olmayan veri işlemeden ayırmayı zorlaştırmaktadır.[210] Faaliyetlerin tamamen kişisel veya hane halkı ile ilgili olup olmadığı, koşullara göre değerlendirilmektedir.[211] Mesleki veya ticari yönleri olan faaliyetler, hane halkı istisnasına giremez.[212] Dolayısıyla, veri işlemenin ölçeğinin ve sıklığının profesyonel veya tam zamanlı bir faaliyet olduğunu gösteren durumlarda, özel şahıs veri sorumlusu olarak kabul edilebilir. İşleme faaliyetinin profesyonel veya ticari karakterine ek olarak, göz önünde bulundurulması gereken bir başka faktör de kişisel verilerin, kişinin açıkça özel alanı dışında olacak şekilde, çok sayıda insana açık olup olmadığıdır. Veri Koruma Regülasyonu kapsamındaki içtihat hukuku, özel bir kişi interneti kullanırken başkalarıyla ilgili verileri halka açık bir internet sitesinde yayınladığında veri koruma kanununun uygulanacağını tespit etmiştir. ABAD henüz sosyal medyayı kişisel amaçlar için kullanma gibi 'hane halkı istisnası' kapsamında veri koruma mevzuatı kapsamı dışında sayılabilecek konular hakkında daha fazla rehberlik sağlayacak benzer vakalar hakkında GDPR kapsamında karar vermemiştir.

Örnek: *Bodil Lindqvist*[213], bir internet sayfasında farklı kişilere isimleriyle veya telefon numaraları ve hobileri hakkındaki bilgiler gibi araçlarla verilen referanslar ile ilgilidir. ABAD, "bir internet sayfasında, çeşitli kişilere atıfta bulunma ve isimleri yoluyla veya [...] gibi başka yollarla kişileri belirleme işlemi, Veri Koruma Direktif'inin 3(1) maddesi anlamında 'kişisel verilerin kısmen veya tamamen otomatik yollarla işlenmesi' teşkil eder" demiştir.[214]

Bu tür bir kişisel veri işleme, AB veri koruma kurallarının kapsamı dışında kalan tamamen kişisel veya hane halkı ile ilgili faaliyetler kapsamında değerlendirilmez, çünkü bu istisna "yalnızca kişilerin özel ya da aile hayatları kapsamında yürütülen faaliyetlerle ilgili olarak yorumlanmalıdır; kişisel verilerin internette yayınlanması yoluyla işlenmesi ve belirsiz sayıda insana ulaşılabilir hale gelmesi açık bir biçimde bu durumun dışındadır."[215]

ABAD'a göre, özel olarak kurulmuş bir güvenlik kamerasının görsel kayıtları da belirli koşullar altında AB veri koruma mevzuatı kapsamında kalabilir.

---

[208] Genel Veri Koruma Regülasyonu, Başlangıç hükmü 18.
[209] *A.g.e.*, Başlangıç hükmü 18; Modernize Edilmiş Sözleşme 108'e İlişkin Açıklayıcı Rapor, para. 29.
[210] Bkz. Veri koruma reform paketine ilişkin Madde 29 Çalışma Grubu on açıklaması (2013), *Ek 2 : Kişisel veya hane halkı faaliyetlerinden istisna tutulmaya ilişkin Teklifler ve Değişiklikler*, 27 Şubat 2013.
[211] Modernize Edilmiş Sözleşme 108'e İlişkin Açıklayıcı Rapor, para. 28.
[212] Bkz. Genel Veri Koruma Regülasyonu, Başlangıç hükmü 18 ve Modernize Edilmiş Sözleşme 108'e İlişkin Açıklayıcı Rapor, para. 27.
[213] ABAD, C-101/01, *Bodil Lindqvist hakkında cezai süreç*, 6 Kasım 2003.
[214] *A.g.e.*, para. 27; Önceki Direktif 95/46/EC, Madde 3 (1), şimdiki Genel Veri Koruma Regülasyonu, Madde 2 (1).
[215] ABAD, C-101/01, *Bodil Lindqvist hakkında cezai süreç*, 6 Kasım 2003, para. 47.

Örnek: František Ryneš[216] davasında, Bay Ryneš, mülkünü korumak için kurduğu ev içi CCTV gözetim sistemi aracılığıyla evindeki pencereleri kıran iki kişinin görüntüsünü kaydetmiştir. Kayıt daha sonra polise verilmiştir ve ceza davalarında bu kayda dayanılmıştır.

ABAD, "gözetiminin kısmen de olsa kamusal bir alanı kapsadığı ve buna göre verileri bu şekilde işleyen kişinin özel alanından dışarıya doğru yönlendirildiği düşünüldüğünde bu faaliyetin tamamen 'kişisel veya hane halkı ile ilgili' bir faaliyet olarak ele alınamayacağını" belirtmiştir.[217]

Veri Sorumlusu

AB hukuku uyarınca, veri sorumlusu "yalnız veya başkalarıyla birlikte kişisel verilerin işlenmesinin amaçlarını ve araçlarını belirleyen kişi" olarak tanımlanmaktadır.[218] Bir veri sorumlusunun kararı, verilerin neden ve nasıl işleneceğini belirlemektedir.

Avrupa Konseyi hukuku uyarınca, Modernize Edilmiş Sözleşme 108 bir 'veri sorumlusu'nu "yalnız veya başkalarıyla birlikte, verilerin işlenmesiyle ilgili olarak karar alma yetkisine sahip olan gerçek veya tüzel kişi, kamu otoritesi, hizmet, kurum veya herhangi başka bir kuruluş" olarak tanımlamaktadır.[219] Böyle bir karar alma gücü, işlemenin amaçları ve araçları ile birlikte işlenecek veri kategorileri ve verilere erişimi ile ilgilidir.[220] Bu gücün yasal bir atamadan mı yoksa fiili durumdan mı kaynaklandığına duruma göre karar verilmelidir.[221]

Örnek: *Google Spain*[222] davası, mali geçmişi hakkında eski bir gazete haberinin Google'dan kaldırılmasını isteyen bir İspanyol vatandaş tarafından açılmıştır.

ABAD'a, Google'ın bir arama motorunun operatörü olarak Veri Koruma Regülasyonu'nun 2 (d) maddesi anlamında "veri sorumlusu" olup olmadığı sorulmuştur.[223] ABAD, "veri sahiplerinin etkin ve eksiksiz bir şekilde korunmasını sağlamak" amacıyla 'veri sorumlusu' kavramını geniş bir biçimde yorumlamıştır.[224] ABAD, arama motoru operatörünün faaliyetin amaçlarını ve araçlarını belirlediğini ve internet sayfalarının yayıncıları tarafından internet sayfalarına yüklenen verileri veri sahibinin ismine dayanarak araştıran herhangi bir internet kullanıcısı tarafından erişilebilir kıldığını tespit etmiştir.[225] Bu nedenle, ABAD, Google'ın "veri sorumlusu" olarak kabul edilebileceğini tespit etmiştir.[226]

---

[216] ABAD, C-212/13, *František Ryneš/Úřad pro ochranu osobních údajů*, 11 Aralık 2014, para. 33.
[217] Önceki Direktif 95/46/EC, Madde 3 (2) ikinci girinti, şimdiki Genel Veri Koruma Regülasyonu, Madde 2 (2) (c).
[218] Genel Veri Koruma Regülasyonu, Madde 4 (7).
[219] Modernize Edilmiş Sözleşme 108, Madde 2 (d).
[220] Modernize Edilmiş Sözleşme 108'e İlişkin Açıklayıcı Rapor, para. 22.
[221] *A.g.e.*
[222] ABAD, C-131/12, *Google Spain SL, Google Inc./Agencia Española de Protección de Datos (AEPD), Mario Costeja González* [GC], 13 Mayıs 2014.
[223] Genel Veri Koruma Regülasyonu, Madde 4 (7); ABAD, C-131/12, *Google Spain SL, Google Inc./Agencia Española de Protección de Datos (AEPD), Mario Costeja González* [GC], 13 Mayıs 2014, para. 21.
[224] ABAD, C-131/12, *Google Spain SL, Google Inc./Agencia Española de Protección de Datos (AEPD), Mario Costeja González* [GC], 13 Mayıs 2014, para. 34.
[225] *A.g.e.*, para. 35–40.
[226] *A.g.e.*, para. 41.

Veri sorumlusu veya veri işleyenin AB dışında kurulması halinde, söz konusu şirketin, yazılı olarak, AB içinde bir temsilci ataması gerekmektedir.[227] GDPR, temsilcinin "kendilerine mal veya hizmetlerin sunulması ile ilgili olarak kişisel verileri işlenen veya davranışları izlenen veri sahiplerinin bulunduğu Üye Devletler'den birinde kurulması gerektiğini" vurgulamaktadır.[228] Temsilci belirlenmemişse, veri sorumlusunun veya veri işleyenin kendisine karşı yasal işlem başlatılabilir.[229]

Birlikte Veri Sorumluluğu

GDPR, iki veya daha fazla veri sorumlusunun işleme amaç ve araçlarını birlikte belirlemeleri halinde birlikte veri sorumlusu olarak kabul edildiklerini ifade etmektedir. Bu, paylaşılan bir amaç için verileri işlemeye birlikte karar verdikleri anlamına gelmektedir.[230] Modernize Edilmiş Sözleşme 108'e İlişkin Açıklayıcı Rapor, **Avrupa Konseyi çerçevesinde** birden fazla veri sorumlusunun veya birlikte veri sorumluluğunun mümkün olduğunu belirtmektedir.[231]

Madde 29 Çalışma Grubu (WP29), birlikte veri sorumluluğunun farklı biçimlerde olabileceğine ve farklı veri sorumlularının kontrol faaliyetlerine katılımının eşit olamayabileceğine işaret etmektedir.[232] Bu esneklik, giderek kompleksleşen veri işleme vakalarına hitap etmeyi mümkün kılmaktadır.[233] Bu sebeple, birlikte veri sorumluları, tüzük kapsamındaki yükümlülüklere uyma konusundaki sorumluluklarını belli bir sözleşmede belirlemelidir.[234]

Birlikte veri sorumluluğu, işleme faaliyeti bakımından birlikte sorumluluğa yol açmaktadır.[235] **AB hukuku** çerçevesinde bu, veri sahibinin etkin bir şekilde tazmin edilmesini sağlamak için, her veri sorumlusu veya veri işleyenin, birlikte veri sorumluluğu kapsamındaki işlemeden kaynaklanan tüm zararlardan tamamen sorumlu tutulabilmesi anlamına gelmektedir.[236]

Örnek: Bazı kredi kuruluşları tarafından, temerrüde düşen müşterileri hakkında birlikte yürütülen bir veri tabanı, birlikte veri sorumluluğunun yaygın bir örneğidir. Bir kişi, birlikte veri sorumlusu olan bir bankaya kredi almak için başvurduğunda, bankalar, başvuru sahibinin kredibilitesi hakkında bilinçli kararlar alınmasına yardımcı olmak için veri tabanını kontrol etmektedir.

Yasal hükümler, birlikte veri sorumluluğunda, paylaşılan amacın veri sorumlularının her biri için aynı olması gerekip gerekmediğini veya amaçların yalnızca kısmen örtüşmesinin yeterli olup olmadığını açıkça ifade etmemektedir. Bununla ilgili olarak şimdiye kadar Avrupa düzeyinde bir içtihat hukuku oluşmuş değildir. Madde 29 Çalışma Grubu (WP29), veri sorumluları ve veri işleyenler hakkındaki 2010 tarihli görüşünde, birlikte veri sorumlularının ya tüm işleme amaçları ve araçlarını paylaşabileceğini ya da sadece bazı işleme amaçlarını ya

[227] Genel Veri Koruma Regülasyonu, Madde 27 (1).
[228] *A.g.e.*, Madde 27 (3).
[229] *A.g.e.*, Madde 27 (5).
[230] *A.g.e.*, Madde 4 (7) ve Madde 26.
[231] Modernize Edilmiş Sözleşme 108, Madde 2 (d); Modernize Edilmiş Sözleşme 108'e İlişkin Açıklayıcı Rapor, para. 22.
[232] Madde 29 Çalışma Grubu (2010), *"Veri sorumlusu" ve "veri işleyen" kavramları hakkında 1/2010 sayılı Görüş"*, WP 169, Brüksel, 16 Şubat 2010, p. 19.
[233] *A.g.e.*
[234] Genel Veri Koruma Regülasyonu, Başlangıç hükmü 79.
[235] *A.g.e.*, para. 21.
[236] *A.g.e.*, Madde 82 (4).

da araçlarını ya da bunların bir kısmını paylaşabileceğini belirtmektedir.[237] İlki farklı oyuncular arasında çok yakın bir ilişki olduğunu ima ederken, ikincisi daha gevşek bir ilişki olduğunu göstermektedir.

Madde 29 Çalışma Grubu (WP29), mevcut veri işleme vakasının artan kompleksliğine hitap etmek için bir miktar esneklik sağlama amacıyla birlikte veri sorumluluğu kavramının daha geniş bir yorumunu savunmaktadır.[238] Society for Worldwide Interbank Financial Telecommunication (SWIFT) ile ilgili bir dava, Çalışma Grubu'nun duruşunu göstermektedir.

Örnek: SWIFT olarak adlandırılan davada, Avrupa bankacılık kurumları, başlangıçta bir veri işleyen olarak, bankacılık işlemleri sırasında veri transferini yürütmesi için, SWIFT'i işe almışlardır. SWIFT, Amerika Birleşik Devletleri'ndeki (ABD) bir bilgi işlem merkezinde depolanan bu tür bankacılık işlem verilerini, kendisini işe Avrupa bankacılık kurumları tarafından açıkça emredilmeksizin ABD Hazine Bakanlığı'na açıklamıştır. Madde 29 Çalışma Grubu, bu durumun hukuka uygunluğunu değerlendirirken, SWIFT'in yanı sıra SWIFT'i işe alan Avrupa bankacılık kurumlarının da Avrupa müşterilerinin verilerinin ABD makamlarına açıklanması konusunda birlikte veri sorumluları olarak görülmesi gerektiği sonucuna varmıştır.[239]

Veri İşleyen

Veri işleyen, **AB hukuku uyarınca**, kişisel verileri veri sorumlusu adına işleyen kişi olarak tanımlanmaktadır.[240] Bir veri işleyene verilen faaliyetler çok özel bir görev veya bağlamla sınırlı olabilir veya oldukça genel ve kapsamlı olabilir.

Avrupa Konseyi hukuku uyarınca, veri işleyenin anlamı AB hukuku ile aynıdır.[241]

Veri işleyenler, başkaları için veri işlemenin yanı sıra, kendi amaçları için gerçekleştirdikleri işlemelerle ilgili olarak, örneğin kendi çalışanlarının idaresi, satışları ve hesapları ile ilgili olarak kendi başlarına veri sorumlusu olacaktır.

Örnek: Everready şirketi, diğer şirketler için insan kaynakları verilerinin yönetimi amacıyla veri işleme konusunda uzmanlaşmıştır. Bu işlev bakımından Everready bir veri işleyendir. Ancak, Everready kendi çalışanlarının verilerini işliyorsa, işveren olarak yükümlülüklerini yerine getirmek amacıyla yapılan veri işleme operasyonlarının veri sorumlusudur.

Veri Sorumlusu ve Veri İşleyen Arasındaki İlişki

Görüldüğü gibi, veri sorumlusu işleme amaç ve araçlarını belirleyen kişi olarak tanımlanmaktadır. GDPR; AB veya Üye Devlet hukuku veri işleyenin kişisel verileri işlemesini

[237] Madde 29 Çalışma Grubu (2010), *"Veri sorumlusu" ve "veri işleyen" kavramları hakkında 1/2010 sayılı Görüş*, WP 169, Brüksel, 16 Şubat 2010, p. 19.
[238] *A.g.e.*
[239] Madde 29 Çalışma Grubu (2006), *Kişisel verilerin the Society for Worldwide Interbank Financial Telecommunication (SWIFT) tarafından işlenmesine ilişkin 10/2006 sayılı Görüş*, WP 128, Brüksel, 22 Kasım 2006.
[240] Genel Veri Koruma Regülasyonu, Madde 4 (8).
[241] Modernize Edilmiş Sözleşme108, Madde 2 (f).

gerektirmedikçe, veri işleyenin sadece veri sorumlusunun talimatlarıyla ilgili kişisel verileri işleyebileceğini açıkça belirtmektedir.[242] Veri sorumlusu ve veri işleyen arasındaki sözleşme, ilişkilerinin bir esas unsurudur ve yasal bir gerekliliktir.[243]

Örnek: Sunshine Company'nin yöneticisi, bulut tabanlı veri depolama alanında uzman olan Cloudy Company'nin Sunshine'ın müşteri verilerini yönetmesi gerektiğine karar vermiştir. Sunshine Company, veri sorumlusu olarak kalmaktadır ve Cloudy Company yalnızca veri işleyendir; çünkü sözleşme uyarınca Cloudy, Sunshine şirketinin müşteri verilerini yalnızca Sunshine şirketinin belirlediği amaçlar doğrultusunda kullanabilecektir.

İşleme araçlarını belirleme gücü veri işleyene devredildiyse, veri sorumlusu yine de veri işleyenin işleme araçlarına ilişkin kararları üzerinde uygun bir kontrol uygulayabilmelidir. Genel sorumluluk, kararlarının veri koruma hukukuna ve kendi talimatlarına uymasını sağlamak için veri işleyenleri denetlemesi gereken veri sorumlusuna aittir.

Ayrıca, bir veri işleyen, veri sorumlusu tarafından emredilen veri işleme koşullarına uymadığında, en azından veri sorumlusunun talimatlarını ihlal ettiği ölçüde veri sorumlusu haline gelecektir. Bu, büyük olasılıkla, veri işleyeni hukuka aykırı davranan bir veri sorumlusu yapacaktır. Buna karşılık, ilk veri sorumlusu, veri işleyenin görevini ihlal etmesinin nasıl mümkün olduğunu açıklamak zorunda kalacaktır.[244] Nitekim, Madde 29 Çalışma Grubu (WP29), bu durumlarda, veri sahiplerinin menfaatlerinin en iyi şekilde korunmasını sağladığı için, birlikte veri sorumluluğunu kabul etme eğilimindedir.[245]

Veri sorumlusunun küçük bir işletme olması ve veri işleyenin hizmet koşullarını belirleme gücüne sahip büyük bir şirket şirketi olması durumunda sorumluluk dağılımı ile ilgili sorunlar olabilir. Ancak, böyle durumlarda, Madde 29 Çalışma Grubu (WP29), ekonomik dengesizlik temelinde sorumluluk standardının düşürülmemesi gerektiğini ve veri sorumlusu kavramı anlayışının sürdürülmesi gerektiğini savunmaktadır.[246]

Bir veri sorumlusu ile bir veri işleyen arasındaki ilişkinin detayları, netlik ve şeffaflık adına, yazılı bir sözleşmede kaydedilmelidir.[247] Sözleşme özellikle; işlemenin konusunu, niteliğini, amacını ve süresini, kişisel verinin türünü ve veri sahiplerinin kategorilerini içermelidir. Sözleşme, ayrıca, veri sorumlusunun ve veri işleyenin gizlilik ve güvenlik ile ilgili şartlar gibi yükümlülüklerini ve haklarını da belirtmelidir. Bu tür bir sözleşmenin olmaması, veri sorumlusunun karşılıklı sorumlulukları yazılı olarak belgeleme yükümlülüğünü ihlal etmektir ve yaptırımlara yol açabilir. Zararın, veri sorumlusunun yasal talimatları dışında hareket etmenin ya da yasal talimatlarına uymamanın bir sonucu olarak oluşması halinde, yalnızca veri sorumlusu değil veri işleyen de sorumlu tutulabilir.[248] Veri işleyen, veri sorumlusu adına

[242] Genel Veri Koruma Regülasyonu, Madde 29.
[243] *A.g.e.*, Madde 28 (3).
[244] *A.g.e.*, Madde 82 (2).
[245] Madde 29 Çalışma Grubu (2010), *"Veri sorumlusu" ve "veri işleyen" kavramları hakkında 1/2010 sayılı Görüş*, WP 169, Brüksel, 16 Şubat 2010, p. 25; Madde 29 Çalışma Grubu (2006), *Kişisel verilerin the Society for Worldwide Interbank Financial Telecommunication (SWIFT) tarafından işlenmesine ilişkin 10/2006 sayılı Görüş*, WP 128, Brüksel, 22 Kasım 2006.
[246] Madde 29 Çalışma Grubu (2010), *"Veri sorumlusu" ve "veri işleyen" kavramları hakkında 1/2010 sayılı Görüş*, WP 169, Brüksel, 16 Şubat 2010, p. 26.
[247] Genel Veri Koruma Regülasyonu, Madde 28 (3) ve (9).
[248] *A.g.e.*, Madde 82 (2).

yürüttüğü tüm işleme faaliyeti kategorilerinin kayıtlarını tutmalıdır.[249] Görevlerini yerine getirmesi sırasında denetleyici makamın talep etmesi halinde, veri sorumlusunun ve veri işleyenin, bu makam ile işbirliği yapması ve bu kayıtların denetleyici makama sunulması gerekmektedir.[250] Veri sorumluları ve veri işleyenler, ayrıca, GDPR gerekliliklerine uygunluklarını kanıtlamak için, onaylanmış bir davranış kurallarına veya bir sertifika mekanizmasına katılma olanağına sahiptir.[251]

Veri işleyenler belirli görevleri başka alt veri işleyenlere devretmek isteyebilirler. Bu; veri sorumlusu ile veri işleyen arasında, her bir durumda veri sorumlusunun yetkisinin gerekli olup olmadığı veya tek başına bilgilendirmenin yeterli olup olmadığı da dahil olmak üzere uygun sözleşme şartlarının sağlanması halinde, yasal olarak izin verilebilirdir. GDPR, bir alt veri işleyenin veri koruma yükümlülüklerini yerine getirmemesi halinde dahi, ilk veri işleyenin veri sorumlusuna karşı tamamen sorumlu olarak kaldığını belirtmektedir.[252]

Avrupa Konseyi hukukuna göre, veri sorumlusu ve veri işleyen kavramlarının yorumlanmasına ilişkin yukarıdaki açıklamalar tamamen uygulanabilirdir.[253]

2.3.2. Alıcılar ve Üçüncü Kişiler

Veri Koruma Regülasyonu tarafından getirilen bu iki kişi veya varlık kategorisi arasındaki farklılık, esas olarak, veri sorumlusu ile olan ilişkilerinde ve bunun sonucunda veri sorumlusu tarafından tutulan kişisel verilere erişme yetkilerinde yatmaktadır.

'Üçüncü kişi', veri sorumlusundan ve veri işleyenden farklı bir kişidir. GDPR'nin 4 (10) maddesine göre üçüncü kişi, "veri sahibi, veri sorumlusu, veri işleyen ve veri sorumlusunun veya veri işleyenin doğrudan yetkisi altında kişisel verileri işlemeye yetkili olanlardan olmamak kaydıyla; gerçek veya tüzel kişi, kamu otoritesi, kurum veya herhangi başka bir kuruluştur". Bu, veri sorumlusundan farklı bir kuruluş için çalışan kişilerin – aynı grup veya holding şirketine ait olsalar bile – 'üçüncü kişi' olacağı (ya da ona ait olacağı) anlamına gelmektedir. Öte yandan, merkezin doğrudan yetkisi altında müşteri hesaplarını işleyen banka şubeleri "üçüncü kişi" olmayacaktır.[254]

'Alıcı', 'üçüncü kişi'den daha geniş bir terimdir. GDPR'nin 4 (9) maddesi anlamında alıcı, "bir üçüncü kişi olsun veya olmasın, verilerin ifşa edildiği gerçek veya tüzel kişi, kamu otoritesi, kurum veya herhangi başka bir kuruluş" anlamına gelmektedir. Bu alıcı; veri sorumlusunun veya veri işleyenin dışındaki bir kişi – bu halde alıcı, bir üçüncü kişi olacaktır – olabileceği gibi bir çalışan veya aynı şirket ya da otorite içindeki başka bir bölüm gibi veri sorumlusunun veya veri işleyenin içindeki bir kişi de olabilir.

Alıcılar ve üçüncü kişiler arasındaki ayrım, sadece, verilerin hukuka uygun olarak ifşa edilmesi koşulları bakımından önemlidir. Bir veri sorumlusunun veya veri işleyenin çalışanları, veri sorumlusunun veya veri işleyenin işleme faaliyetlerinde yer almaları durumunda, yasal bir zorunluluk gerekmeksizin kişisel verilerin alıcıları olabilir. Oysa, veri sorumlusundan veya veri işleyenden ayrı olan bir üçüncü kişi, belirli bir durumda belirli yasal gerekçeler olmadıkça veri

[249] *A.g.e.*, Madde 30 (2).
[250] *A.g.e.*, Madde 30 (4) ve 31.
[251] *A.g.e.*, Madde 28 (5) ve 42 (4).
[252] *A.g.e.*, Madde 28 (4).
[253] Örneğin, bkz. Modernize Edilmiş Sözleşme 108, Madde 2 (b) ve (f); Profilleme Tavsiyesi, Madde 1.
[254] Madde 29 Çalışma Grubu (2010), *"Veri sorumlusu" ve "veri işleyen" kavramları hakkında 1/2010 sayılı Görüş*, WP 169, Brüksel, 16 Şubat 2010, p. 31.

sorumlusunun işlediği kişisel verileri kullanma yetkisine sahip değildir.

Örnek: İşverenin kendisine verdiği görevler kapsamında kişisel verileri kullanan bir veri sorumlusunun çalışanı, bir veri alıcısıdır ancak bir üçüncü kişi değildir çünkü verileri veri sorumlusu adına ve veri sorumlusunun talimatlarına göre kullanmaktadır. Örneğin, bir işveren, yaklaşmakta olan performans değerlendirmeleri için çalışanlarının kişisel verilerini insan kaynakları departmanına açıklarsa, insan kaynakları ekibi bu verilerin alıcısı olacaktır çünkü bu veriler veri sorumlusunun işleme süreci için kendilerine açıklanmıştır.

Ancak, bir kuruluşun, çalışanları hakkındaki verileri, çalışanlar için kişiye özel eğitim programları hazırlayan bir eğitim şirketine sunması halinde, eğitim şirketi bir üçüncü kişidir. Bunun nedeni, eğitim şirketinin bu kişisel verileri işlemek için ("insan kaynakları" durumunda veri sorumlusu ile iş ilişkisinden kaynaklanan) belirli bir meşruiyete veya yetkiye sahip olmamasıdır. Başka bir deyişle, eğitim şirketi bu bilgileri veri sorumlusundan iş ilişkisi sırasında almamıştır.

2.4. Rıza

Kilit Noktalar

• Kişisel verilerin işlenmesi için yasal bir temel oluşturan rıza serbestçe verilmeli, aydınlatılmalı, işlemeye yönelik mutabakatı gösteren açık bir onaylayıcı eylem yoluyla istenenin spesifik ve açık bir göstergesi olmalıdır.

• Özel nitelikli kişisel veri kategorilerinin işlenmesi için açık rıza gerekmektedir.

4. Bölüm'de ayrıntılı olarak ele alınacağı üzere, rıza, kişisel verilerin işlenmesinde kullanılan altı meşru gerekçeden biridir. Rıza, "serbestçe verilen, aydınlatılmış, veri sahibinin istediğini açık bir biçimde gösteren gösterge" anlamına gelmektedir.[255]

AB hukuku, rızanın geçerli olması için çeşitli unsurlar ortaya koymaktadır; bu unsurlar, veri sahiplerinin kendi verilerinin belirli bir husus için kullanılmasını gerçekten kabul ettiklerini garantilemeyi amaçlamaktadır:[256]

• Rıza; serbestçe verildiğine, spesifik olduğuna, aydınlatıldığına, veri sahibinin kişisel verilerinin işlenmesine onay verdiğini açık bir şekilde gösterdiğine ilişkin açık bir onaylayıcı hareket yoluyla verilmelidir. Böyle bir hareket; bir eylem veya bir açıklama olabilir.

• Veri sahibi, herhangi bir zamanda rızasını geri alma hakkına sahip olmalıdır.

• 'Hizmet şartları' gibi diğer hususları da içeren yazılı bir bildirim bağlamında; rıza taleplerinin açık ve sade bir dilde ve diğer hususlardan açıkça ayrılan, anlaşılır ve kolay erişilebilir bir biçimde olması gerekir; bu bildirimin bir kısmının GDPR'ye aykırı olması durumunda bildirim bağlayıcı olmayacaktır.

[255] Genel Veri Koruma Regülasyonu, Madde 4 (11). Ayrıca bkz. Modernize Edilmiş Sözleşme 108, Madde 5 (2).
[256] Genel Veri Koruma Regülasyonu, Madde 7.

Rıza, ancak tüm bu şartların yerine getirilmesi halinde veri koruma kanunu bağlamında geçerli olacaktır. Veri sahibinin verilerinin işlenmesi için rıza gösterdiğini kanıtlamak, veri sorumlusunun sorumluluğundadır.[257] Geçerli rızanın unsurları, kişisel verilerin işlenmesi ile ilgili yasal gerekçelerle Bölüm 4.1.1'de daha ayrıntılı olarak ele alınacaktır.

Sözleşme 108, rızaya ilişkin bir tanım içermemektedir; bu husus iç hukuka bırakılmıştır. Ancak, **Avrupa Konseyi hukuku uyarınca**, geçerli rızanın unsurları daha önce açıklananlara karşılık gelmektedir.[258]

Geçerli bir rıza için medeni hukuk kapsamında gereken – fiil ehliyeti gibi – ek şartlar, veri koruma bağlamında da uygulama bulmaktadır çünkü bu şartlar temel hukuki ön koşullardır. Fiil ehliyeti olmayan kişilerin geçersiz rızaları, bu kişilerin verilerinin işlenmesi için yasal bir dayanak bulunmamasına neden olacaktır.

Reşit olmayanların sözleşme akdetme konusundaki fiil ehliyetleri ile ilgili olarak GDPR, geçerli rıza alınması için öngördüğü asgari yaş kurallarının Üye Devletler'in genel sözleşme hukukunu etkilemediğini söylemektedir.[259]

Rıza, veri sahibinin niyetinden şüphe duyulmayacak şekilde açık bir şekilde verilmelidir.[260] Rıza; hassas verilerin işlenmesiyle ilgili ise açık bir şekilde verilmelidir ve sözlü ya da yazılı olarak verilebilir.[261] Yazılı rıza elektronik araçlarla da verilebilir.[262] Hem AB hem de Avrupa Konseyi hukuku çerçevesinde, bir kişinin kişisel verilerinin işlenmesine ilişkin kabulü bir açıklama veya açık bir olumlu eylemle yapılmalıdır.[263] Dolayısıyla; sessiz kalma, önceden tik atılmış kutular, önceden doldurulmuş formlar veya hareketsizlik rıza sayılmaz.[264]

3. Avrupa Veri Koruma Kanunu'nun Ana Prensipleri

AB	Ele Alınan Konular	Avrupa Konseyi
Genel Veri Koruma Regülasyonu, Madde 5 (1) (a)	Meşruluk prensibi	Modernize Edilmiş Sözleşme 108, Madde 5 (3)
Genel Veri Koruma Regülasyonu, Madde 5 (1) (a)	Adillik prensibi	Modernize Edilmiş Sözleşme 108, Madde 5 (4) (a)

[257] *A.g.e.*, Madde 7 (1).
[258] Modernize Edilmiş Sözleşme 108, Madde 5 (2); Modernize Edilmiş Sözleşme 108'e İlişkin Açıklayıcı Rapor, para. 42–45.
[259] Genel Veri Koruma Regülasyonu, Madde 8 (3).
[260] *A.g.e.*, Madde 6 (1) (a) ve 9 (2) (a).
[261] *A.g.e.*
[262] *A.g.e.*, Başlangıç hükmü 32.
[263] *A.g.e.*, Madde 4 (11); Modernize Edilmiş Sözleşme 108'e İlişkin Açıklayıcı Rapor, para. 42.
[264] Genel Veri Koruma Regülasyonu, Başlangıç hükmü 32; Modernize Edilmiş Sözleşme 108'e İlişkin Açıklayıcı Rapor, para. 42.

		AİHM, *K.H. ve Diğerleri/Slovakya*, No. 32881/04, 2009
Genel Veri Koruma Regülasyonu, Madde 5 (1) (a) ABAD, C-201/14, *Smaranda Bara ve Diğerleri/Casa Naţională de Asigurări de Sănătate ve Diğerleri*, 2015	Şeffaflık prensibi	Modernize Edilmiş Sözleşme 108, Madde 5 (4) (a) ve Madde 8 AİHM, *Haralambie/Romanya*, No. 21737/03, 2009
Genel Veri Koruma Regülasyonu, Madde 5 (1) (b)	Amaç sınırlaması prensibi	Modernize Edilmiş Sözleşme 108, Madde 5 (4) (b)
Genel Veri Koruma Regülasyonu, Madde 5 (1) (c) ABAD, Birleşik davalar C-293/12 ve C-594/12, *Digital Rights Ireland ve Kärntner Landesregierung ve Diğerleri* [GC], 2014	Veri minimizasyonu prensibi	Modernize Edilmiş Sözleşme 108, Madde 5 (4) (c)
Genel Veri Koruma Regülasyonu, Madde 5 (1) (d) ABAD, C-553/07, *College van burgemeester en wethouders van Rotterdam/M. E. E. Rijkeboer*, 2009	Veri doğruluğu prensibi	Modernize Edilmiş Sözleşme 108, Madde 5 (4) (d)
Genel Veri Koruma Regülasyonu, Madde 5 (1) (e) ABAD, Birleşik davalar C-293/12 ve C-594/12, *Digital Rights Ireland ve Kärntner*	Depolama sınırlaması prensibi	Modernize Edilmiş Sözleşme 108, Madde 5 (4) (e) AİHM, *S. ve Marper/Birleşik Krallık* [GC], Nos. 30562/04 ve 30566/04, 2008

Landesregierung ve Diğerleri [GC], 2014		
Genel Veri Koruma Regülasyonu, Madde 5 (1) (f) ve 32	Veri güvenliği (bütünlük ve gizlilik) prensibi	Modernize Edilmiş Sözleşme 108, Madde 7
Genel Veri Koruma Regülasyonu, Madde 5 (2)	Sorumlu tutulabilme prensibi	Modernize Edilmiş Sözleşme 108, Madde 10

Genel Veri Koruma Regülasyonu 5. madde, kişisel verilerin işlenmesini düzenleyen ilkeleri belirlemektedir. Bu ilkeler şunları kapsamaktadır:

• meşruluk, adillik ve şeffaflık;

• amaç sınırlaması;

• veri minimizasyonu;

• veri doğruluğu;

• depolama sınırlaması;

• bütünlük ve gizlilik.

İlkeler, tüzüğün sonraki maddelerindeki daha ayrıntılı hükümler için başlangıç noktası görevi görmektedir. İlkeler, ayrıca, Modernize Edilmiş Sözleşme 108'in 5., 7., 8. ve 10. maddelerinde de yer almaktadır. Avrupa Konseyi veya AB seviyesindeki tüm veri koruma mevzuatı bu ilkelerle uyumlu olmalıdır ve bu mevzuat yorumlarken bu ilkeler akılda tutulmalıdır. AB hukuku uyarınca, işleme ilkelerine getirilen kısıtlamalara ancak 12. ve 22. maddelerde öngörülen hak ve yükümlülüklere karşılık geldikleri ölçüde izin verilir ve bunların temel hak ve özgürlüklerin özüne saygı göstermeleri gerekir. Bu temel ilkelerden herhangi bir muafiyet ve bu temel ilkelere getirilen herhangi bir kısıtlama AB düzeyinde veya ulusal düzeyde sağlanabilir;[265] bunlar kanunlarda öngörülmeli, meşru bir amaç izlemeli ve demokratik bir toplumda gerekli ve orantılı önlemler olmalıdır.[266] Üç koşulun da yerine getirilmesi gerekmektedir.

3.1. Veri İşleme Prensiplerinin Meşruluğu, Adilliği, Şeffaflığı

Kilit Noktalar

• Meşruluk, adillik ve şeffaflık ilkeleri tüm kişisel veri işlemelerine uygulanmaktadır.

• GDPR'ye göre, meşruluk, aşağıdakilerden birini gerektirmektedir:

  • veri sahibinin rızası;

  • sözleşme yapma zorunluluğu;

  • yasal bir yükümlülük;

  • veri sahibi veya başka bir kişinin hayati menfaatlerini koruma zorunluluğu;

  • kamu yararına bir görevi yerine getirme zorunluluğu;

  • veri sahibinin menfaatleri ve hakları baskın gelmediği takdirde, veri sorumlusunun veya bir üçüncü kişinin yasal menfaatleri için gereklilik.

[265] Modernize Edilmiş Sözleşme 108, Madde 11 (1); Genel Veri Koruma Regülasyonu, Madde 23 (1).
[266] Genel Veri Koruma Regülasyonu, Madde 23 (1).

• Kişisel veri işleme adil bir şekilde yapılmalıdır.

  • İşlemin öngörülemeyen olumsuz etkileri olmamasını sağlamak için veri sahibi riskten haberdar edilmelidir.

• Kişisel veri işleme şeffaf bir şekilde yapılmalıdır.

  • Veri sorumluları, verilerini işlemeden önce, diğer ayrıntıların yanı sıra, işlemenin amacı ile veri sorumlusunun kimliği ve adresi hakkında veri sahiplerini bilgilendirmelidir.

  • İşleme faaliyetlerine ilişkin bilgiler; veri sahiplerinin ilgili kuralları, riskleri, güvenceleri ve hakları kolayca anlayabilmeleri için açık ve sade bir dilde temin edilmelidir.

  • Veri sahipleri, verilerine işlendikleri her yerde erişme hakkına sahiptir.

3.1.1. Veri İşlemenin Meşruluğu

AB ve Avrupa Konseyi veri koruma hukuku, kişisel verilerin hukuka uygun/meşru şekilde işlenmesini gerektirmektedir.[267] Meşru işleme, veri sahibinin rızasını veya veri koruma mevzuatında öngörülen başka bir meşru dayanağı gerektirmektedir.[268] GDPR'nin 6 (1) maddesi, rızaya ek olarak; bir sözleşmenin ifa edilmesi, bir kamu otoritesinin görevini yerine getirmesi, bir yasal yükümlülüğe uyulması, veri sorumlusunun veya bir üçüncü kişinin meşru menfaatleri ya da gerektiğinde veri sahibinin hayati menfaatlerinin korunması için kişisel verilerin işlenmesi halleri bakımından işlemeye ilişkin beş meşru dayanak içermektedir. Bu husus Bölüm 4.1'de daha ayrıntılı olarak ele alınacaktır.

3.1.2. Veri İşlemenin Adilliği

Meşru işlemeye ek olarak, AB ve Avrupa Konseyi veri koruma hukuku, kişisel verilerin adil bir şekilde işlenmesini gerektirmektedir.[269] Adil işleme ilkesi, öncelikle veri sorumlusu ile veri sahibi arasındaki ilişkiyi yönetmektedir.

Veri sorumluları; veri sahiplerine ve kamuoyuna verileri meşru ve şeffaf bir şekilde işleyeceklerini bildirmeli ve işleme faaliyetlerinin GDPR ile uyumlu olduğunu gösterebilmelidir. İşleme faaliyetleri gizli olarak yapılmamalı ve veri sahipleri potansiyel risklerin farkında olmalıdır. Dahası, veri sorumluları, mümkün olduğu ölçüde, özellikle de rızanın veri işleme için yasal dayanak oluşturduğu durumlarda, veri sahibinin isteklerine en uygun şekilde davranmalıdır.

Örnek: *K.H. ve Diğerleri v. Slovakya*[270] davasında başvuru sahipleri – Roman etnik kökenli kadınlar – hamilelikleri ve doğumları sırasında doğu Slovakya'daki iki hastanede tedavi edilmişlerdir. Sonrasında, başvuru sahiplerinden hiçbiri, tekrarlanan denemelerine rağmen, tekrar çocuk sahibi olamamıştır. Yerel mahkemeler, hastanelerin, başvuru sahiplerine ve

[267] Modernize Edilmiş Sözleşme 108, Madde 5 (3); Genel Veri Koruma Regülasyonu, Madde 5 (1) (a).
[268] Avrupa Birliği Temel Haklar Bildirgesi, Madde 8 (2); Genel Veri Koruma Regülasyonu, Başlangıç hükmü 40 ve Madde 6–9; Modernize Edilmiş Sözleşme 108, Madde 5 (2); Modernize Edilmiş Sözleşme 108'e İlişkin Açıklayıcı Rapor, para. 41.
[269] Genel Veri Koruma Regülasyonu, Madde 5 (1) (a); Modernize Edilmiş Sözleşme 108, Madde 5 (4) (a).
[270] AİHM, *K.H. ve Diğerleri/Slovakya*, No. 32881/04, 28 Nisan 2009.

onların temsilcilerine tıbbi kayıtlara bakmaları ve bunların el yazısı örneklerini almaları için izin vermelerine karar vermiştir; ancak sözde kötüye kullanmaları önlemek amacıyla ilgili belgelerin fotokopisinin alınması talebini reddetmiştir. Devletlerin AİHS'nin 8. maddesi kapsamındaki pozitif yükümlülükleri, veri sahiplerine kendi veri dosyalarının kopyalarının mutlaka sunulması yükümlülüğünü de içermektedir. Kişisel veri dosyalarının kopyalanmasına ilişkin düzenlemeleri belirlemek veya uygun olduğunda, bunu yapmayı reddetmek için zorlayıcı nedenler göstermek devletlerin görevidir. Başvuru sahiplerinin davasında, yerel mahkemeler, başvuru sahiplerinin tıbbi kayıtlarının kopyalarını almalarını, esas olarak ilgili bilgilerin kötüye kullanılmasını engellemek gerekçesiyle reddetmiştir. Ancak AİHM, başvuru sahiplerinin tıbbi dosyalarının tümüne erişim sahibi olmaları halinde, kendileriyle ilgili bilgileri nasıl kötüye kullanacaklarını anlayamamıştır. Ayrıca bu tür suiistimal riski, dosyaların kopyalarının başvuru sahiplerine verilmesinin engellenmesi dışında, dosyalara erişim hakkına sahip kişilerin sınırlandırılması gibi önlemlerle de önlenebilir. Devlet, başvuru sahiplerinin sağlıklarıyla ilgili bilgilere etkili bir şekilde erişmelerinin engellenmesi için yeterince zorlayıcı nedenlerin var olduğunu gösterememiştir. Mahkeme, 8. maddenin ihlal edildiğine karar vermiştir.

İnternet hizmetleriyle ilgili olarak, veri işleme sistemlerinin özellikleri, veri sahiplerinin verileri ile ilgili neler yapıldığını gerçekten anlamalarını sağlamalıdır. Her durumda, adalet ilkesi şeffaflık yükümlülüklerinin ötesine geçer ve aynı zamanda kişisel verilerin etik bir şekilde işlenmesiyle de bağlantılı olabilir.

Örnek: Bir üniversite araştırma departmanı, 50 kişinin ruh halindeki değişiklikleri analiz eden bir deney yapar. İlgili kişilerden, belirlenmiş olan bir zamanda saatlik düşüncelerini elektronik bir dosyaya kaydetmeleri talep edilmiştir. 50 kişi bu özel projeye ve verinin üniversite tarafından bu şekilde kullanımına ilişkin rızalarını vermiştir. Araştırma departmanı, elektronik olarak düşüncelerin kaydedilmesinin, başka bir ekibin koordinasyonundaki zihinsel sağlık odaklı bir başka proje için çok yararlı olacağını keşfeder. Her ne kadar üniversite, veri sorumlusu olarak, bu verileri işlemenin yasallığını sağlamak için daha fazla adım atmadan başka bir ekibin çalışması için aynı verileri amaçların uyumlu olması durumunda kullanabilirdiyse de üniversite araştırma etiği kuralları ve adil veri işleme ilkesini izleyerek veri sahiplerini bilgilendirmiş ve yeni rızalarını istemiştir.

3.1.3. Veri İşlemenin Şeffaflığı

Avrupa Birliği ve Avrupa Komisyonu veri koruma mevzuatı, kişisel veri işlemenin "veri sahibi ile ilgili şeffaf bir şekilde" yapılmasını gerektirir.[271]

Bu ilke, veri sorumlularına, veri sahiplerinin -kullanıcılar, müşteriler veya müvekkiller olabilir- verilerinin nasıl kullanıldığı hakkında bilgilendirilmesi için uygun herhangi bir önlemi alma yükümlülüğü getirmektedir.[272] Şeffaflık, veri işlemeye başlamadan önce bireye verilen bilgiyi,[273] veri işleme sırasında veri sahiplerinin kolayca erişmesi gereken bilgileri,[274] aynı zamanda kendi verilerine erişim talebini izleyen veri sahiplerine verilen bilgileri ifade

[271] Avrupa Genel Veri Koruma Regülasyonu, Md. 5 (1) (a); Moderleştirilen Sözleşme 108, Md. 5 (4) (a) ve 8.

[272] Avrupa Genel Veri Koruma Regülasyonu, Md. 12.

[273] Age., Md. 13 ve 14.

[274] Madde 29 Çalışma Grubu, İşyerinde veri işlenmesine ilişkin 2/2017 sayılı görüş, sf. 23.

edebilir.[275]

Örnek Haralambie v. Romanya Davası'nda,[276] Başvuran, gizli servis organizasyonu tarafından kendisi hakkında tutulan bilgilere ancak talep etmesinden beş yıl sonra erişebilmiştir. Avrupa İnsan Hakları Mahkemesi, kamu makamları tarafından tutulan kişisel dosyalara konu olan kişilerin, bunlara erişebilmelerinin esaslı menfaatleri olduğunu yinelemiştir. Yetkili makamların, bu tür bilgilere erişebilmeleri için etkili bir yöntem sağlama görevi vardır. AİHM, ne aktarılan dosya miktarının ne de arşiv sistemindeki eksikliklerin başvuru sahibinin dosyalarına erişim talebini sağlamada beş yıllık bir gecikmeyi haklı çıkarmadığını belirtmiştir. Yetkili makamlar, başvuru sahibine kişisel dosyalarına makul bir süre içinde ulaşabilmesi için etkili ve erişilebilir bir yöntem sunmamışlardır. Bu kapsamda Mahkeme, AİHS Madde 8'in ihlal edildiği sonucuna varmıştır.

Veri işleme operasyonları, veri sahiplerinin verilerine ne olacağını anlamalarını sağlayacak şekilde kolay erişilebilir bir şekilde açıklanmalıdır. Bu, kişisel verilerin işlenmesinin özel amacının, kişisel verilerin toplanması sırasında veri sahipleri tarafından bilinmesi gerektiği anlamına gelir.[277] Veri işlemenin şeffaflığı, açık ve sade bir dilin kullanılmasını gerektirir.[278] İlgili kişiler için, kişisel verilerinin işlenmesiyle ilgili risklerin, kuralların, güvencelerin ve hakların ne olduğu açık olmalıdır.[279]

Avrupa Komisyonu Hukuku ayrıca, belirli temel bilgilerin, veri sorumluları tarafından veri sahiplerine proaktif bir şekilde zorunlu olarak verilmesi gerektiğini belirtir. Veri sorumlusunun (veya ortak veri sorumlularının) ad ve adres bilgileri, veri işlemenin yasal dayanağı ve amaçları, işlenen veri kategorileri ve alıcılar ile hakların kullanımına ilişkin bilgiler, veri sahibine adil ve etkin bir şekilde sağlandığı sürece herhangi bir uygun formatta (bir web sitesi, kişisel cihazlardaki teknolojik araçlar vb. aracılığıyla) sunulabilir. Sunulan bilgiler kolayca erişilebilir, okunaklı, anlaşılabilir ve ilgili veri sahiplerine uyarlanmış olmalıdır (örneğin gerektiği yerde çocukların anlayabileceği bir dilde). Muhafaza süresi, veri işlemenin altında yatan nedene ilişkin bilgi veya Taraf olan veya Taraf olmayan bir alıcıya veri aktarılmasına ilişkin bilgi (söz konusu Taraf olmayanların uygun bir koruma seviyesi sağlayıp sağlamadığı veya böyle uygun bir veri koruma seviyesini garanti etmek için veri sorumlusu tarafından alınan önlemler dahil) gibi adil veri işlemenin sağlanması için gerekli olan ya da bu amaç için faydalı olabilecek herhangi bir ek bilgi de sağlanmalıdır.[280]

Erişim hakkı uyarınca,[281] bir veri sahibi veri sorumlusundan, kendi verisinin işlenip işlenmediğini ve eğer işleniyorsa hangi verilerin işlendiğini öğrenme hakkına sahiptir.[282] Ek olarak, bilgi edinme hakkı uyarınca,[283] verileri işlenen kişiler, işleme faaliyeti başlamadan önce prensip olarak diğer detayların yanı sıra işlemenin amaçları, uzunluğu ve araçları hakkında proaktif bir şekilde veri sorumluları veya veri işleyenler tarafından bilgilendirilmelidir.

Örnek: Smaranda Bara and Others/Preşidentele Casei Naţionale de Asigurări de Sănătate, Casa

[275] Avrupa Genel Veri Koruma Regülasyonu, Md. 15.
[276] AİHM, Haralambie/Romanya, No. 21737/03, 27 Kasım 2009.
[277] Avrupa Genel Veri Koruma Regülasyonu, Başlangıç Hükmü 29.
[278] *Age*.
[279] *Age*.
[280] Modernize Edilmiş Sözleşme'nin Açıklayıcı Raporu 108, para. 28-46.
[281] Avrupa Genel Veri Koruma Regülasyonu, Md. 15.
[282] Modernize Edilmiş Sözleşme 108, Md. 8 ve 9 (1) (b).
[283] Avrupa Genel Veri Koruma Regülasyonu, Md. 13 ve 14.

Naţională de Administrare Fiscală (ANAF)[284] Davası, sağlık sigortası prim borçlarının ödenmesi gerektiğine dayanarak, serbest meslek sahibi kişilerin gelirine ilişkin vergi verilerinin Ulusal Vergi İdaresi Kurumu'ndan Romanya'daki Ulusal Sağlık Sigortası Fonu'na aktarılmasına ilişkindir. Avrupa Birliği Adalet Divanı'ndan veri sorumlusunun kimliği ve ilgili verilerin aktarım amacına ilişkin bilgilendirmenin veri sahibine ilgili veriler Ulusal Sağlık Sigortası Fonu tarafından işlenmeden önce yapılması gerekip gerekmediğini belirlemesi istenmiştir. ABAD, kişisel verilerin bir Üye Devletin kamu idari organı tarafından, ikincil işleme yapan başka bir kamu idari organına aktarılması durumunda veri sahiplerine bu aktarım veya işleme hakkında bilgi verilmesi gerektiği kanısındadır.

Bazı durumlarda, veri işleme hakkında veri sahiplerini bilgilendirme yükümlülüğünün istisnaları söz konusu olabilir ve bunlar veri sahibinin haklarına ilişkin Bölüm 6.1'de daha ayrıntılı olarak ele alınacaktır.

3.2. Amaç sınırlaması prensibi

Kilit noktalar

- Veri işlenmesine başlanmadan önce, veri işlemenin amaçları belirlenmelidir.
- Avrupa Genel Veri Koruma Regülasyonu kamu yararı, bilimsel veya tarihi araştırma ve istatistiksel amaçlarla arşivlemek amacıyla bu kuralın istisnalarını öngörmüş olsa da ana amaç ile bağdaşmayan bir şekilde veri işlenemeyecektir.
- Temel olarak, amaç sınırlama ilkesi, kişisel verilerin işlenmesinin sınırı belli bir amaç için ve yalnızca ek olarak belirtilmiş ve ana amaç ile uyumlu amaçlarla gerçekleştirilmesi gerektiği anlamına gelir.

Amaç sınırlama ilkesi, Avrupa veri koruma hukukunun temel ilkelerinden biridir. Şeffaflık, öngörülebilirlik ve kullanıcı kontrolü ile güçlü bir şekilde bağlantılıdır: veri işlemenin amacı yeterince belirli ve açıksa, bireyler ne bekleyeceklerini bilir ve şeffaflık ve hukuk güvenliği gelişir. Aynı zamanda, veri işleme amacının açık bir şekilde tasvir edilmesi veri sahiplerinin veri işlemesine itiraz etme hakkı gibi haklarını etkin bir şekilde kullanmalarını sağlamak için önemlidir.[285]

İlke, kişisel verilerin işlenmesinin belirli, sınırı belli bir amaç ve yalnızca asıl amaç ile uyumlu ek amaçlar için yapılmasını gerektirir.[286] Bu nedenle, kişisel verilerin belirsiz ve/veya sınırsız amaçlarla işlenmesi hukuka aykırıdır. Kişisel verilerin belirli bir amaç olmadan, sadece gelecekte yararlı olabileceği düşüncesine dayanarak işlenmesi de hukuken geçerli olmayacaktır. Kişisel verilerin işlenmesinin meşruiyeti, açık, belirli ve meşru olması gereken işleme amacına bağlı olacaktır.

---

[284] ABAD, C-201/14, Smaranda Bara and Others/Casa Naţională de Asigurări de Sănătate and Others, 1 Kasım 2015, paras. 28–46.
[285] Madde 29 Çalışma Grubu (2013), amaç sınırlamasına ilişkin 2/2018 sayılı görüş, WP 203, 2 Nisan 2013.
[286] Avrupa Genel Veri Koruma Regülasyonu, Md. 15 (1) (b).

Verilerin işlenmesine yönelik asıl amaç ile uyumlu olmayan her yeni amaç, kendi özel hukuki dayanağına sahip olmalıdır ve verilerin başlangıçta başka bir meşru amaç için elde edilmiş ya da işlenmiş olduğuna dayanamaz. Böylece, meşru veri işleme başlangıçta belirtilen amacı ile sınırlıdır ve herhangi bir yeni veri işleme amacı ayrı bir hukuki dayanak gerektirecektir. Örneğin, kişisel verilerin yeni bir amaç için üçüncü şahıslara aktarılması dikkatli bir şekilde değerlendirilmelidir, çünkü bu aktarım muhtemelen verilerin en başta toplanmasından farklı ek bir hukuki dayanağa ihtiyaç duyacaktır.

Örnek: Bir havayolu şirketi, uçuşu doğru bir şekilde yürütmek amacıyla rezervasyon yapmak için yolcularından veri toplamaktadır. Havayolunun şu bilgilere ihtiyacı olacaktır: yolcuların koltuk numaraları; tekerlekli sandalye ihtiyaçları gibi özel fiziksel sınırlamalar; koşer veya helal yiyecek gibi özel yiyecek gereksinimleri. Eğer havayollarından Yolcu Adı Kaydı'nda yer alan bu verileri iniş havalimanındaki göçmenlik yetkililerine iletmesi talep edilirse, bu durumda ilgili veriler ilk veri toplama amacından farklı olan göçmenlik kontrolü amacıyla kullanılmış olacaktır. Bu nedenle, bu verilerin göçmenlik yetkililerine iletilmesi için yeni ve ayrı bir hukuki dayanak gerekecektir.

Belirli bir amacın kapsamı ve sınırları değerlendirilirken, Modernize Edilmiş Sözleşme 108 ve Avrupa Genel Veri Koruma Regülasyonu uyumluluk kavramına dayanmaktadır: verilerin uyumlu amaçlar için kullanılmasına başlangıçtaki hukuki dayanaktan yola çıkılarak izin verilir. Bu nedenle, ikincil veri işleme veri sahibi için beklenmeyen, uygunsuz veya sakıncalı bir şekilde yapılamaz.[287] İkincil işlemenin uyumlu olup olmadığını değerlendirmek için, veri sorumlusu aşağıdakileri göz önünde tutmalıdır (diğer hususlar ile birlikte):

- bu amaçlar ve istenilen ikincil işlemenin amaçları arasındaki herhangi bir bağlantıyı;
- kişisel verinin toplandığı durum, özellikle ilgili kişinin veri sorumlusu ile olan ilişkisi özelinde ikincil işlemeye yönelik makul beklentileri;
- kişisel verinin doğası;
- veri sahipleri için amaçlanan ikincil işlemenin sonuçları; ve
- hem asıl hem de amaçlanan ikincil işleme operasyonlarında yeterli korumaların varlığı.[288] Bu, örneğin şifreleme veya maskeleme yoluyla yapılabilir.

Örnek: Sunshine şirketi, müşteri ilişkileri yönetimi (CRM) sürecinde müşteri verilerini elde eder. Daha sonra bu verileri, üçüncü şirketlerin pazarlama kampanyalarında destek vermek için bu verileri kullanmak isteyen doğrudan pazarlama şirketi olan Moonlight şirketine iletir. Sunshine'ın başka şirketler tarafından pazarlama yapılması amacıyla veri aktarması, Sunshine şirketinin müşteri verilerini toplamaktaki ilk amacına ve CRM ile uyumlu olmayan yeni bir amaç için veri kullanımını oluşturmaktadır. Verilerin Moonlight şirketine aktarılması bu nedenle ayrı bir hukuki dayanağa dayanmalıdır.

Buna karşılık, Sunshine şirketinin kendi müşterilerine kendi ürünlerine ilişkin pazarlama

[287] Modernize Edilmiş Sözleşme Açıklayıcı Raporu 108, para. 49.
[288] Avrupa Genel Veri Koruma Regülasyonu, Başlangıç Hükmü ve Md.6 (4); Modernize Edilmiş Sözleşme Açıklayıcı Raporu 108, para. 49.

mesajları göndermesi şeklinde CRM verilerini kendi pazarlama amaçları için kullanması genellikle uyumlu bir amaç olarak kabul edilir.

Avrupa Genel Veri Koruma Regülasyonu ve Modernize Edilmiş Sözleşme 108, "kamu yararı, bilimsel veya tarihi araştırma amaçlarına veya istatistiksel amaçlara yönelik arşivleme amaçlı gerçekleştirilen ikincil işlemenin", öncül olarak ilk amaç ile uyumlu kabul edildiğini belirtmektedir.[289] Bununla birlikte, verilerin ikincil işlenmesi sırasında verilerin anonimleştirilmesi, şifrelenmesi veya maskelenmesi ve verilere erişimin kısıtlanması gibi uygun önlemler alınması zorunludur.[290] Avrupa Genel Veri Koruma Regülasyonu şunu eklemektedir; "veri sahibinin rıza gösterdiği ya da özellikle de işlemenin, demokratik bir toplumda genel kamu yararı için önemli hedeflere koruma sağlamak için gerekli ve orantılı bir tedbir teşkil eden Birlik veya Üye Devlet yasalarına ve özellikle kamu yararının önemli amaçlarına dayandığı durumlarda, veri sorumlusuna, amaçların uygunluğundan bağımsız olarak kişisel verileri ikincil işlemesine izin verilmelidir."[291] İkincil işleme taahhüt edildiğinde, veri sahibi, itiraz hakkı gibi haklarının yanı sıra amaçlardan haberdar edilmelidir.[292]

Örnek: Sunshine şirketi müşterileri hakkında Müşteri İlişkileri Yönetimi (CRM) verilerini toplamış ve saklamıştır. Bu verilerin, Sunshine şirketi tarafından müşterilerinin satın alma davranışlarının istatistiksel bir analiz etmesi için ikincil kullanılmasına istatistikler uyumlu amaç doğrultusunda ise izin verilir. Veri sahiplerinin rızası gibi ek hukuki dayanağa ihtiyaç duyulmamaktadır. Bununla birlikte, kişisel verilerin istatistiksel amaçlarla ikincil işlenmesi için, Sunshine şirketinin, veri sahiplerinin hak ve özgürlükleri için uygun koruma önlemlerini alması gerekir. Sunshine'ın uygulamak zorunda olduğu teknik ve örgütsel önlemler maskelendirmeyi içerebilir.

3.3. Veri minimizasyonu prensibi

Kilit noktalar

- Veri işleme meşru bir amacı yerine getirmek için gerekenlerle sınırlı olmalıdır.
- Kişisel verilerin işlenmesi, ancak işleme amacının başka yollarla makul bir şekilde yerine getirilemediğinde gerçekleşmelidir.
- Veri işleme, söz konusu çıkarlara, haklara ve özgürlüklere orantısız şekilde müdahale edemez.

Bu tür veriler sadece "toplandıkları ve/veya ikincil işlendikleri amaçlarla ilgili olarak yeterli, ilgili ve aşırı olmayan" şekilde işlenmelidir.[293] Veri işleme için belirlenen veri kategorileri, beyan edilen veri işleme operasyonunun ana amacının gerçekleştirilmesi için gerekli olmalıdır

[289] Avrupa Genel Veri Koruma Regülasyonu, Md. 5 (1) (b); Modernize Edilmiş Sözleşme 108, Md. 5 (4). Bu tür ulusal hükümlerin bir örneği Avusturya Veri Koruma Yasasıdır (Datenschutzgesetz), Federal Hukuk Gazetesi I No. 165/1999, para. 46.
[290] Avrupa Genel Veri Koruma Regülasyonu, Md. 6 (4); Modernize Edilmiş Sözleşme 108, Md. 5 (4) (b); Modernize Edilmiş Sözleşme Açıklayıcı Raporu 108, para. 50.
[291] Avrupa Genel Veri Koruma Regülasyonu, Başlangıç Hükmü 50.
[292] *Age*.
[293] Modernize Edilmiş Sözleşme 108, Md. 5 (4) (c); Avrupa Genel veri Koruma Regülasyonu, Md. 5 (1) (c).

ve veri sorumlusu, veri işlenmesindeki belirli amaç ile doğrudan ilgili bilgilerin veri olarak toplanmasını katı bir şekilde sınırlamalıdır.

Örnek: Dijital Haklar İrlanda davasında,[294] ABAD, yetkili kişilere örgütlü suç ve terörizm gibi ciddi suçlarla mücadele etmeleri için muhtemel olarak aktarılacak kamuya açık elektronik iletişim hizmetleri veya ağlar tarafından oluşturulan veya işlenen kişisel verilerin saklanmasına yönelik ulusal hükümlerin uyumlaştırılmasını amaçlayan Veri Saklama Direktifi'nin geçerliliğini değerlendirmiştir. Bununla birlikte, kamu yararı hedefini gerçekten yerine getiren bir amaç olarak görülmesine rağmen, Direktif'in "ciddi suçlara karşı mücadele hedefi ışığında herhangi bir farklılaşma, sınırlama ya da istisna olmaksızın, tüm bireyleri ve tüm trafik verilerinin yanı sıra tüm elektronik iletişim araçlarını" kapsaması şeklindeki genelleştirilmiş yönteminin problemli olduğu kabul edildi.[295]

Ayrıca, özel gizlilik arttırıcı teknolojiden yararlanarak, kişisel verilerin kullanılmasından kaçınmak veya verilerin bir veri sahibine (örneğin maskelendirme yoluyla) bağlanmasını azaltmak için gizlilik dostu bir çözümle sonuçlanan önlemler kullanmak mümkündür. Bu özellikle daha kapsamlı işleme sistemlerinde uygundur.

Örnek: Bir belediye meclisi, şehrin toplu taşıma sisteminin düzenli kullanıcılarına belirli bir ücret karşılığında bir çip kartı sunmaktadır. Kart, kullanıcının ismini, kartın yüzeyinde yazılı biçimde ve ayrıca çipte elektronik biçimde taşımaktadır. Bir otobüs ya da tramvay kullanıldığında, çip kart, örneğin otobüs ve tramvaylara takılan okuma cihazlarına okutularak geçilmelidir. Cihaz tarafından okunan veriler, seyahat kartını alan kişilerin isimlerini içeren bir veri tabanında elektronik olarak kontrol edilir.

Bir kişinin taşıma olanaklarını kullanma izni olup olmadığı, kart çipindeki kişisel verilerin bir veri tabanı ile karşılaştırılmadan kontrol edilebileceği için bu sistem veri minimizasyonu prensibine uymamaktadır. Örneğin, kartın çipi okuma cihazının önüne getirildiğinde, kartın geçerli olup olmadığını teyit edecek barkod gibi özel bir elektronik görüntünün kullanılması yeterli olacaktır. Böyle bir sistem hangi taşıma aracını kimin hangi zamanda kullandığını kaydetmeyecektir. Bu prensip veri toplamanın en aza indirilmesi yükümlülüğü ile sonuçlandığından, minimizasyon prensibi açısından en uygun çözüm olacaktır.

Modernize Edilmiş Sözleşme 108'in 5. Maddesi (1), izlenen meşru amaç hususunda kişisel verilerin işlenmesi için orantılılık şartını öngörmektedir. Veri işlemenin tüm aşamalarında ilişkili bütün menfaatler arasında adil bir denge olmalıdır. Bu, "yeterli ve ilgili ancak temel haklara ve söz konusu özgürlüklere orantısız bir müdahaleye yol açacak kişisel verilerin aşırı olarak kabul edilmesi gerektiği" anlamına gelir.[296]

3.4. Veri doğruluğu prensibi

Kilit noktalar

[294] ABAD, C-293/12 ve C-594/12 sayılı birlikte görülen davalar, Digital Rights Ireland Ltd/Haberleşme Bakanlığı, Denizcilik ve Doğal Kaynaklar ve Diğerleri ve Kärntner Landesregierung ve Diğerleri [GC], 8 Nisan 2014.
[295] *Age*., paras. 44 ve 57.
[296] Modernize Edilmiş Sözleşme 108 Açıklayıcı Raporu, para. 52; Avrupa Genel Veri Koruma Regülasyonu, Md. 5 (1) (c).

- Veri doğruluğu prensibi, tüm veri işleme faaliyetlerinde veri sorumlusu tarafından uygulanmalıdır.

- Yanlış veriler gecikmeksizin silinmeli veya imha edilmelidir.

- Doğruluğun sağlanabilmesi için veriler düzenli olarak kontrol edilmeli ve güncel tutulmalıdır.

Elinde kişisel bilgiler bulunduran bir veri sorumlusu, verilerin doğru ve güncel olduğundan emin olmak için gerekli adımları atmadan bu bilgileri kullanmayacaktır.[297]

Veri doğruluğunu sağlama yükümlülüğü, veri işleme amacı kapsamında görülmelidir.

Örnek: Rijkeboer davasında,[298] ABAD Hollandalı bir vatandaşın Amsterdam'ın yerel yönetimden geçen iki yılda kendisine ait yetkili yerel makamda bulunan kayıtların paylaşıldığı kişilerin kimliklerine ilişkin ve bununla beraber aktarılan verilerin içeriğine dair bilgi alınmasına ilişkin talebini değerlendirmiştir. ABAD, "gizlilik hakkının, veri sahibinin, kişisel verilerinin doğru ve yasal bir şekilde işlendiği, özellikle de kendisiyle ilgili temel verilerin doğru olduğu ve bunların yetkili alıcılara aktarıldığı anlamına geldiğini" belirtmiştir. ABAD, daha sonra, verilerin doğru olup olmadığını kontrol edebilmek için veri sahiplerinin kişisel verilerine erişim hakkına sahip olması gerektiğini belirten Veri Koruma Direktifinin giriş kısmına atıfta bulunmuştur.[299]

Saklanan verilerin güncellenmesinin hukuken yasak olduğu durumlar da olabilir, çünkü verilerin saklanma amacı, esasen olayları tarihsel bir "anlık fotoğraf" olarak belgelemek içindir.

Örnek: Bir operasyonun tıbbi kaydı, kayıtta belirtilen bulguların daha sonra yanlış olduğu ortaya çıkmış olsa bile, değiştirilmemelidir bir başka deyişle "güncellenmemelidir". Bu gibi durumlarda, sonraki bir aşamada yapılan katkı olarak açıkça işaretlendikleri sürece sadece kayıttaki açıklamalara ilaveler yapılabilir.

Öte yandan, verilerin yanlış kalması durumunda, veri sahibinin uğrayabileceği olası zararlar nedeniyle, verilerin güncellenmesinin ve doğruluğunun düzenli olarak kontrol edilmesinin mutlak olarak zorunlu olduğu durumlar vardır.

Örnek: Eğer bir kişi bir bankacılık kurumuyla bir kredi sözleşmesi yapmak isterse, banka genellikle müstakbel müşterinin kredibilitesini kontrol edecektir. Bu amaçla, özel kişilerin kredi geçmişine ilişkin verileri içeren özel veri tabanları vardır. Böyle bir veri tabanının kişi hakkında yanlış veya eski veriler taşıması durumunda bu kişi olumsuz etkilere maruz kalabilir. Bu nedenle, veri doğruluğu prensibine uymak için veri tabanlarının veri sorumlularının özel çaba sarf etmesi gereklidir.

[297] Avrupa Genel Veri Koruma Regülasyonu, Md. 5 (1) (d); Modernize Edilmiş Sözleşme 108, Md. 5 (4) (d).
[298] ABAD, C-553/07, College van burgemeester en wethouders van Rotterdam/M. E. E. Rijkeboer, 7 Mayıs 2009.
[299] Geçmiş Başlangıç Hükmü 41, 95/46/EC sayılı Direktif'in girişi.

3.5. Veri depolaması sınırlaması prensibi

Kilit noktalar

- Veri depolaması sınırlaması prensibi, kişisel verilerin, toplandıkları amaçlara göre artık ihtiyaç duyulmadığında en kısa zamanda silinmesi veya anonim hale getirilmesi gerektiği anlamına gelir.

GDPR Madde 5 (1) (e) ve aynı şekilde Modernize Edilmiş Sözleşme 108'in 5 (4) (e) maddesi kişisel verilerin, "gerekli olandan daha uzun olmamak üzere ve verilerin işlendikleri amaca göre veri sahiplerinin kimliğini saptayacak biçimde tutulmasını" gerektirir. Bu nedenle, bu amaçlar yerine getirildiğinde, veriler silinmeli veya anonimleştirilmelidir. Bu amaçla, verilerin gerekenden daha uzun süre tutulmaması adına "veri sorumlusu tarafından silme veya periyodik inceleme için zaman sınırları oluşturulmalıdır".[300]

S. ve Marper Davasında, AİHM Avrupa Konseyinin ilgili kurumlarının temel ilkelerinin ve diğer Akit Tarafların yasa ve uygulamalarının, özellikle polislik sektöründe, veri saklamanın, toplama amacıyla ve zaman sınırlamasıyla orantılı olmasını gerektirdiği sonucuna varmıştır.[301]

Örnek: S. ve Marper Davasında,[302] AİHM, iki başvuru sahibinin parmak izlerinin, hücre örneklerinin ve DNA profillerinin belirsiz bir şekilde saklanmasının, her iki başvurana yönelik cezai işlemlerin sırasıyla beraat ve yer olmadığına ilişkin karar ile sonlandırıldığını dikkate alarak demokratik bir toplum düzeninde orantısız ve gereksiz olduğuna karar vermiştir.

Kişisel verilerin saklanmasına ilişkin süre sınırlaması, sadece veri sahiplerinin kimliklerinin belirlenmesine izin verecek biçimde tutulan verilere uygulanır. Bu nedenle, artık ihtiyaç duyulmayan verilerin hukuka uygun bir biçimde saklanması, verilerin anonimleştirilmesi ile sağlanabilir.

Kamu yararı, bilimsel veya tarihi amaçlarla veya istatistiki kullanım için arşivlenen verilerin yalnızca bu amaçlarla kullanılması sağlandığında, bu veriler daha uzun süre saklanabilir.[303] Veri sahibinin hak ve özgürlüklerini korumak adına, halihazırda devam eden veri saklama ve kullanma faaliyetlerine ilişkin uygun teknik ve organizasyonel önlemler uygulanmalıdır.

Modernize Edilmiş Sözleşme 108 ayrıca, kanunlarda öngörülmesi şartıyla, temel hak ve özgürlüklerin özüne saygı göstermesi ve sınırlı sayıda meşru amaç için gerekli ve orantılı olması şartıyla, veri depolaması sınırlaması ilkesinin istisnalarına da izin vermektedir.[304] Diğerlerinin yanı sıra, bunlar, ulusal güvenliği korumayı, cezai suçları soruşturmayı ve kovuşturmayı, ceza vermeyi, veri sahibini korumayı ve başkalarının haklarını ve temel özgürlüklerini korumayı içermektedir.

---

[300] Avrupa Genel Veri Koruma Regülasyonu, Başlangıç Hükmü 39.
[301] AİHM, S. ve Marper/Birleşik Krallık [GC], No. 30562/04 ve 30566/04, 4 Aralık 2008; ayrıca bakınız, örneğin: AİHM, M.M./Birleşik Krallık, No. 24029/07, 13 Kasım 2012.
[302] AİHM, S. ve Marper/Birleşik Krallık [GC], No. 30562/04 ve 30566/04, 4 Aralık 2008.
[303] Avrupa Genel Veri Koruma Regülasyonu, Md. 5 (1) (e); Modernize Edilmiş Sözleşme 108, Md. 5 (4) (b) ve 11(2).
[304] Modernize Edilmiş Sözleşme 108, Md. 11.1; Modernize Edilmiş Sözleşme 108 Açıklayıcı Raporu, para. 91-98.

Örnek: Dijital Haklar İrlanda Davası'nda,[305] ABAD, organize suç ve terör gibi ciddi suçlarla mücadele için kamuya açık elektronik iletişim hizmetleri veya ağlar tarafından üretilen veya işlenen kişisel verilerin saklanmasına ilişkin ulusal hükümleri uyumlu hale getirmeyi amaçlayan Veri Saklama Direktifi'nin geçerliliğini değerlendirmiştir. Veri Saklama Direktifi, "ilgili kişilere göre veya izlenen hedefin amaçları için olası yararları temelinde, bu Direktif'in 5. Maddesinde belirtilen veri kategorileri arasında herhangi bir ayrım yapılmaksızın, en az altı aylık" bir veri saklama süresi öngörmüştür.[306] ABAD ayrıca, en az altı ay ile en fazla 24 ay arasında değişebilen kesin veri saklama süresinin kesin olarak gerektiği kadarıyla sınırlı olmasını sağlamak için bu sürenin belirlenmesi gerektiği temelinde Veri Saklama Direktifi'ndeki nesnel kriterlerin bulunmadığı hususunu gündeme getirmiştir.[307]

3.6. Veri güvenliği prensibi

Kilit noktalar

- Kişisel verilerin güvenliği ve gizliliği, veri sahibi için olumsuz etkileri önlemenin anahtarıdır.
- Güvenlik önlemleri teknik ve/veya organizasyonel nitelikte olabilir.
- Maskeleme, kişisel verileri koruyabilecek bir işlemdir.
- Güvenlik önlemlerinin uygunluğu duruma göre belirlenmeli ve düzenli olarak gözden geçirilmelidir.

Veri güvenliği ilkesi, verilerin yanlışlıkla, yetkisiz veya yasadışı erişim, kullanım, değişiklik, açıklama, kayıp, imha veya zararlara karşı korunması için kişisel verilerin işlenmesi sırasında uygun teknik veya organizasyonel önlemlerin uygulanmasını gerektirir.[308] GDPR, veri sorumlusu ve veri işleyenlerin bu önlemleri uygularken "gerçek kişilerin hak ve özgürlükleri için değişen olasılık ve zorluk riskinin yanı sıra mevcut durumu, uygulama maliyetlerini ve veri işlemenin doğası, kapsamı, içeriği ve amacını" dikkate alması gerektiğini belirtmektedir.[309] Her bir olayın özel şartlarına bağlı olarak, uygun teknik ve organizasyonel önlemler, örneğin kişisel verilerin maskelenmesi ve şifrelenmesini ve/veya veri işlemenin güvenli olmasını sağlamak adına önlemlerin etkinliğinin düzenli olarak test edilmesini ve değerlendirilmesini içerebilir.[310]

Bölüm 2.1.1'de açıklandığı gibi, verinin maskelenmesi, veri sahibinin tanımlanmasını mümkün kılan kişisel verinin niteliklerinin, maske ile değiştirilmesi ve bu niteliklerin teknik veya organizasyonel önlemler altında ayrı tutulması anlamına gelir. Maskeleme işlemi, kişiyi tanımlamayan tüm bağlantılarının kopuk olduğu anonimleştirme süreci ile karıştırılmamalıdır.

---

[305] ABAD, C-293/12 ve C-594/12 sayılı birlikte görülen davalar, Digital Rights Ireland Ltd/Haberleşme Bakanlığı, Denizcilik ve Doğal Kaynaklar ve Diğerleri ve Kärntner Landesregierung ve Diğerleri [GC], 8 Nisan 2014.
[306] *Age*., para.63.
[307] *Age*., para.64.
[308] Avrupa Genel Veri Koruma Regülasyonu, Başlangıç Hükmü 39 ve Md.5 (1) (f); Modernize Edilmiş Sözleşme 108, M.7.
[309] Avrupa Genel Veri Koruma Regülasyonu, Md. 32 (1).
[310] *Age*.

Örnek: "Charles Spencer, 3 Nisan 1967 doğumlu, iki erkek ve iki kız olmak üzere dört çocuktan oluşan bir ailesinin babasıdır" cümlesi, aşağıda yer alan örneklerdeki gibi maskelenebilir: "C.S.1967 iki erkek ve iki kız olmak üzere dört çocuktan oluşan bir ailesinin babasıdır"; veya "324 iki erkek ve iki kız olmak üzere dört çocuktan oluşan bir ailesinin babasıdır"; veya "YESz3201 iki erkek ve iki kız olmak üzere dört çocuktan oluşan bir ailesinin babasıdır".

Maskelenmiş veriye erişen kullanıcılar "324" veya "YESz3201" ifadelerinden "3 Nisan 1967 doğumlu, Charles Spencer"ın kimliğini tespit etme yeteneğine genellikle sahip olmayacaktır. Bu nedenle bu tür verilerin kötüye kullanımdan korunma olasılığı daha yüksektir.

Ancak birinci örnek daha az güvenlidir. İlk cümle olan "C.S.1967 iki erkek ve iki kız olmak üzere dört çocuktan oluşan bir ailesinin babasıdır", Charles Spencer'ın yaşadığı küçük kasabada kullanılıyorsa, Bay Spencer kolayca tanınabilir. Maskeleme yöntemi, veri korumanın etkinliğini etkileyebilir.

Şifreli veya ayrı tutulan niteliklere sahip kişisel veriler, kişisel kimlikleri gizli tutma bağlamında kullanılır. Bu özellikle, veri sorumlularının, veri sahiplerinin gerçek kimlikleri gerekmeden veya bunlara ihtiyaç duymaksızın aynı veri sahipleriyle ilgilendiklerine emin olmaları gerektiği durumlarda faydalıdır. Bu, örneğin bir araştırmacının, kimliği yalnızca tedavi gördükleri hastane tarafından bilinen hastaların maskelenmiş vaka çalışmalarını elde ettiği ve hastalığın seyrini araştırdığı durumdur. Maskeleme, gizlilik arttırıcı teknoloji kapsamında güçlü bir bağdır. Tasarımdan itibaren gizliliği uygularken önemli bir unsur olarak işlev görebilir. Bu, veri işleme sistemlerinin özünde veri korumasına sahip olduğu anlamına gelmektedir.

Tasarımdan itibaren gizliliği düzenleyen GDPR'nin 25. maddesi açıkça maskelemeyi, veri sorumlularının veri koruma prensiplerini yerine getirmek ve gerekli önlemleri almak için uygulamaları gereken uygun teknik ve organizasyonel önlemin bir örneği olarak göstermektedir. Bunu yaparken, veri sorumluları tüzüğün gerekliliklerini yerine getirecek ve kişisel verileri işlerken veri sahiplerinin haklarını koruyacaktır.

Onaylı bir davranış kuralına veya onaylı bir sertifika mekanizmasına uymak, veri işleme gereksiniminin güvenliğine uygunluğun gösterilmesine yardımcı olabilir.[311] Avrupa Konseyi, Yolcu Adı Kayıtlarının işlenmesinin Veri koruma üzerindeki etkileri hakkındaki Görüşünde, yolcu adı kayıt sistemlerinde kişisel verilerin korunması için uygun güvenlik önlemleri hakkında başka örnekler sunmaktadır. Bunlar, verilerin güvenli bir fiziksel ortamda tutulması, katmanlı giriş yoluyla erişim kontrolünün sınırlandırılması ve güçlü şifreleme ile veri iletişiminin korunmasını içermektedir.[312]

Örnek: Sosyal ağ siteleri ve e-posta sağlayıcıları, iki aşamalı kimlik doğrulamanın tanıtımı ile, kullanıcılarına sağladıkları hizmetlerde ekstra bir veri güvenliği katmanı ekleme imkanını sağlamaktadır. Kullanıcıların kişisel hesaplarına girebilmeleri için kişisel şifre girmeye ek olarak, ikinci bir oturum açma işlemini tamamlaması gerekmektedir. İkincisi, örneğin kişisel hesaba bağlı cep telefonuna gönderilen bir güvenlik kodunun girilmesi olabilir. Böylece, iki aşamalı doğrulama, hackleme yoluyla kişisel hesaplara yetkisiz erişime karşı kişisel bilgilerin daha iyi korunmasını sağlar.

[311] *Age*. Md. 32 (3).
[312] Avrupa Konseyi, Sözleşme 108 Komitesi, Yolcu Adı Kayıtlarının işlenmesinin Veri koruma üzerindeki etkileri hakkında Görüş, T-PD(2016)18rev, 19 Ağustos 2016, sf. 9.

Modernize Edilmiş Sözleşme 108 Açıklayıcı Raporu, profesyonel gizlilik yükümlülüğünün uygulanması gibi uygun koruma önlemlerine veya veri şifrelemesi gibi nitelikli teknik güvenlik önlemlerinin kabul edilmesine ek örnekler sunmaktadır.[313] Belirli güvenlik önlemlerini uygulamaya koyarken, veri sorumlusu -veya uygun olduğu durumlarda veri işleyen- işlenen kişisel verilerin niteliği ve hacmi, veri sahipleri için olası olumsuz sonuçları ve verilere sınırlı erişim ihtiyacı gibi birkaç unsuru dikkate almalıdır.[314] Uygun güvenlik önlemleri uygulanırken veri güvenliği yöntemleri ve veri işleme tekniklerinin mevcut durumu dikkate alınmalıdır. Bu tür önlemlerin maliyeti, potansiyel risklerin ciddiyeti ve olasılığı ile orantılı olmalıdır. Güvenlik önlemlerinin gerektiğinde güncellenebilmeleri için düzenli olarak gözden geçirilmesi gerekmektedir.[315]

Bir kişisel veri ihlalinin yaşandığı durumlarda, hem Modernize Edilmiş Sözleşme 108 hem de GDPR, veri sorumlusunun, ihlali denetleyen yetkili otoriteye, bireylerin hakları ve özgürlüklerine ilişkin riskleri gecikmeksizin bildirmesini gerektirmektedir.[316] Veri sahipleri ile benzer bir iletişim yükümlülüğü, kişisel veri ihlallerinin bu kişilerin hak ve özgürlükleri için yüksek bir risk oluşturması muhtemel olduğunda mevcuttur.[317] Bu tür ihlallerin veri sahiplerine iletilmesi açık ve net bir dilde olmalıdır.[318] Veri işleyenin kişisel veri ihlalini fark etmesi halinde, veri sorumlusuna derhal bildirimde bulunulmalıdır.[319] Bazı durumlarda, bildirim yükümlülüğünün istisnaları geçerli olabilir. Örneğin, veri sorumlusu, "kişisel veri ihlalinin, gerçek kişilerin hak ve özgürlükleri için bir risk oluşturması muhtemel olmadığında" denetleme otoritesini bilgilendirmek zorunda değildir.[320] Ayrıca, uygulanan güvenlik önlemleri verileri yetkili olmayanlar için anlaşılmaz hale getirdiğinde veya sonraki önlemlerin yüksek riskin artık gerçekleşmemesini sağladığından emin olduğunda, veri sahibini bilgilendirmek de gerekli değildir.[321] Veri sahiplerine kişisel bir ihlalin iletilmesi, veri sorumlusu adına orantısız çaba gerektiriyorsa, kamu iletişimi veya benzeri bir önlem, "veri sahiplerinin eşit derecede etkili bir şekilde bilgilendirilmesini" sağlayabilir.[322]

3.7. Sorumlu Tutulabilme Prensibi

Kilit noktalar

- Sorumlu tutulabilme, veri sorumlularının ve veri işleyenlerin, veri işleme faaliyetlerinde veri korumasını kurmak ve korumak için önlemleri aktif ve sürekli olarak uygulamalarını gerektirir.
- Veri sorumluları ve veri işleyenler, veri işleme faaliyetlerinin veri koruma yasasına ve ilgili yükümlülüklerine uyumlu olmasından sorumludur.

[313] Modernize Edilmiş Sözleşme 108 Açıklayıcı Raporu, para. 56.
[314] *Age*., para. 62.
[315] *Age*., para. 63.
[316] Modernize Edilmiş Sözleşme 108, Md. 7 (2); Avrupa Genel Veri Koruma Regülasyonu, Md. 33 (1).
[317] Modernize Edilmiş Sözleşme 108, Md. 7 (2); Avrupa Genel Veri Koruma Regülasyonu, Md. 34 (1).
[318] Avrupa Genel Veri Koruma Regülasyonu, Md. 34 (2).
[319] *Age*., Md. 33 (1).
[320] *Age*., Md. 32 (1).
[321] *Age*., Md. 34 (3) (a) ve (b).
[322] *Age*., Md. 34 (3) (c).

- Veri sorumluları, veri sahiplerine, genel kamu ve denetleme otoritelerine veri koruma hükümlerine uygunluğu her zaman kanıtlayabilmelidir. Veri işleyenler ayrıca sorumluluk tutulabilme ile bağlantılı bazı yükümlülüklere de sıkı bir şekilde uymak zorundadır (veri işleme faaliyetlerinin kaydını tutmak ve bir Veri Koruma Görevlisi atamak gibi).

GDPR ve Modernize Edilmiş Sözleşme 108, veri sorumlusunun bu bölümde açıklanan kişisel veri işleme ilkelerine uymakla sorumlu olduğunu ve bunlara uygun olduğunu kanıtlayabilmesi gerektiğini belirtmiştir.[323] Bu amaçla, veri sorumlusu uygun teknik ve organizasyonel önlemleri almalıdır.[324] GDPR Madde 5 (2)'de yer alan sorumlu tutulabilme prensibinin yalnızca veri sorumlularına yönelik olmasına rağmen, veri işleyenlerin ayrıca, çeşitli yükümlülüklere uymaları gerektiği ve sorumlu tutulabilme ile yakından bağlantılı olmaları koşuluyla sorumlu olmaları beklenmektedir.

AB ve Avrupa Konseyi veri koruma yasaları ayrıca, 3.1 ila 3.6 arasındaki Bölümlerde açıklanan veri koruma ilkelerine uyulmasından veri sorumlusunun sorumlu olduğunu ve bunu sağlamasının gerektiğini belirtmektedir.[325] Madde 29 Çalışma Grubu, "prosedürlerin ve mekanizmaların türünün, veri işleme ve verilerin niteliği tarafından temsil edilen risklere göre değişebileceğini" belirtmektedir.[326]

Veri Sorumluları, aşağıda yazılı olanlar da dahil olmak üzere çeşitli şekillerde bu gereksinimlere uyumu kolaylaştırabilir:

- veri işleme faaliyetlerini kaydederek ve talep etmesi halinde bunları denetim otoritesine sunarak;[327]
- belirli durumlarda, kişisel verilerin korunmasına ilişkin tüm konulara dahil olan bir veri koruma görevlisi atayarak;[328]
- gerçek kişilerin hak ve özgürlüklerine muhtemelen yüksek risk oluşturacak veri işleme türleri için veri koruma etki değerlendirmeleri yaparak;[329]
- başlangıçtan itibaren ve tasarımdan itibaren veri korumasını sağlayarak;[330]
- veri sahiplerinin haklarının kullanılmasına yönelik usul ve prosedürleri uygulayarak;[331]
- onaylı davranış kurallarına veya sertifika mekanizmalarına bağlı kalarak.[332]

[323] *Age*., Md. 5 (2): Modernize Edilmiş Sözleşme 108, Md. 10 (1).
[324] Avrupa Genel Veri Koruma Regülasyonu, Md. 24.
[325] *Age*., Md. 5 (2); Modernize Edilmiş Sözleşme 108, Md. 10 (1).
[326] Madde 29 Çalışma Grubu, Sorumlu tutulabilme hakkındaki 3/2010 sayılı Görüş, WP 173, Brüksel, 13 Temmuz 2010, para. 12.
[327] Avrupa Genel Veri Koruma Regülasyonu, Md. 30.
[328] *Age*., Md. 37-39.
[329] *Age*., Md. 35; Modernize Edilmiş Sözleşme 108, Md. 10 (2).
[330] Avrupa Genel Veri Koruma Regülasyonu, Md. 25; Modernize Edilmiş Sözleşme 108, Md. 10 (2) ve (3).
[331] *Age*., Md. 12 ve Md. 24.
[332] *Age*., Md. 40 ve Md. 42.

GDPR Madde 5 (2) sorumlu tutulabilme ilkesi özel olarak veri işleyenlere yönelik olmamakla birlikte, veri işleme faaliyetlerinin kaydını tutmak ve Veri Koruma Görevlisi atamasını gerektiren veri işleme faaliyetlerine bu kişileri atamak gibi veri işleyenler için yükümlülükler de içeren sorumlu tutulabilme ile bağlantılı hükümler vardır.[333] Veri işleyenler ayrıca, verilerin güvenliğini sağlamak için gerekli tüm önlemlerin uygulanmasını sağlamalıdır.[334] Veri sorumlusu ile veri işleyen arasında yasal olarak bağlayıcı olan sözleşme, veri işleyenin, veri koruma etki değerlendirmesi yaparken veya herhangi bir kişisel veri ihlalini veri sorumlusuna bunu fark eder etmez bildirmek gibi bazı uyumluluk şartlarında veri sorumlusuna yardımcı olacağını düzenlemedir.[335]

Ekonomik Kalkınma ve İşbirliği Örgütü (OECD), 2013 yılında veri sorumlularının veri korumayı pratikte işler hale getirmede önemli bir rolü olduğunu vurgulayan gizlilik esaslarını kabul etmiştir. Esaslar, "yukarıda belirtilen [maddi] ilkelere etki eden önlemlere uymada bir veri sorumlusunun sorumlu tutulması gerektiği" etkisinde sorumlu tutulabilme prensibini içermektedir.[336]

Örnek: 2002/58/EC sayılı Direktif'te 2009 yılında yapılan değişiklik[337] sorumlu tutulabilme prensibini vurgulayan yasal bir örnektir. Değiştirilmiş haliyle 4. maddeye göre, direktif "kişisel verilerin işlenmesi ile ilgili bir güvenlik politikasının uygulanmasını sağlama" yükümlülüğü getirmektedir. Dolayısıyla, bu direktifin güvenlik hükümleri söz konusu olduğunda, yasa koyucu, bir güvenlik politikasına sahip olma ve uygulama için açık bir zorunluluk getirmenin gerekli olduğuna karar vermiştir.

Madde 29 Çalışma Grubu'nun görüşüne göre,[338] sorumlu tutulabilme prensibinin özü, veri sorumlusunun aşağıda yazılı borçlarıdır:

- -normal şartlar altında- veri işleme faaliyetleri kapsamında veri koruma kurallarına uyulduğunu garanti edecek önlemlerin alınması; ve

- veri sahiplerine ve denetim otoritelerine veri koruma kurallarına uyumu sağlamak için alınmış önlemleri gösteren belgeleri hazır bulundurmak.

Bu nedenle sorumlu tutulabilme prensibi, veri sorumlularının aktif olarak uyum göstermesini ve sadece veri sahiplerinin veya denetleyici otoritelerin eksikliklere işaret etmesini beklememesini gerektirmektedir.

4. Avrupa Veri Koruma Hukuku'nun Kuralları

[333] *Age*., Md. 5 (2), 30 ve 37.
[334] *Age*., Md. 28 (3) c.
[335] *Age*., Md. 28 (3) d.
[336] OECD (2013), Kişisel Verilerin Güvenliğinin Korunması ve sınırlar arası akışının yönetimi hakkında Kurallar, Md. 14.
[337] Elektronik iletişim ağları ve hizmetleriyle ilgili evrensel hizmet ve kullanıcı haklarına ilişkin 2002/22/EC sayılı Direktif'te değişiklik yapan 2009/136/EC sayılı ve 25 Kasım 2009 tarihli Avrupa Parlamentosu ve Konseyi Direktifi; elektronik haberleşme sektöründe kişisel verilerin işlenmesi ve gizliliğin korunmasına ilişkin 2002/58/EC sayılı Direktif; Tüketicinin korunmasına ilişkin yasaların uygulanmasından sorumlu ulusal makamlar arasındaki işbirliğine ilişkin 2006/2004 (EC) sayılı Tüzük, OJ 2009 L 337, sf. 11.
[338] Madde 29 Çalışma Grubu, sorumlu tutulabilme prensibi hakkında 3/2010 sayılı Görüş, WP 173, Brüksel, 13 Temmuz 2010.

Avrupa Birliği	Ele alınan konular	Avrupa Konseyi
Verilerin hukuka aykırı işlenmesine ilişkin kurallar		
Avrupa Genel Veri Koruma Regülasyonu, Madde 6 (1) (a) ABAD, C-543/09, *Deutsche Telekom AG/Bundesrepublik Deutschland*, 2011 ABAD, C-536/15, *Tele2 (Hollanda) BV ve Others/Autoriteit Consument en Markt (AMC)*, 2017	Rıza	Profilleme Önerisi, Madde 3.4 (b) ve 3.6 Modernize Edilmiş Sözleşme 108, Madde 5 (2)
Avrupa Genel Veri Koruma Regülasyonu, Madde 6 (1) (b)	Sözleşme (öncesi) ilişkisi	Profilleme Önerisi, Madde 3.4 (b)
Avrupa Genel Veri Koruma Regülasyonu, Madde 6 (1) (c)	Veri sorumlusunun yasal görevleri	Profilleme Önerisi, Madde 3.4 (a)
Avrupa Genel Veri Koruma Regülasyonu, Madde 6 (1) (d)	Veri sahibinin önemli menfaatleri	Profilleme Önerisi, Madde 3.4 (b)
Avrupa Genel Veri Koruma Regülasyonu, Madde 6 (1) (e) ABAD, C-524/06, *Huber./Bundesrepublik Deutschland* [GC], 2008	Kamu yararı ve resmi makamın uygulaması	Profilleme Önerisi, Madde 3.4 (b)

Prensipler mutlaka genel niteliktedir. Somut durumlara uygulanmaları, belli bir yorum marjı ve yöntem seçimi bırakmaktadır. Avrupa Konseyi yasası uyarınca, bu yorum marjının Modernize Edilmiş Sözleşme 108'in taraflarının yerel hukuklarında netleştirilmesi ilgili taraflara bırakılmıştır. AB Hukukundaki durum farklıdır: iç pazarda veri korumanın kurulması için, Üye Devletlerin ulusal yasalarının veri koruma seviyesini uyumlu hale getirmek için AB düzeyinde daha ayrıntılı kurallara sahip olmak gerekli görülmüştür. Avrupa Genel Veri Koruma

Regülasyonu, 5. Maddede belirtilen ve ulusal hukuk düzeninde doğrudan uygulanabilecek prensipler çerçevesinde ayrıntılı bir kurallar katmanı oluşturur. Avrupa düzeyindeki ayrıntılı veri koruma kurallarına ilişkin aşağıda yer alan açıklamalar nedeniyle, ağırlıklı olarak AB yasalarını ele alınmaktadır.

4.1. Meşru veri işleme kuralları

Kilit noktalar

- Kişisel veriler, aşağıdaki kriterlerden birini karşıladığında yasal olarak işlenebilir:
    - veri işleme, veri sahibinin rızasına dayanıyorsa;
    - sözleşmeye dayalı bir ilişki kişisel verilerin işlenmesini gerektiriyorsa;
    - veri işleme, veri sorumlusunun yasal bir yükümlülüğünü yerine getirmesi için gerekliyse;
    - veri sahiplerinin veya başka bir kişinin hayati çıkarları, verilerinin işlenmesini gerektiriyorsa;
    - kamu yararına bir görevin yerine getirilmesi için veri işlenmesine ihtiyaç duyuluyorsa;
    - yalnızca veri sahiplerinin menfaatleri ya da temel hakları zarar verilmediği müddetçe, veri işlemenin nedeni veri sorumlularının ya da üçüncü tarafların meşru menfaatleri ise.
- Hassas kişisel verilerin yasal olarak işlenmesi özel, daha katı bir rejime tabidir.

4.1.1. Veri işlemenin kanuni gerekçeleri

"Prensipler" başlıklı Avrupa Genel Veri Koruma Regülasyonu'nun 2. Bölümü, tüm kişisel veri işlemelerinin öncelikle, GDPR'nin 5. Maddesinde belirtilen veri özellikleri ile ilgili ilkelere uymasını zorunlu kılar. Prensiplerden biri, kişisel verilerin "yasal, adil ve şeffaf bir şekilde işlenmesi" gerektiğidir. İkinci olarak, verilerin yasal olarak işlenmesi için, hassas olmayan kişisel veriler için 6.[339] maddede ve özel nitelikli veri kategorileri (veya hassas veriler) için 9. maddede belirtilen hukuki dayanaklara uygun olması gerekir. Benzer şekilde, "kişisel verilerin korunmasına ilişkin temel prensipleri" ortaya koyan Modernize Edilmiş Sözleşme 108'in II. Bölüm'ü veri işlemenin yasal olması için, "izlenen meşru amaç ile orantılı" olması gerekliliğini belirtir.

Bir veri sorumlusunun bir kişisel veri işleme işlemini başlatmak için dayandığı hukuki dayanağa bakmaksızın, veri sorumlusu ayrıca, genel veri koruma kanunu rejiminde öngörülen

[339] ABAD, birleştirilmiş davalar C-465/00, C-138/01 ve C-139/01, Rechnungshof/Österreichischer Rundfunk ile Diğerleri ve Christa Neukomm ve Jospeh Lauermann/Österreichischer Rundfunk, 20 Mayıs 2003, para. 65; ABAD, C-524/06, Heinz Huber/Bundesrepublik Deutschland [GC], 16 Aralık 2008, para. 48; ABAD, birleştirilmiş davalar C-468/10 ve C-469/10, Asociación Nacional de Establecimientos Financieros de Crédito (ASNEF) ve Federación de Comercio Electrónico y Marketing Directo (FECEMD)/Administración del Estado, 24 Kasım 2011, para. 26.

koruma önlemlerini uygulamak zorunda kalacaktır.

Rıza

Avrupa Konseyi Hukuku uyarınca, Modernize Edilmiş Sözleşme 108'in 5 (2) maddesinde rıza konusu ele alınmıştır. Ayrıca AİHM içtihat hukukunda ve birkaç Avrupa Konseyi tavsiyesinde de belirtilmektedir.[340] AB hukuku uyarınca, yasal veri işlemenin temeli olarak rıza, GDPR'nin 6. maddesinde net olarak belirtilmiştir ve ayrıca açıkça Tüzük'ün 8. maddesinde de açıkça belirtilmektedir. Geçerli rızanın özellikleri 4. maddede rıza tanımında açıklanırken, geçerli rıza alma koşulları madde 7'de ayrıntılı olarak açıklanır ve bilgi toplumu hizmetleriyle ilgili olarak çocuğun rızası için özel kurallar GDPR'nin 8. maddesinde belirlenmiştir.

Bölüm 2.4'te açıklandığı gibi, rıza serbestçe verilmiş, bilgilendirilmiş, özel ve açık olmalıdır. Rıza, veri işlemeye yönelik bir anlaşmayı belirten bir beyan veya açıklayıcı bir eylem olmalıdır ve kişi, rızasını istediği zaman geri çekme hakkına sahiptir. Veri sorumluları, rızanın doğrulanabilir bir kaydını tutma görevine sahiptir.

Özgür rıza

Modernize Edilmiş Sözleşme 108'in Avrupa Konseyi çerçevesinde, veri sahibinin rızası "kasıtlı bir seçimin serbest ifadesini temsil etmelidir".[341] Serbest rızanın varlığı ancak "eğer konu gerçek bir seçim yapabilirse ve rıza göstermezse aldatma, korkutma, zorlama veya önemli olumsuz sonuçlar söz konusu değilse" geçerlidir.[342] Bu bağlamda, AB Hukuku, "veri sahibinin gerçek veya özgür bir seçimi yoksa veya zarar görmeden rızayı reddedemiyor veya geri çekemiyorsa" rızanın serbestçe verilmediğini öngörmektedir.[343] GDPR, "rızaların bağımsız olarak verilip verilmediğinin değerlendirilmesinde, diğerlerinin yanı sıra, bir hizmetin sunulması da dahil olmak üzere bir sözleşmenin ifasının, ifa için gerekli olmayan kişisel verilerin işlenmesine izin verilmesine bağlı olup olmadığı dikkate alınacağını" vurgulamaktadır.[344] Modernize Edilmiş Sözleşme 108 Açıklayıcı Raporu, "doğrudan veya dolaylı olarak, herhangi bir aşırı etki veya baskının (ekonomik veya başka bir nitelikte olabilir) veri sahibine uygulanabileceğini ve veri sahibinin gerçek bir seçeneğinin olmadığı veya önyargı olmadan reddedemediği veya geri çekemediği durumlarda rızanın bağımsız olarak verildiğinin kabul edilmeyeceğini" belirtmektedir.[345]

Örnek: A Devletindeki bazı belediyeler, içinde çip bulunan oturum kartları geliştirmeye karar vermiştir. Sakinlerin bu elektronik kartları almaları zorunlu değildir. Ancak, karta sahip olmayan sakinlerin Belediye vergilerini çevrimiçi olarak ödeme kabiliyeti, kurumun yanıt vermesi için üç günlük bir süreden itibaren elektronik olarak şikayetleri sunmak ve hatta kuyrukları atlamak, belediye konser salonunu ziyaret ederken indirimli bilet satın almak ve girişteki tarayıcıları kullanmak gibi bir dizi önemli idari hizmete erişimi bulunmamaktadır.

[340] Örneğin, Avrupa Konseyi, Bakanlar Komitesi (2010), Kişisel Verilerin profilleme bağlamında otomatik olarak işlenmesi konusunda bireylerin korunmasına ilişkin Bakanlar Komitesinin Üye Devletlere Önerisi CM/Rec (2010), 23 Kasım 2010, Md. 3.4 (b).
[341] Modernize Edilmiş Sözleşme 108 Açıklayıcı Raporu, para. 42.
[342] Ayrıca bakınız, Madde 29 Çalışma Grubu (2011), 15/2011 sayılı rıza kavramı üzerine görüş, WP 187, Brüksel, 13 Temmuz 2011, s. 12.
[343] Avrupa Genel Veri Koruma Regülasyonu, Başlangıç Hükmü 42.
[344] *Age*., Md. 7 (4).
[345] Modernize Edilmiş Sözleşme 108 Açıklayıcı Raporu, para. 42.

Belediyelerin bu örnekte kişisel verileri işlemesi, rızaya dayanamaz. Sakinlerin elektronik kartı almaları ve işlemeyi kabul etmeleri için en azından dolaylı bir baskı olduğu için, rıza serbestçe olarak verilemez. Belediyelerin bir elektronik kart sistemi geliştirmesi bu nedenle işlemeyi haklı kılan başka bir meşru temele dayanmalıdır. Örneğin, GDPR'nin 6 (1) (e) maddesi uyarınca işlem yapmak için hukuki bir temel teşkil eden kamu yararına yürütülen bir görevin yerine getirilmesi için işlemenin gerekli olduğunu söyleyebilirler.[346]

Serbest rıza, rızayı güvende tutan veri sorumlusu ile rızayı sağlayan veri sahibi arasında önemli bir ekonomik ya da başka bir dengesizliğin olduğu bir bağlılık kurulması durumunda şüpheli olabilir.[347] Bu dengesizliklerin ve bağlantının tipik bir örneği, bir işverenin, bir iş ilişkisi kapsamında, kişisel verileri işlemesidir. Madde 29 Çalışma Grubu'na göre, "İşçiler, işveren/işçi ilişkisinden kaynaklanan bağımlılık göz önüne alındığında, neredeyse hiçbir zaman serbestçe rıza verme, reddetme veya geri alma konumunda değildir. Güç dengesizliği göz önüne alındığında, işçiler yalnızca bir teklifin kabulü veya reddine bağlı bir sonuç olmadığında, istisnai durumlarda serbest rıza verebilir."[348]

Örnek: Büyük bir şirket, yalnızca şirket içi iletişimi geliştirmek için tüm çalışanların adlarını, şirket içindeki işlevlerini ve iş adreslerini içeren bir dizin oluşturmayı planlamaktadır. Personel müdürü, toplantılarda meslektaşları tanımayı kolaylaştırmak için her çalışanın fotoğrafını dizine eklemeyi önerir. Çalışanların temsilcileri, bunun sadece çalışanın izin vermesi durumunda yapılması gerektiğini talep eder.

Böyle bir durumda, bir çalışanın rızası, dizindeki fotoğrafların işlenmesinin hukuki dayanağı olarak kabul edilmelidir, çünkü çalışanın, ilgili dizinde fotoğrafının yayımlanmasını kabul etmeye karar verip vermesinde herhangi bir sonuçla karşılaşmayacağına inanılır.

Örnek: A Şirketi, gelecekteki bir projedeki iş birliğini görüşmek üzere çalışanlarından üçü ile B Şirketi'nin yöneticileri arasında bir toplantı gerçekleştirmeyi planlıyor. Toplantı, A Şirketi'nden toplantıya katılacakların adlarını, özgeçmişlerini ve fotoğraflarını e-posta ile göndermelerini isteyen B Şirketi'nde gerçekleştirilecektir. B Şirketi, binanın girişindeki güvenlik görevlilerinin gelen kişilerin doğru kişiler olup olmadıklarını kontrol etmeleri için katılımcıların adlarına ve fotoğraflarına ihtiyaç duyduğunu, özgeçmişlerin ise yöneticilerin toplantıya daha iyi hazırlanmasını sağlayacağını savunmaktadır. Bu durumda, A Şirketinin çalışanlarının kişisel verilerini aktarması rızaya dayanamaz. Rıza 'serbestçe verilmiş' olarak kabul edilemez, çünkü çalışanların teklifi reddetmeleri durumunda olumsuz sonuçlarla karşılaşmaları mümkündür (örneğin, yalnızca toplantıya katılmakla değil, aynı zamanda B şirketi ve projeye genel olarak katkıda bulunmak konusunda başka bir çalışan ile değiştirilebilir). Bu nedenle veri işlemesi, işleme için başka bir yasal zemine dayanmalıdır.

[346] Madde 29 Çalışma Grubu (2011), Rıza tanımına ilişkin 15/2011 sayılı Görüşü, WP187, Brüksel, 13 Temmuz 2011, p. 16. Veri işlemenin rızaya dayanamadığı ancak işlemin yasallaştırılması için farklı bir yasal dayanak gerektiği durumlarda başka örnekler de görüşün 14 ve 17. sayfasında bulunabilir.
[347] Ayrıca bakınız, Madde 29 Çalışma Grubu (2001), İstihdam bağlamında kişisel verilerin işlenmesi hakkındaki 8/2001 sayılı Görüş, WP48, Brüksel, 13 Eylül 2001; Madde 29 Çalışma Grubu (2005), 24 Ekim 1995 tarih ve 95/46/EC sayılı Direktif'in 26 (1) maddesinin ortak yorumu hakkında çalışma belgesi, WP 114, Brüksel, 25 Kasım 2005; Madde 29 Çalışma Grubu (2017), İşyerinde veri işleme hakkındaki 2/2017sayılı görüş, WP 249, Brüksel, 8 Haziran 2017.
[348] Madde 29 Çalışma Grubu, İşyerinde veri işleme hakkındaki 2/2017sayılı görüş, WP 249, Brüksel, 8 Haziran 2017.

Bununla birlikte, bu, rıza vermenin bazı olumsuz sonuçları olacağı durumlarda, rızanın hiçbir zaman geçerli olmayacağı anlamına gelmez. Örneğin, bir süpermarketin müşteri kartına sahip olmayı kabul etmemekle birlikte, yalnızca belirli malların fiyatında küçük bir indirim yapılmamasına neden olursa, rıza, böyle bir karta sahip olmak isteyen müşterilerin kişisel verilerini işleme koymak için geçerli bir hukuki dayanak olabilir. Şirket ile müşteri arasında hiçbir bağlantı yoktur ve rızanın bulunmamasının sonuçları, veri sahibinin serbest seçimini engellemek için yeterince ciddi değildir (fiyat indirimlerinin serbest seçimi etkilemeyecek kadar küçük olması şartıyla).

Bunun yanında, ancak belirli kişisel verilerin veri sorumlusuna veya daha sonra üçüncü şahıslara aktarılması ile mal veya hizmetler elde edilebiliyor ise, veri sahibinin sözleşme için gerekli olmayan verilerinin aktarılmasına ilişkin rızası serbestçe verilmiş olarak kabul edilemez ve bu nedenle veri koruma yasası kapsamında geçerli değildir.[349] GDPR, mal ve hizmetlerin sağlanması ile rızaların birleştirilmesini yasaklamakta oldukça katıdır.[350]

Örnek: Yolcuların, yolcu adı kayıtlarını (yani kimlikleri, beslenme alışkanlıkları veya sağlık sorunları ile ilgili verileri) belirli bir yabancı ülkenin göçmenlik makamlarına aktaran bir havayoluyla yaptığı anlaşma seyahat eden yolcuların bu ülkeyi ziyaret etmek istiyorlarsa seçme şansı bulunmadığından, veri koruma yasası uyarınca geçerli bir rıza olarak kabul edilemez. Eğer bu tür veriler yasalara uygun bir şekilde aktarılacaksa, rıza dışında, büyük olasılıkla belirli bir yasa olan, bir hukuki dayanak gereklidir.

Bilgilendirilmiş rıza

Veri sahibi, seçimini yapmadan önce yeterli bilgiye sahip olmalıdır. Bilgilendirilmiş rıza genellikle rıza gerektiren konunun kesin ve kolay anlaşılır bir tanımını içerir. Madde 29 Çalışma Grubunun açıkladığı gibi, rıza, veri sahibince işlemeye rıza gösterme eyleminin gerçeklerinin ve sonuçlarının takdir edilmesine ve anlaşılmasına dayanmalıdır. Bu nedenle, "ilgilenen kişiye, açık ve anlaşılır bir şekilde, işlenen verilerin niteliği, işlemenin amaçları, olası alıcılar ve veri sahibinin hakları […] gibi ilgili tüm konulara doğru ve tam bilgi verilmelidir."[351] Bilgilendirilmiş rızanın olması için bireylerin veri işlemeye izin vermemeleri durumundaki sonuçların farkında olmaları gerekir.

Bilgilendirilmiş rızanın önemi göz önüne alındığında, GDPR ve Modernize Edilmiş Sözleşme 108'in Açıklayıcı Raporu kavramı netleştirmeye çalışmıştır. GDPR'nin gerekçeleri, bilgilendirilmiş rızanın "veri sahibinin, en azından veri sorumlusunun kimliğinin ve işlenen kişisel verilerin işlendiği işlemin amaçlarının farkında olması gerektiğini" ifade eder.[352]

Uluslararası bir veri transferinin hukuki dayanağını sağlamak amacıyla kullanılan istisnai rıza durumunda, rızanın geçerli sayılması için veri sorumlusu veri sahibini ilgili ülkede yeterlilik kararının bulunmaması ve uygun güvencelerin bulunmaması nedeniyle doğacak olası riskler hakkında bilgilendirecektir.[353]

Modernize Edilmiş Sözleşme 108 Açıklayıcı Raporu, veri sahibinin kararının çıkarımları

[349] Avrupa Genel Veri Koruma Regülasyonu, Md. 7 (4).
[350] *Age*.
[351] Madde 29 Çalışma Grubu (2007), Elektronik sağlık kayıtlarında sağlığa ilişkin kişisel verilerin işlenmesi ile ilgili Çalışma Belgesi (EHR), WP 131, Brüksel, 15 Şubat 2007.
[352] Avrupa Genel Veri Koruma Regülasyonu, Başlangıç Hükmü 42.
[353] *Age*., Md. 49 (1) (a).

hakkında, "rıza verme gerçeğinin ne olduğu ve rızanın ne ölçüde verildiği" gibi bilgilerin verilmesi gerektiğini belirtir.[354]

Bilginin kalitesi önemlidir. Bilginin kalitesi, bilgi dilinin öngörülen alıcılara uyarlanması gerektiği anlamına gelir. Bilgiler jargon içermeden normal bir kullanıcının anlayabileceği açık ve net bir dille verilmelidir.[355] Bilgi, veri sahibi için de kolayca erişilebilir olmalı ve sözlü veya yazılı olarak sağlanmalıdır. Bilgilerin erişilebilirliği ve görünürlüğü önemli unsurlardır: bilgi açıkça görünür ve belirgin olmalıdır. Çevrimiçi bir ortamda, katmanlı bilgi bildirimleri iyi bir çözüm olabilir, çünkü bunlar veri sahiplerinin bilginin kısa ya da daha kapsamlı sürümlerini seçmesine olanak tanır.

Belirli rıza

Rızanın geçerli olması için, açıkça ve açık ifadelerle belirtilmesi gereken veri işleme amacına özgü olması gerekir. Bu, rızanın amacı hakkında verilen bilgilerin kalitesi ile birlikte gider. Bu kapsamda, ortalama bir veri sahibinin makul beklentileri ilgili olacaktır. İşleme operasyonlarının, ilk onay verildiğinde makul bir şekilde öngörülemeyecek şekilde eklenmesi veya değiştirilmesi durumunda ve dolayısıyla bir amaç değişikliğine yol açması durumunda veri sahibinden tekrar rıza istenmesi gerekir. Veri işlemenin birden fazla amacı olduğunda, hepsine rıza verilmelidir.[356]

Örnek: Deutsche Telekom AG Davasında,[357] ABAD, rehberlerde yayımlanacak olan abonelerin kişisel verilerini aktarmak zorunda olan bir telekom sağlayıcısının, rıza verildiği anda veri alıcısının adı belirtilmediği için, veri sahiplerinden[358] yeni rıza alınması gerekip gerekmediğini değerlendirmiştir.

ABAD, gizlilik ve elektronik haberleşme hakkındaki Direktif'in 12. maddesi uyarınca, verileri aktarmadan önce yenilenen rızanın gerekli olmadığına karar vermiştir. Veri sahipleri, yalnızca verilerinin işlenme amaçlarına – verilerinin yayımlanması- rıza verme seçeneğine sahip olduklarından, verilerin yayımlanabileceği farklı dizinler arasından seçim yapamamışlardır.

ABAD'nin vurguladığı gibi, "gizlilik ve elektronik haberleşmeye ilişkin Direktif'in 12. maddesinin bağlamsal ve sistematik bir yorumunun sonucu olarak, Madde 12 (2) kapsamındaki rızanın, kişisel verinin kamuya açık bir dizinde yayımlanması amacına ilişkin olduğu ve belirli bir dizin sağlayıcısının kimliğine ilişkin olmadığı" belirtilmiştir.[359] Ek olarak, yayıncının kimliğine ilişkin olmaktan ziyade; "kişisel verilerin kamuya açık bir dizinde yayınlanmasına ilişkin spesifik amaç bir abone için zararlı sonuçlar ortaya çıkarabilecektir"[360].

Tele2 (Netherlands) BV, Ziggo BV, Vodafone Libertel BV/Autoriteit Consument en Markt

[354] Modernize Edilmiş Sözleşme 108 Açıklayıcı Raporu, para. 42.
[355] Madde 29 Çalışma Grubu (2011), rızanın tanımı hakkında 15/2011 sayılı Görüş, WP 187, Brüksel, 13 Temmuz 2011, p. 19.
[356] Avrupa Genel Veri Koruma Regülasyonu, Başlangıç Hükmü 32.
[357] ABAD, C-543/09, Deutsche Telekom AG/Bundesrepublik Deutschland, 5 Mayıs 2011. Özellikle bakınız paras. 53 ve 54.
[358] Elektronik iletişim sektöründe kişisel verilerin işlenmesi ve gizliliğin korunmasına ilişkin 12 Temmuz 2002 tarih ve 2002/58/EC sayılı Avrupa Parlamentosu ve Konsey Direktifi, OJ 2002 L 201 (Gizlilik ve elektronik iletişim hakkında Direktif).
[359] ABAD, C-543/09, Deutsche Telekom AG/Bundesrepublik Deutschland, 5 Mayıs 2011; paras. 61.
[360] *Age*., para. 62.

(AMC)[361] davası, ilgili Belçika şirketinin, Hollanda'da telefon numarası ataması yapan şirketlerin rehber sorgulama hizmetlerinin ve rehberlerinin, abonelerine ait verilere erişim ile birlikte sağlanması talebine ilişkindir. Belçika şirketi Evrensel Hizmetler Direktifi uyarınca bir yükümlülüğe dayanmıştır.[362] Bu yükümlülük numara ataması yapan şirketler tarafından, abonelerin numaralarının yayınlanması yönünde rızalarının bulunması durumunda, bu telefon numaralarının talep eden dizinlerce erişilebilir kılınmasını düzenlemektedir. Hollanda şirketleri, söz konusu verileri başka bir Üye Ülke'de kurulan teşebbüse sağlamak zorunda olmadıklarını belirterek, bu yönde hareket etmeyi reddetmiştir. Kullanıcıların numaralarının yayınlanmasına, bunların bir Hollanda dizininde yayınlanacağı düşüncesiyle rıza verdiklerini savunmuşlardır. ABAD, Evrensel Hizmetler Direktifi'nin, kuruldukları Üye Ülke'den bağımsız olarak, rehberlik hizmeti teşebbüsleri tarafından yapılan tüm talepleri kapsadığını belirtmiştir. ABAD ayrıca, aynı verilerin abonelerden yenilenmiş rıza alınmadan kamuya açık bir rehber yayınlamayı amaçlayan başka bir kuruluşa iletilmesinin kişisel verilerin korunma hakkına önemli ölçüde zarar vermediğini belirtmiştir.[363] Sonuç olarak, abonelerine telefon numarası tahsis eden teşebbüsün, aboneye yönelteceği rıza talebini kendisiyle ilgili verilerin gönderilebileceği Üye Ülke'ye göre farklılaştırmasına gerek olmadığı değerlendirilmiştir.[364]

Açık rıza [ÇN: *Unambiguous consent*]

Tüm rızalar şüpheye mahal bırakmayacak şekilde verilmelidir.[365] Bu, veri sahibinin, verilerinin işlenmesine izin vermek için yaptığı anlaşmayı ifade etmek istediğine dair makul hiçbir şüphe bulunmaması gerektiği anlamına gelir. Örneğin, veri sahibinin hareketsiz kalması, açık rıza anlamına gelmez.

Bu, veri sorumlularının "hizmetimizi kullanarak, kişisel verilerinizin işlenmesine rıza vermektesiniz" gibi gizlilik politikalarındaki ifadelerle rıza alması halinde söz konusu olacaktır. Bu durumda, veri sorumluları, kullanıcıların bu politikalara şahsen ve bireysel olarak rıza vermesini sağlamak zorunda kalabilir. Eğer rıza bir sözleşmenin parçası olarak yazılı bir şekilde verilmişse, kişisel verilerin işlenmesi için rıza kişiselleştirilmeli ve her durumda "güvenceler, veri sahibinin rızayı verdiğini ve ne ölçüde verdiğinin farkında olduğunu temin etmelidir".[366]

Çocuklara ilişkin rıza gereksinimleri

GDPR, bilgi toplumu hizmetlerinin sunulması bağlamında çocuklara özel bir koruma sağlamaktadır, çünkü "kişisel verilerin işlenmesi ile ilgili risklerin, sonuçların, korunmaların ve haklarının daha az farkında olabileceklerdir".[367] Bu nedenle, AB Hukuku uyarınca, bilgi toplumu hizmet sağlayıcıları, 16 yaşın altındaki çocukların kişisel verilerini rıza esasına göre işlerken, bu tür işlemeler "ancak çocuk üzerinde velayet sorumluluğu sahibi tarafından onay veya izin verildiği müddetçe" hukuka uygun olacaktır.[368] Üye Ülkeler, 13 yaşın altında

[361] ABAD, C-536/15, Tele2 (Netherlands) BV and Others/Autoriteit Consument en Markt (AMC), 15 Mart 2017.
[362] Elektronik haberleşme ağları ve hizmetleri ile ilgili evrensel hizmet ve kullanıcıların hakları hakkındaki 7 Mart 2002 tarih ve 2002/22/EC sayılı Avrupa Parlamentosu ve Konseyi Direktifi (Evrensel Hizmet Direktifi), OJ 2002 L 108, p. 51, Avrupa Parlamentosu ve Konseyi'nin 25 Kasım 2009 tarih 2009/136/EC sayılı Direktifi ile değiştirildiği gibi (Evrensel Hizmetler Direktifi), OJ 2009 L 337, p. 11.
[363] ABAD, C-536/15, Tele2 (Netherlands) BV and Others/Autoriteit Consument en Markt (AMC), 15 Mart 2017, para. 36.
[364] *Age*. Paras. 40-41.
[365] Avrupa Genel Veri Koruma Regülasyonu, Md. 4 (11).
[366] *Age*., Başlangıç Hükmü 42.
[367] *Age*., Başlangıç Hükmü 38.
[368] *Age*. Md. 8 (1) ilk girdi. Bilgi toplumu hizmetleri kavramı, Avrupa Genel Veri Koruma Regülasyonu'nun 4 (25) maddesinde tanımlanmıştır.

olmamak üzere, ulusal hukuklarında daha düşük bir yaş sınırı öngörebilirler.[369] Velayet sorumluluğu sahibinin rızası, "doğrudan çocuğa sunulan önleyici hizmetler ya da danışmanlık hizmetleri bakımından" gerekli değildir.[370] Bir çocuğa ait kişisel verilerin işlendiği durumlarda yapılacak bilgilendirme ve iletişim, çocuk tarafından kolayca anlaşılabilir, açık ve net bir dilde olmalıdır.[371]

Herhangi bir zamanda rızayı geri alma hakkı

GDPR, herhangi bir zamanda rızayı geri alma genel hakkını içermektedir.[372] Veri sahiplerinin rıza göstermeden önce bu haklarının varlığından ve bu hakkı kendi takdirine bağlı olarak kullanabileceği konularında bilgilendirilmelidir. Rızayı geri alma sebebini açıklama zorunluluğu getirilmemeli ve önceden izin verilen veri kullanımından kaynaklanabilecek herhangi bir faydanın sona ermesine yönelik olumsuz sonuçların ortaya çıkma riski bulunmamalıdır. Rızanın geri alınması, rızanın verilmesi ile eşit kolaylıkta olmalıdır.[373] Eğer veri sahibi herhangi bir zarara uğramaksızın veya rızanın verilmesinden daha zor bir yöntemle geri alınması gerekmekte ise, rızanın özgür iradeye dayalı olarak verildiğinden söz edilemeyecektir.[374]

Örnek: Bir müşteri, veri sorumlusuna sağladığı adrese promosyon amaçlı posta gönderilmesini kabul etmiştir. Müşterinin rızasını geri alması durumunda, veri sorumlusunun promosyon amaçlı posta göndermeyi derhal durdurması gerekmektedir. Ücret ödeme zorunluğu gibi herhangi bir cezai sonuç getirilmemelidir. Ancak geri alma ileriye etkili olacak şekilde gerçekleştirilebilecek ve geriye dönük uygulanması söz konusu olmayacaktır. Müşterinin rızasının bulunması sebebiyle, bu süre içerisinde geçekleştirilen işleme faaliyetleri hukuka uygundur. Rızanın geri alınması, bu tür işlemeler silme hakkının kullanılması kapsamında olmadığı müddetçe, kişisel verilerin bu aşamadan sonra işlenmesini önlemektedir.[375]

Bir sözleşmenin ifası için gereklilik

AB Hukuku uyarınca, GDPR'nin 6 (1) (b) maddesi, "veri sahibinin taraf olduğu bir sözleşmenin ifası için gerekliyse" hukuka uygun veri işleme için başka bir temel sağlamaktadır. Bu hüküm sözleşme öncesi ilişkileri de kapsamaktadır. Bir tarafın bir sözleşme akdetme iradesinin bulunduğu, ancak sözleşmenin muhtemelen bazı kontrollerin halihazırda tamamlanmamış olması sebebiyle henüz kurulmadığı durumlar örnek verilebilecektir. Bir tarafın bu amaçla veri işlemesi gerekiyorsa, veri işleme faaliyeti "bir sözleşmeye girmeden önce veri sahibinin talebi üzerine adım atılması için gerekli" olduğu sürece meşrudur.[376]

Modernize Edilmiş Sözleşme 108'in 5(2) maddesinde "hukuken belirlenen meşru temel" olarak veri işleme kavramı, aynı zamanda "veri sahibinin taraf olduğu bir sözleşmenin (veya veri sahibinin talebi üzerine sözleşme öncesi önlemlerin) yerine getirilmesi için veri işlemeyi" de

[369] Avrupa Genel Veri Koruma Regülasyonu Md. 8 (1) ikinci girdi.
[370] *Age*., Başlangıç Hükmü 38.
[371] *Age*., Başlangıç Hükmü 58. Ayrıca bakınız, Modernize Edilmiş Sözleşme 108 Md. 15 (2) (e). Modernize Edilmiş Sözleşme 108 Açıklayıcı Raporu, paras. 68 ve 125.
[372] Avrupa Genel Veri Koruma Regülasyonu Md. 7 (3). Modernize Edilmiş Sözleşme 108 Açıklayıcı Raporu, paras. 68 ve 125.
[373] Avrupa Genel Veri Koruma Regülasyonu Md. 7 (3).
[374] Avrupa Genel Veri Koruma Regülasyonu, Başlangıç Hükmü 42; Modernize Edilmiş Sözleşme 108 Açıklayıcı Raporu, para. 42.
[375] Avrupa Genel Veri Koruma Regülasyonu Md. 17 (1) (b).
[376] *Age*., Md. 6 (1) (b).

içerir.[377]

Veri sorumlusunun hukuki yükümlülükleri

AB Hukuku, veri işlemenin meşrulaştırılması için bir başka temel belirlemektedir: "veri sorumlusunun tabi olduğu hukuki bir yükümlülüğün yerine getirilmesi için gerekli ise" (GDPR Madde 6 (1) (c)). Bu hüküm hem özel hem de kamu sektöründe faaliyet gösteren veri sorumlularına atıf yapmaktadır; kamu sektöründe faaliyet gösteren veri sorumlularının yasal yükümlülükleri GDPR'nin 6 (1) (e) maddesine kapsamında da değerlendirilebilir. Yasanın, özel sektör veri sorumlularını somut veri sahiplerine ilişkin verileri işlemesinin zorunlu olduğu birçok durum vardır. Örneğin, işverenlerin çalışanları ile ilgili verileri sosyal güvenlik ve vergilendirme sebepleriyle işlemesi gerekir ve işletmelerin, müşterileriyle ilgili verileri vergi amacıyla işlemesi zorunludur.

Hukuki yükümlülük, bir veya birkaç veri işleme faaliyetinin temeli olabilecek Birlik veya Üye Ülke yasalarından kaynaklanabilir. Veri işleme amacının, veri sorumlusunun tespitine ilişkin spesifikasyonların oluşturulması, işleme faaliyetine tabi tutulan kişisel verilerin tipi, ilgili veri sahipleri, verilerin aktarılabileceği kurumlar, amaç sınırlamaları, saklama süresi ve hukuka uygun ve adil veri işlemeye ilişkin diğer önlemler kanunla belirlenmelidir.[378] Kişisel veri işleme faaliyetinin temelini teşkil eden bu tür bir yasa hem Regülasyon'un 7 ve 8'inci maddelerine hem de AİHS'in 8. maddesine uygun olmalıdır.

Avrupa Konseyi Hukuku uyarınca, veri sorumlusunun hukuki yükümlülükleri aynı zamanda hukuka uygun veri işleme için bir temel teşkil eder.[379] Daha önce de belirtildiği gibi, bir özel sektör veri sorumlusunun yasal yükümlülükleri, AİHS'in 8 (2) maddesinde belirtildiği üzere, başkalarının meşru menfaatlerinin yalnızca bir örneğidir. Bu nedenle, çalışanları hakkında veri işleyen işverenlerle ilgili örnek, aynı zamanda Avrupa Konseyi Hukuku için de geçerlidir.

Veri sahibinin ya da başka bir gerçek kişinin hayati çıkarları

AB Hukuku uyarınca, GDPR'nin 6 (1) (d) maddesi, "veri sahibinin veya başka bir gerçek kişinin hayati çıkarlarını korumak için gerekli ise" kişisel veri işlemenin hukuka uygun olduğunu kabul etmektedir. Bu yasal zemin, eğer böyle bir veri işleme faaliyeti "açıkça başka bir hukuki temele dayanamıyorsa" kişisel verilerin başka bir gerçek kişinin hayati çıkarlarına dayanarak işlenmesi için ileri sürülebilir.[380] Bazen bir veri işleme türü, hem kamu yararına hem de veri sahibinin ya da başka bir kişinin hayati çıkarlarına dayanabilir. Örneğin, salgınları ve gelişimlerini izlerken ya da insani bir acil durum söz konusu olduğunda bu temele dayanılabilecektir.

Avrupa Konseyi Hukuku uyarınca, veri sahibinin hayati çıkarları AİHS'in 8. maddesinde belirtilmemiştir. Bununla birlikte, veri sahibinin hayati çıkarlarından, kişisel veri işlemenin meşruiyetini düzenleyen Modernize Edilmiş Sözleşme 108'in 5 (2) maddesinde yer alan "meşru temel" kavramı kapsamında bahsedildiği düşünülmektedir.[381]

---

[377] Modernize Edilmiş Sözleşme 108 Açıklayıcı Raporu, para. 46; Avrupa Konseyi, Bakanlar Komitesi (2010), Kişisel verilerin profilleme bağlamında otomatik olarak işlenmesi konusunda bireylerin korunmasına ilişkin Üye Devletlerin Bakanlar Komitesinin CM/Rec(2010)13 sayılı Tavsiyesi 23 Kasım 2010, Md. 3, 4 (b).
[378] Avrupa Genel Veri Koruma Regülasyonu, Başlangıç Hükmü 45.
[379] Avrupa Konseyi, Bakanlar Komitesi (2010), Kişisel verilerin profilleme bağlamında otomatik olarak işlenmesi konusunda bireylerin korunmasına ilişkin Üye Devletlerin Bakanlar Komitesinin CM/Rec(2010)13 sayılı Tavsiyesi 23 Kasım 2010, Md. 3, 4 (a).
[380] Avrupa Genel Veri Koruma Regülasyonu, Başlangıç Hükmü 46.
[381] Modernize Edilmiş Sözleşme 108 Açıklayıcı Raporu, para. 46.

Kamu yararı ve resmi yetkinin kullanılması

Kamu işlerini organize etmenin birçok olası yöntemi bulunduğu göz önüne alındığında, GDPR'nin 6 (1) (e) maddesi, kişisel verilerin "kamu yararına görülen bir işin yerine getirilmesi veya veri sorumlusuna verilen resmi yetkinin kullanılması için gerekli ise [...]" hukuka uygun olarak işlenebileceğini öngörmektedir.[382]

Örnek: Huber/Bundesrepublik Deutschland Davasında,[383] Almanya'da ikamet eden bir Avusturya vatandaşı olan Bay Huber, Federal Göçmen ve Mülteciler Bürosu'ndan, Yabancı Uyruklu Merkez Kayıt Defteri'nde ("AZR") yer alan verilerinin silmesini istedi. Üç aydan fazla bir süredir Almanya'da ikamet eden Alman olmayan AB vatandaşları hakkında kişisel veriler içeren bu kayıt, istatistiksel amaçlar için ve kamu güvenliğini tehdit edenleri soruştururken ve kovuştururken kolluk kuvvetleri ve adli makamlar tarafından kullanılmaktadır. Başvurucu mahkeme, Alman vatandaşları için böyle bir sicilin bulunmadığı göz önüne alındığında diğer kamu kurumlarının da erişebildiği Yabancı Uyruklu Merkez Kayıt Defteri gibi bir sicilde yapılan kişisel veri işleme faaliyetlerinin AB Hukukuna uygun olup olmadığını sormuştur.

ABAD, 95/46[384] sayılı Direktif'in 7 (e) maddesine göre, kamu yararına bir görevin yerine getirilmesi veya resmi bir yetkinin kullanılması için gerekli ise, kişisel verilerin hukuka uygun olarak işlenebileceğini belirtmiştir.

ABAD, "Tüm Üye Ülkeler'de eşdeğer bir koruma seviyesi sağlama hedefi göz önüne alındığında, 95/46[385] sayılı Direktif'in 7 (e) maddesinde ortaya koyulan zorunluluk kavramı [...] Üye Ülkeler arasında değişen bir anlama sahip olamaz. Bu nedenle, bahse konu kavramın Topluluk hukukunda kendine ait bir anlamı olduğu ve Madde 1 (1) kapsamında belirtilen şekilde, bu direktifin amacını tamamen yansıtacak şekilde yorumlanması gereken bir kavram"[386] olduğunu belirtir.

ABAD, bir Birlik vatandaşının, vatandaşı olmadığı bir Üye Ülke'de serbest dolaşım hakkının koşulsuz olmadığını ve Avrupa Topluluğu'nun Kurucu Antlaşması ile yürürlüğe girmesi için alınan tedbirlerin getirdiği sınırlama ve koşullara tabi olabileceğini belirtmiştir. Bu nedenle, ilke olarak, bir Üye Ülke'nin, yerleşim hakkına ilişkin mevzuatı uygulamaktan sorumlu makamları desteklemek için AZR gibi bir kayıt defteri kullanması meşru ise, böyle bir kayıt, bu amaç için gerekli olandan başka hiçbir bilgi içermemelidir. ABAD, kişisel verilerin işlenmesi için böyle bir sistemin, yalnızca bu mevzuatı uygulamak için gerekli verileri içermesi ve merkezi yapısının bu mevzuatın uygulanmasını daha etkili hale getirmesi için gerekli olması şartıyla AB Hukukuna uygun olduğu sonucuna varmıştır. Ulusal mahkeme, bu şartların bu özel durumda yerine getirilip getirilmediğini tespit etmelidir. Aksi takdirde, kişisel verilerin AZR gibi bir kayıtta istatistiksel amaçlarla saklanması ve işlenmesi, 95/46 sayılı Direktifin 7 (e)[387] maddesinin anlamı dahilinde, hiçbir şekilde gerekli sayılmaz.[388]

Son olarak, sicilde yer alan verilerin suçla mücadele amacıyla kullanımına ilişkin olarak, ABAD, bu amacın "faillerinin milliyetine bakılmaksızın mutlaka işlenen suç ve suçların

[382] Bakınız Avrupa Genel Veri Koruma Regülasyonu, Başlangıç Hükmü 45.
[383] ABAD, C-524/06, Heinz Huber/Bundesrepublik Deutschland [GC], 16 Aralık 2008.
[384] Geçmiş Veri Koruma Drektifi, Md. 7 (e), şimdiki Avrupa Genel Veri Koruma Regülasyonu, Md. 6 (1) (e).
[385] *Age*.
[386] ABAD, C-524/06, Heinz Huber/Bundesrepublik Deutschland [GC], 16 Aralık 2008, para. 52.
[387] Geçmiş Veri Koruma Drektifi, Md. 7 (e), şimdiki Avrupa Genel Veri Koruma Regülasyonu, Md. 6 (1) (e).
[388] ABAD, C-524/06, Heinz Huber/Bundesrepublik Deutschland [GC], 16 Aralık 2008, para. 54, 58-59 ve 66-68.

kovuşturulmasını içerdiğini" belirtmiştir. Söz konusu sicil, ilgili Üye Ülke'nin vatandaşları ile ilgili kişisel verileri içermemektedir ve bu muameledeki farklılık, TFAB'nun 18. maddesi tarafından yasaklanan bir ayrımcılık teşkil etmektedir. Sonuç olarak, ABAD bu hükmün "Üye Ülke tarafından suçla mücadele amacıyla, Üye Ülke'nin vatandaşı olmayan Birlik vatandaşlarına özgü kişisel verilerin işlenmesine ilişkin bir sistemin kurulmasını engellediğini" tespit etmiştir.[389]

Kişisel verilerin kamusal alanda faaliyet gösteren makamlar tarafından kullanılması da AİHS'in 8. maddesine tabidir ve uygun düştüğü ölçüde Modernize Edilmiş Sözleşme 108'in 5 (2) Maddesi kapsamında değerlendirilmektedir.[390]

Veri sorumlusu veya üçüncü bir tarafın meşru menfaatleri

AB Hukukuna göre, veri sahibi meşru menfaatleri olan tek kişi değildir. GDPR'nin 6 (1) (f) maddesi, kişisel verilerin "veri sorumlusunun veya verilerin açıklandığı üçüncü tarafın veya tarafların [görevlerini yerine getiren kamu yetkilileri hariç olmak üzere] meşru menfaatleri için gerekli olması durumunda, bu tür menfaatlerin korunma gerektiren veri sahiplerinin menfaatlerine veya temel hak ve özgürlüklerine zarar vermemesi şartıyla […]" hukuka uygun olarak işlenmesini sağlar.[391]

Meşru bir menfaatin varlığı, her bir durum özelinde dikkatlice değerlendirilmelidir.[392] Veri sorumlusunun meşru menfaatleri tanımlanırsa, bu menfaatler ve veri sahibinin temel hak ve özgürlükleri veya menfaatleri arasında bir dengeleme çalışması yapılmalıdır.[393] Veri sahibinin makul beklentileri, veri sorumlusunun menfaatlerinin, veri sahibinin menfaatlerini veya temel haklarını geçersiz kılmadığını belirlemek için böyle bir değerlendirme sırasında göz önünde bulundurulmalıdır.[394] Veri sahibinin hakları veri sorumlusunun meşru menfaatlerine zarar verirse, daha sonra veri sorumlusu, veri sahibinin hakları üzerindeki etkisinin en aza indirgenmesini sağlamak için önlemler alabilir ve güvenlik önlemleri uygulayabilir (örneğin; verilerin maskelenmesi) ve hukuka uygun veri işleme için bu meşru temele dayanmadan önce "dengeyi" tersine çevirir. Veri sorumlusunun meşru menfaatleri kavramı hakkındaki görüşünde, Madde 29 Çalışma Grubu, hesap verebilirliğin ve şeffaflığın ve veri sahibinin, veri sorumlusunun meşru menfaatlerini ve veri sahibinin temel haklar ve menfaatlerini dengelerken, verilerinin işlenmesine veya erişilmesine, değiştirilmesine, silinmesine veya aktarılmasına itiraz etme haklarının kritik rolünü vurgulamıştır.[395]

GDPR başlangıç hükümlerinde, ilgili veri sorumlularının meşru menfaatlerini teşkil eden hususlara ilişkin bazı örnekler verilmiştir. Örneğin, doğrudan pazarlama amacıyla yapıldığında veya böyle bir işlemin "dolandırıcılığı önlemek için kesin olarak gerekli" olduğu durumlarda, veri sahibinin rızası olmadan kişisel verilerin işlenmesine izin verilir.[396]

ABAD içtihadında, neyin meşru bir menfaat teşkil ettiğini belirleyen testini genişletmiştir.

---

[389] *Age*., paras. 78 ve 81.
[390] Modernize Edilmiş Sözleşme 108 Açıklayıcı Raporu, paras. 46 ve 47.
[391] 95/46 sayılı Direktife kıyasla, Avrupa Genel Veri Koruma Regülasyonu meşru menfaat teşkil ettiği düşünülen davalara daha fazla örnek sunmaktadır.
[392] Avrupa Genel Veri Koruma Regülasyonu, Başlangıç Hükmü 47.
[393] Madde 29 Çalışma Grubu (2014), 95/46/EC sayılı Direktifin 7. Maddesi uyarınca veri sorumlusunun meşru menfaatleri kavramı hakkında 06/2014 sayılı Görüş, 4 Nisan 2014.
[394] *Age*.
[395] *Age*.
[396] Avrupa Genel Veri Koruma Regülasyonu, Giriş, Başlangıç Hükmü 47

Örnek: Valsts policijas Rīgas reģiona pārvaldes Kārtības policijas pārvalde Davası[397], aniden taksi kapısını açan bir yolcunun, Rīgas Nakliyat Şirketi troleybüsüne zarar vermesine ilişkindir. Rīgas satiksme, yolcuya tazminat davası açmak istemiştir. Bununla birlikte, polis sadece yolcunun ismini vermiştir ve yolcunun kimlik numarası ve adresini açıklamanın ulusal veri koruma yasaları uyarınca yasadışı olacağını savunarak bunları vermeyi reddetmiştir.

Letonya sevk mahkemesi, ABAD'den AB veri koruma mevzuatının idari suçtan sorumlu olduğu iddia edilen kişiye karşı adli işlem başlatmak için gerekli tüm kişisel verileri ifşa etme yükümlülüğü getirip getirmediği konusunda bir ön karar vermesini istemiştir.[398]

ABAD, AB veri koruma yasasının, üçüncü bir tarafın meşru menfaatlerine ilişkin amaçları için söz konusu taraf ile veri paylaşılması olasılığını (bir zorunluluk değil) içerdiğini netleştirmiştir.[399] ABAD, kişisel verilerin işleme faaliyetlerinin "meşru menfaat" temelinde hukuka uygun olarak değerlendirilmesi için kümülatif olarak sağlanması gereken üç koşul belirlemiştir.[400] İlk olarak, kişisel verilerin açıklandığı üçüncü tarafın meşru bir menfaati bulunmalıdır. Bu spesifik durumda, eşyanın zarara uğraması nedeniyle bir kişiye dava açılması için kişisel bilgilerin talep edilmesi üçüncü kişi için meşru bir menfaati teşkil ettiği anlamına gelir. İkinci olarak, kişisel verilerin işlenmesi, meşru menfaatin elde edilmesi için gerekli olmalıdır. Bu spesifik durumda, adres ve/veya kimlik numarası gibi kişisel bilgilerin alınması, bu kişiyi tanımlamak için kesinlikle gereklidir. Üçüncü olarak, veri sahibinin temel hak ve özgürlükleri veri sorumlusunun veya üçüncü tarafların meşru menfaatlerinden öncelikli olmamalıdır. Menfaatler dengesi, veri sahibinin haklarının ihlal edilmesinin ciddiyeti, hatta bazı durumlarda veri sahibinin yaşı gibi unsurlar dikkate alınarak, her somut duruma göre yapılmalıdır. Bununla birlikte, bu spesifik durumda, ABAD, veri sahiplerinin küçük olmasını, kişisel verilerin açıklanmasının reddini haklı göstermediğini kabul etmiştir.

ASNEF ve FECEMD yargılamasında, ABAD açıkça, kişisel verilerin Veri Koruma Direktifi'nin 7 (f) maddesinde detaylandırılan 'meşru menfaat' hukuki temeline dayalı olarak işlenmesine karar vermiştir.[401]

Örnek: ASNEF ve FECEMD davasında,[402] ABAD, ulusal yasaların, verilerin hukuka uygun işlenmesine ilişkin Direktif'in 7 (f) Maddesinde belirtilenlere ek şart getirme yetkisi bulunmadığını açıklığa kavuşturmuştur.[403] Bu, bir bilginin zaten kamuya açık kaynaklarda ortaya çıkmış olması halinde diğer özel tarafların kişisel bilgileri işlemede meşru bir çıkar talep edebilecekleri yönünde bir hüküm içeren İspanya veri koruma kanununa atıfta bulunmuştur.

ABAD, ilk olarak 95/46[404] sayılı Direktif'in, kişisel verilerin işlenmesiyle ilgili olarak bireylerin hak ve özgürlüklerinin korunma seviyesinin tüm Üye Ülkeler nezdinde eşdeğer olmasını sağlamaya yönelik olduğunu belirtti. Bu alanda geçerli olan ulusal yasaların

[397] ABAD, C-13/16, Valsts policijas Rīgas reģiona pārvaldes Kārtības policijas pārvalde/Rīgas pašvaldības SIA 'Rīgas satiksme', 4 Mayıs 2017.
[398] *Age*. para. 23.
[399] *Age*., para. 26.
[400] *Age*. para. 28-34.
[401] Eski Veri Koruma Direktifi, Md. 7 (f), şimdi Avrupa Genel Veri Koruma Regülasyonu, Md. 6 (1) (f).
[402] ABAD, birleştirilmiş davalar C-468/10 ve C-469/10, Asociación Nacional de Establecimientos Financieros de Crédito (ASNEF) ve Federación de Comercio Electrónico y Marketing Directo (FECEMD)/Administración del Estado, 24 Kasım 2011.
[403] Eski Veri Koruma Direktifi, Md. 7 (f), şimdi Avrupa Genel Veri Koruma Regülasyonu, Md. 6 (1) (f).
[404] Eski Veri Koruma Direktifi, şimdi Avrupa Genel Veri Koruma Regülasyonu.

uyumlulaştırılmasının da sağladıkları sağlanan korumanın azalmasına neden olmamalıdır. Bunun yerine, AB'de yüksek düzeyde koruma sağlamaya çalışmalıdır.[405] Sonuç olarak, ABAD "tüm Üye Ülkeler nezdinde 95/46[406] sayılı Direktif'in 7. maddesinin, kişisel verilerin işlenmesine ilişkin hukuka uygunluk halleri kapsamında değerlendirilebilecek durumların kapsamlı ve kısıtlayıcı bir listesini ortaya koyduğunu belirten bir koruma seviyesi sağlama hedefi izlediğini" belirtmiştir. Ayrıca, "Üye Ülkeler, Direktif'in 7. maddesi kapsamına kişisel verilerin işlenmesinin hukuka uygunluğu ile ilgili yeni ilkeler ekleyemez ve 95/46[407] sayılı Direktif'in 7. maddesinde öngörülen altı ilkeden birinin kapsamını değiştirme etkisi olan ek şartlar belirleyemez".[408] ABAD, 95/46/EC sayılı Direktif'in 7 (f) maddesi uyarınca gerekli olan denge bakımından, kişisel verilerinin işlenmesi ile veri sahibinin temel haklarının ihlalinin ciddiyetinin, söz konusu verilerin zaten halka açık kaynaklarda bulunup bulunmamasına bağlı olarak değişebileceğinin dikkate alınmasın mümkün olduğunu kabul etmiştir.

Ancak, Direktifin 7 (f) maddesi, bir Üye Ülkeler'in kategorik ve genelleştirilmiş bir şekilde, kişisel verilerin çatışan hak ve menfaatlerin birbirlerine karşı dengelenmesini sağlamaksızın, belirli kişisel veri kategorilerinin işlenmesini engellemektedir."

Bu değerlendirmeler ışığında, ABAD 95/46[409] sayılı Direktif'in 7 (f) maddesinin "veri sahibinin rızası bulunmaksızın kişisel verilerinin, veri sorumlusunun ya da bu verilerin aktarıldığı üçüncü tarafların meşru menfaatinin elde edilmesi amacıyla zorunlu olarak işlenmesine yalnızca veri sahibinin temel hak ve özgürlüklerine müdahale edilmemesi değil; aynı zamanda kişisel verilerin kamuya açık kaynaklarda bulunmadığı durumlar hariç olmak üzere, kategorik ve genelleştirilmiş bir şekilde bu tür kaynaklarda bulunan verilerin işlenmesine izin veren ulusal düzenlemelerin önüne geçmekte olduğu" şeklinde yorumlanması gerektiği sonucuna varmıştır.[410]

Kişisel verilerin meşru menfaat temelinde işlendiği durumlarda, GDPR'nin 21 (1) maddesi uyarınca, veri sahipleri kendi özel durumlarına ilişkin sebeplere dayanarak, kişisel verilerinin işlenmesine itiraz etme hakkına sahiptir. Veri sorumlusu, işleme faaliyetinin devam etmesi yönünde meşru bir gerekçe sunmadığı müddetçe, kişisel veri işleme faaliyetini durdurmalıdır.

Avrupa Konseyi Hukuku bakımından benzer formülasyonlar, Modernize Edilen Sözleşme 108'de[411] Avrupa Konseyi'nin tavsiye kararlarında bulunabilecektir. Profilleme Tavsiye Kararı, kişisel verilerin profilleme amacıyla işlenmesinin, başkalarının meşru menfaatlerinin elde edilmesi için gerekli ise "bu tür menfaatlerin, veri sahiplerinin temel hak ve özgürlüklerine müdahale teşkil ettiği durumlar hariç olmak üzere" meşru olduğunu kabul etmiştir.[412] Buna ek olarak, "başkalarının hak ve özgürlüklerinin korunması", AİHS'nin 8(2) Maddesi'nde, kişisel verilerin korunması hakkının sınırlandırılmasının meşru dayanaklarından biri olarak

[405] ABAD, birleştirilmiş davalar C-468/10 ve C-469/10, Asociación Nacional de Establecimientos Financieros de Crédito (ASNEF) ve Federación de Comercio Electrónico y Marketing Directo (FECEMD)/Administración del Estado, 24 Kasım 2011, para. 28. Bakınız Veri Koruma Direktifi, Başlangıç Hükümleri 8 ve 10.
[406] Eski Veri Koruma Direktifi, Md. 7, şimdi Avrupa Genel Veri Koruma Regülasyonu, Md. 6 (1) (f).
[407] Eski Veri Koruma Direktifi, Md. 7, şimdi Avrupa Genel Veri Koruma Regülasyonu, Md. 6.
[408] *Age*.
[409] Eski Veri Koruma Direktifi, Md. 7 (f), şimdi Avrupa Genel Veri Koruma Regülasyonu, Md. 6 (1) (f).
[410] ABAD, birleştirilmiş davalar C-468/10 ve C-469/10, Asociación Nacional de Establecimientos Financieros de Crédito (ASNEF) ve Federación de Comercio Electrónico y Marketing Directo (FECEMD)/Administración del Estado, 24 Kasım 2011, para. 40, 44 ve 48-49.
[411] Modernize Edilmiş Sözleşme 108 Açıklayıcı Raporu, para. 46.
[412] Avrupa Konseyi, Bakanlar Komitesi (2010), Kişisel Verilerin profilleme bağlamında otomatik olarak işlenmesi konusunda bireylerin korunmasına ilişkin Bakanlar Komitesinin Üye Devletlere Önerisi CM/Rec (2010), 23 Kasım 2010, Md. 3.4 (b) (Profilleme Tavsiyesi).

belirtilmiştir.

Örnek: Y/Türkiye Davası'nda,[413] başvuru sahibi HIV pozitiftir. Hastaneye geldiği sırada bilinçsiz olduğu için, ambulans ekibi, hastane çalışanlarına kişinin HIV pozitif olduğunu bildirmiştir. Başvuru sahibi, bu bilgilerin açıklanmasının özel hayata saygı hakkını ihlal ettiğini AİHM nezdinde iddiasında bulunmuştur. Bununla birlikte, hastane personelinin güvenliğinin koruması ihtiyacı bulunması sebebiyle, bilginin paylaşılmasının ihlalini teşkil etmeyeceği belirtilmiştir.

4.1.2. Özel nitelikli kişisel verilerin (hassas veriler) işlenmesi

Avrupa Konseyi Hukuku, Modernize Edilmiş Sözleşme 108'in 6. maddesinde belirlenen şartların sağlanması; yani Sözleşme'nin diğer hükümlerini tamamlayıcı uygun korumaların yasayla belirlenmiş olması kaydıyla, hassas verilerin kullanılmasına için uygun korumaların düzenlenmesini iç hukuka bırakmaktadır. **AB Hukuku**, GDPR'nin 9. maddesinde, özel nitelikli kişisel verilerin ("hassas veriler" olarak da adlandırılmaktadır) işlenmesine ilişkin ayrıntılı bir rejim öngörmektedir. Bu veriler, ırk veya etnik köken, siyasi görüş, dini veya felsefi inanç ve sendika üyeliğine ilişkin bilgilerin yanı sıra, gerçek bir kişiyi şüpheye yer bırakmayacak şekilde tanımlamaya elverişli genetik ve biyometrik veriler ile bir kişinin cinsel yaşamı veya cinsel yönelimi ve sağlığı ile ilgili verileri teşkil etmektedir. Kural olarak, hassas verilerin işlenmesi yasaktır.[414]

Bununla birlikte, regülasyonun 9 (2) maddesinde söz konusu yasağa ilişkin, hassas verilerin işlenmesine ilişkin hukuka uygunluk hallerini teşkil eden sınırlı sayıda istisna hali düzenlenmiştir. Bu istisnalar aşağıdaki hallerde söz konusu olacaktır:

- veri sahibini açık rızasının bulunması;
- veri işlemenin, kar amacı gütmeyen siyasi, felsefi, dini veya sendikal bir kuruluş tarafından, meşru faaliyetleri sırasında e yalnızca (eski) üyeleriyle veya bu tür amaçlar için düzenli olarak temas eden kişilere yönelik olarak gerçekleştirilmesi;
- veri sahibi tarafından alenileştirilen kişisel verilerin işlenmesi;
- kişisel verilerin işlenmesinin:
    - İstihdam, sosyal güvenlik ve sosyal koruma bağlamında veri sorumlusunun veya veri sahibinin yükümlülüklerinin yerine getirilmesi ve belirli hakların kullanılması;
    - veri sahibinin ya da başka bir gerçek kişinin hayati çıkarlarının korunması (veri sahibinin rızasını açıklayamadığı hallerde);
    - hukuki taleplerin oluşturulması, kullanılması veya korunması veya mahkemelerin kendi yargı yetkileri dahilinde hareket etmesi;
    - koruyucu veya mesleki hekimlik: "çalışanın çalışma kapasitesinin ölçülmesi, tıbbi teşhis, sağlık ve sosyal hizmetler ile tedavi, veya sağlık çalışanı ile tesis

[413] AİHM, Y/Türkiye, No. 648/10, 17 Şubat 2015.
[414] Eski Veri Koruma Direktifi, Md. 7 (f), şimdi Avrupa Genel Veri Koruma Regülasyonu, Md. 9 (1).

edilen bir sözleşmeye dayalı olarak Birlik veya Üye Ülke kanunları uyarınca sağlık veya sosyal bakım sistem ve hizmetlerinin yönetimi";

- kamu yararına yönelik arşiv oluşturma, bilimsel veya tarihi araştırma yapılması,
- halk sağlığı alanındaki kamu menfaati nedeniyle; veya
- önemli kamu yararı nedenleri için gerekli olması.

Özel nitelikli kişisel verilerin işlenmesi, mesleki sır saklama yükümlülüğüne tabi bir sağlık çalışanı ile yapılan sözleşmeler hariç olmak üzere, veri sahibi ile sözleşmeye dayalı bir ilişkinin varlığı, hassas verilerin hukuka uygun olarak işlenmesi için yasal bir temel olarak değerlendirilmemektedir.[415]

Veri sahibinin açık rızası

AB Hukuku uyarınca, hassas veri olup olmadığına bakılmaksızın, herhangi bir kişisel verinin hukuka uygun olarak işlenmesinin ilk şartı, veri sahibinin rızasıdır. Hassas verilerin işlendiği durumlarda, rızanın açık olması zorunludur. Bununla birlikte, Birlik veya Üye Ülke kanunları kapsamında, özel nitelikli kişisel verilerin işlenmesine ilişkin yasağın veri sahibi tarafından kaldırılmamasını sağlayabilir.[416] Bu, örneğin kişisel verilerin işlemesi, veri sahibi için olağandışı riskler teşkil ettiği durumlarda söz konusu olabilecektir.

İş hukuku veya sosyal güvenlik ve sosyal koruma hukuku

AB Hukuku uyarınca, kişisel verilerin işlemesinin, veri sorumlusu veya veri sahibinin istihdam veya sosyal güvenlik alanındaki yükümlülüklerinin yerine getirilmesi veya haklarının kullanılması için gerekli olması durumunda 9. maddenin 1. fıkrasının öngördüğü yasak kaldırılabilecektir. Ancak, veri işleme faaliyetine, veri sahibinin temel hak ve menfaatlerine uygun koruma sağlayan AB yasaları, iç hukuk düzenlemeleri veya ulusal yasalar uyarınca akdedilen toplu bir anlaşma ile izin verilmiş olması gerekmektedir.[417] Bir kuruluş tarafından tutulan özlük kayıtları, GDPR ve ilgili iç hukukta belirtilen belirli koşullar altında hassas kişisel verileri içerebilir. Hassas verilere ilişkin örnekler arasında sendika üyeliği veya sağlık bilgileri yer alabilir.

Veri sahibinin veya bir başkasının hayati çıkarları

AB Hukuku uyarınca, hassas olmayan verilerde olduğu gibi, hassas veriler, veri sahibinin veya başka bir gerçek kişinin hayati çıkarları nedeniyle işlenebilir.[418] Kişisel veri işlenmesi bir başkasının hayati çıkarları temeline dayanıyorsa, bu meşru zemin ancak böyle veri işlemenin "açıkça başka bir yasal temele dayanmıyor ise" öne sürülebilir.[419] Bazı durumlarda, kişisel verilerin işlenmesi, hem bireysel hem de kamu menfaatlerini örneğin; insani yardım amacıyla kişisel verilerin işlenmesi koruyabilecektir.[420]

---

[415] Avrupa Genel Veri Koruma Regülasyonu, Md. 9 (2) (h) ve (i).
[416] *Age*., Md. 9 (2) (a).
[417] Avrupa Genel Veri Koruma Regülasyonu, Md. 9 (2) (b).
[418] *Age*., Md. 9 (2) (c).
[419] *Age*., Başlangıç Hükmü 46.
[420] *Age*.

Hassas verilerin işlenmesinin bu temel kapsamında hukuka uygun kabul edilmesi için, veri sahibinin rızasının istenmesi imkansız olmalıdır. Örneğin; veri sahibinin bilincinin açık olmadığı ya da bulunamadığı veya ulaşılamadığı için veri sahibinin rızasını istemenin imkânsız kabul edilecektir. Başka bir deyişle, kişi fiilen veya hukuken rıza verememektedir.

Hayır kurumları veya kâr amacı gütmeyen kuruluşlar

Siyasi, felsefi, dini veya sendikal amaçlı vakıfların, derneklerin veya diğer kâr amacı gütmeyen kuruluşların meşru faaliyetleri sırasında da kişisel verilerin işlenmesine izin verilmektedir. Bununla birlikte, kişisel verilerin işlenmesi yalnızca kuruluşun üyeleri veya eski üyeleri veya kuruluş ile düzenli temas halinde olanlar kişilere yönelik olmalıdır.[421] Hassas veriler, veri sahibinin izni olmaksızın bu kuruluşların dışındakilere açıklanamaz.

Veri sahibi tarafından açıkça alenileştirilmiş veriler

GDPR'nin 9 (2) (e) maddesi veri sahibi tarafından açıkça alenileştirilen verilere yönelik olmak kaydıyla; kişisel verilerin işlenebileceğini öngörmektedir. "Veri sahibi tarafından açıkça alenileştirilmiş olma" tanımı Regülasyon kapsamında yapılmamış olsa da; hassas verilerin veri sahibinin açık rızası olmaksızın işlenememesine ilişkin kuralın bir istisnasını teşkil ettiği için veri sahibinin kişisel verilerini bilinçli olarak alenileştirmiş olması gerektiği şeklinde yorumlanmalıdır. Böylelikle, televizyonda kapalı devre kayıt yapan bir kameradan alınan görüntülerin arasında, binayı tahliye etmeye çalışırken yaralanmış olan itfaiyecinin bulunduğu bir videonun yayınlanması durumunda, itfaiyecinin açıkça kişisel verilerini alenileştirdiğinden söz edilemeyecektir. Öte yandan, itfaiyecinin olayı açıklamaya ve video ve fotoğrafları kamuya açık bir internet sayfasında yayınlamaya karar vermesi halinde, kişisel verilerin alenileştirilmesine yönelik kasıtlı ve olumlu bir eylemde bulunduğu değerlendirilebilecektir. Kişisel verilerin alenileştirilmesinin rıza verildiği anlamına gelmeyeceği, ancak özel nitelikli kişisel verilerin işlenmesine izin verildiği durumlardan birini teşkil ettiğine dikkat çekilmelidir.

Veri sahibi tarafından kişisel verilerinin alenileştirilmesi, veri sorumlularının veri koruma mevzuatı kapsamındaki yükümlülüklerinin yerine getirilmesinden muaf tutulduğu anlamına gelmemektedir. Örneğin, amaç sınırlaması prensibi, kişisel verilerin alenileştirilmesi durumunda da uygulanmaya devam edecektir.[422]

Hukuki talepler

GDPR[423] uyarınca, özel nitelikli kişisel verilerin, "hukuki taleplerin oluşturulması, kullanılması veya korunması amacıyla dava süreçlerinde veya mahkeme dışı idari işlemler kapsamında işlenmesine"[424] izin verilmektedir. Bu durumda, kişisel verilerin işlenmesi, sırasıyla hukuki bir talebin oluşturulması, kullanılması veya korunmasına yönelik olması gerekmekte ve bu uyuşmazlığın tarafı konumunda olanlar tarafından ileri sürülebilecektir.

Yargı yetkileri çerçevesinde hareket ettikleri sırada mahkemeler, hukuki bir uyuşmazlığın çözümlenmesi amacıyla özel nitelikli kişisel verileri işleyebilir.[425] Bu bağlamda işlenen özel nitelikli kişisel verilere, nesep bağı kurulurken genetik veriler veya suçun mağdurunun

[421] *Age*., Md. 9 (2) (d).
[422] Madde 29 Çalışma Grubu (2013), amaç sınırlamasına ilişkin 3/13 sayılı Görüş, WP 203, Brüksel, 2 Nisan 2013, p. 14.
[423] *Age*., Md. 9 (2) (f).
[424] Avrupa Genel Veri Koruma Regülasyonu, Giriş, Başlangıç Hükmü 52.
[425] *Age*.

yaralanmasına ilişkin delillerin bir kısmının sağlık durumuna ilişkin olması örnek verilebilecektir.

Üstün kamu yararına ilişkin sebepler

GDPR'nin 9 (2) (g) maddesine göre, aşağıdaki hallerde; Üye Ülkeler hassas verilerin işlenmesine ilişkin ilave koşullar öngörebilecektir:

- üstün kamu yararına ilişkin sebeplerle kişisel verilerin işlenmesi;
- Avrupa mevzuatı veya ulusal kanunlarda öngörülmüşse;
- Avrupa mevzuatı ya da ulusal yasaların orantılı, kişisel verilerin korunması hakkına saygılı olması ve veri sahibinin hak ve menfaatlerinin korunması için uygun ve belirli önlemler sağlaması.[426]

Buna ilişkin en önemli örneklerden biri, elektronik sağlık dosyası sistemleridir. Bu tür sistemler, bir hastanın tedavisi sırasında sağlık hizmeti sağlayıcıları tarafından toplanan sağlık verilerinin, hastanın hizmet aldığı diğer sağlık hizmeti sağlayıcılarına, genellikle ülke çapında, geniş bir ölçekte sunulmasını sağlamaktadır.

Madde 29 Çalışma Grubu, hastalara ilişkin kişisel verilerin işlenmesine yönelik mevcut yasal kurallar altında bu tarz sistemlerin kurulmasının vuku bulamayacağı sonucuna varmıştır.[427]Ancak, elektronik sağlık dosya sistemlerinin var olmaları "üstün kamu yararı sebeplerine" dayanıyorsa mümkündür.[428] Bu durum bu tarz sistemlerin kurulması, sistemin güvenli bir şekilde çalıştırılmasını sağlayan gerekli önlemleri de içeren belirli bir hukuki dayanağın varlığını gerektirmektedir.[429]

Hassas verilerin işlenmesi için diğer gerekçeler

GDPR, hassas verilerin işlenmesini aşağıdaki durumlar için gerekli olması durumunda mümkün kılmaktadır:[430]

- koruyucu veya meslek hekimliğine ilişkin amaçlar kapsamında, çalışanın çalışma kapasitesinin değerlendirilmesi, tıbbi teşhis, sağlık veya sosyal bakım veya tedavi sağlanması veya Birlik veya Üye Ülke yasası temelinde veya bir sağlık uzmanıyla sözleşmeye bağlı olarak sağlık veya sosyal bakım sistemlerinin ve hizmetlerinin yönetimi;
- kamu sağlığı alanında, sağlığa yönelik ciddi sınır ötesi tehditlere karşı korumanın sağlanması veya AB ya da Üye Ülke kanunları uyarınca sağlık hizmetleri ile tıbbi ürünler veya tıbbi cihazların yüksek kalite ve güvenlik standartlarını sağlanması. İlgili kanunlar, veri sahibinin haklarının korunması için uygun ve belirli önlemlerin alınmasını sağlamalıdır;

---

[426] *Age*., Md. 9 (2) (g).
[427] Madde 29 Çalışma Grubu (2007), Elektronik sağlık kayıtlarında sağlığa ilişkin kişisel verilerin işlenmesiyle ilgili Çalışma Belgesi (EHR), WP 131, Brüksel, 15 Şubat 2007. Ayrıca bakınız Avrupa Genel Veri Koruma Regülasyonu, Md. 9 (3).
[428] Avrupa Genel Veri Koruma Regülasyonu, Md. 9 (2) (g).
[429] Madde 29 Çalışma Grubu (2007), Elektronik sağlık kayıtlarında sağlığa ilişkin kişisel verilerin işlenmesiyle ilgili Çalışma Belgesi (EHR), WP 131, Brüksel, 15 Şubat 2007.
[430] Avrupa Genel Veri Koruma Regülasyonu, Md. 9 (2) (h), (i) ve (j).

- Birlik veya Üye Ülke kanunları uyarınca, arşivleme, bilimsel veya tarihi araştırma veya istatistiki çalışmaların gerçekleştirilmesi. İlgili kanun, izlenen amaç ile orantılı olmalı, kişisel verilerin korunması hakkının özüne saygı göstermeli ve veri sahibinin hak ve menfaatlerini korumak için uygun ve belirli önlemlerin alınmasını sağlamalıdır.

Ulusal hukuk çerçevesinde ek koşullar

GDPR, aynı zamanda Üye Ülkelerine genetik, biyometrik ve sağlıkla ilgili kişisel verilerin işlenmesiyle ilgili sınırlamalar da dahil olmak üzere ek koşullar getirmesine veya uygulamasına izin vermektedir.[431]

4.2. Veri işleme faaliyetlerinin güvenliğine ilişkin kurallar

Kilit noktalar

- Veri işleme faaliyetinin güvenliğine ilişkin kurallar, veri sorumlusu ve veri işleyen tarafından, veri işleme operasyonlarına yetkisiz müdahale edilmesini önlemek amacıyla uygun teknik ve organizasyonel tedbirlerin alınmasını zorunlu kılmaktadır.
- Gerekli veri güvenliği seviyesi aşağıdakiler doğrultusunda belirlenecektir:
    - belirli bir kişisel verilerin işlenmesi türü için piyasada mevcut olan güvenlik unsurları;
    - maliyetler;
    - Veri sahiplerinin temel hak ve özgürlükleri bakımından kişisel verilerin işlenmesine ilişkin riskler.
- Kişisel verilerin gizliliğinin sağlanması, Avrupa Genel Veri Koruma Regülasyonu'nda belirlenen genel bir prensibin parçası olarak değerlendirilmektedir.

Hem AB hem de Avrupa Konseyi Hukuku uyarınca, veri sorumluları, kişisel verilerin işlenmesinde, bilhassa veri ihlalleri meydana geldiğinde, şeffaf ve hesap verebilir olma yükümlülüğü altındadır. Veri ihlalinin gerçek kişilerin hak ve özgürlükleri için bir risk oluşturmasının muhtemel olmadığı durumlar hariç olmak üzere, bir kişisel veri ihlali durumunda veri sorumlularının denetim makamlarını bilgilendirmesi gerekir. Kişisel veri ihlalinin gerçek kişilerin hak ve özgürlükleri bakımından yüksek risk oluşturmasının muhtemel olduğu durumlarda, veri sahipleri de bu konuda bilgilendirilmelidir.

4.2.1. Veri güvenliğinin unsurları

AB Hukuku'nun ilgili hükümleri uyarınca:

"*Teknolojinin mevcut durumu, uygulama maliyetleri ve işleyişin doğası, kapsamı, bağlamı ve amaçları ile gerçek kişilerin hak ve özgürlükleri bakımından gerçekleşme olasılığı ve ciddiyetini de göz önünde bulundurarak, veri sorumlusu ve veri işleyen, riske uygun bir güvenlik seviyesini tesis etmek için uygun teknik ve organizasyonel tedbirleri uygulamalıdır*

[431] *Age*., Md. 9 (2) (h) ve 9 (4).

[...]."[432]

Bu önlemler diğerlerinin yanı sıra aşağıdakileri de kapsamaktadır:

- kişisel verilerin maskelenmesi ve şifrelenmesi;[433]
- veri işleme sistem ve hizmetinin gizlilik, bütünlük, ulaşılabilirlik ve dirençliliğinin temini;[434]
- veri kaybı durumunda, gecikmeksizin kişisel verilere ulaşılabilirliğin ve erişilebilirliğin geri kazanılması;[435]
- kişisel veri işleme faaliyetlerinin güvenliğinin sağlanmasına yönelik önlemlerin etkinliğinin test edilmesi, ölçülmesi ve değerlendirilmesine ilişkin süreçlerin mevcudiyeti.[436]

Avrupa Konseyi Hukuku'nda da benzer bir hüküm bulunmaktadır:

"*Taraflardan her biri, veri sorumlusunun ve uygulanabilir olduğu durumlarda veri işleyenin kişisel verilerin kazara veya yetkisiz erişim, imha, kayıp, kullanım, değişiklik veya açıklanması gibi risklere karşı uygun güvenlik önlemleri almasını sağlayacaktır."*[437]

AB ve Avrupa Konseyi Hukuku uyarınca, bireylerin hak ve özgürlüklerini etkileyebilecek bir veri ihlali durumunda, veri sorumlusunun bu ihlali denetleyici otoriteye bildirmekle zorunluluğu bulunmaktadır (bakınız Bölüm 4.2.3).

Genellikle, kişisel verilerin işlenmesinde güvenliğin sağlanması amacıyla geliştirilen endüstriyel, ulusal ve uluslararası standartlar da bulunmaktadır. Örneğin, Avrupa Gizlilik Mührü (EuroPriSe), Avrupa veri koruma mevzuatı ile uyumun sağlanmasını kolaylaştırmak amacıyla ürünleri, özellikle de yazılımları onaylama olanaklarını araştıran bir eTEN (Trans-Avrupa Telekomünikasyon Ağları) projesidir. Avrupa Ağ ve Bilgi Güvenliği Ajansı (ENISA), AB'nin, AB Üye Ülkelerinin ve iş dünyasının ağ ve bilgi güvenliği sorunlarını önleme, çözme ve bunlara cevap verme yeteneğini geliştirmek üzere kurulmuştur.[438] ENISA düzenli olarak mevcut güvenlik tehditlerinin analizlerini yayınlamakta ve bunların nasıl ele alınacağına dair tavsiyelerde bulunmaktadır.[439]

Veri güvenliği sadece, donanım ve yazılım gibi doğru araçlara sahip olunması ile sağlanmaz. Ayrıca uygun iç organizasyon kurallarının uygulamaya alınmasını gerektirir. Bu tür iç kuralların ideal olarak aşağıdaki konuları kapsaması gerektiği değerlendirilmektedir:

- özellikle gizlilik yükümlülükleri konusunda, tüm çalışanlara veri güvenliği kuralları ve veri koruma yasası kapsamındaki yükümlülüklere ilişkin düzenli bilginin sağlanması;

---

[432] *Age*., Md. 32 (1).
[433] *Age*., Md. 32 (1) (a).
[434] *Age*., Md. 32 (1) (b).
[435] *Age*., Md. 32 (1) (c).
[436] *Age*., Md. 32 (1) (d).
[437] Modernize Edilmiş Sözleşme 108, Md. 7 (1).
[438] 460 /, OJ 2013 L 165 sayılı Regülasyonu yürürlükten kaldıran, Avrupa Birliği Ağ ve Bilgi Güvenliği Ajansı (ENISA) ile ilgili 21 Mayıs 2013 tarih ve 526/2013 sayılı Avrupa Parlamentosu ve Konsey Regülasyonu.
[439] Örneğin, ENISA (2016), Akıllı Araçların Siber Güvenliği ve Esnekliği. İyi uygulamalar ve öneriler; ENISA (2016), Mobil Ödeme ve Dijital Cüzdan Güvenliği.

- kişisel verilerin işlenmesine, üçüncü taraflara ve veri sahiplerine aktarılmasına ilişkin kararlar başta olmak üzere, kişisel verileri işlenmesine ilişkin, sorumlulukların açık bir şekilde dağıtılması ve yetkilerin açık bir şekilde belirtilmesi;

- kişisel verilerin yalnızca yetkili kişinin talimatlarına göre veya genel olarak belirlenmiş kurallara göre kullanılması;

- erişim yetkilerinin kontrolü de dahil olmak üzere, veri sorumlusunun veya veri işleyenin donanımına ve yazılımına ve bunların bulunduğu yerlere erişimin korunması;

- kişisel verilere erişim yetkilerinin yetkili kişi tarafından verilmiş olduğundan ve uygun belgelerin hazırlandığından emin olunması;

- kişisel verilere elektronik erişim konusunda otomatik protokoller ve iç denetim masası tarafından bu tür protokollerin düzenli kontrollerinin sağlanması (bu nedenle tüm veri işleme faaliyetlerine ilişkin kayıtların oluşturulması gerekir);

- hukuka aykırı veri aktarımlarının gerçekleşmediğinin ispatı amacıyla otomatik erişimden başka aktarım biçimleri için özenli belgeleme süreçlerinin işletilmesi.

Personele yeterli veri güvenliği eğitimlerinin verilmesi de etkili güvenlik önlemlerinin önemli bir unsurudur. Yalnızca kağıt üzerinde değil, uygulamada ve pratikte de (iç veya dış denetimler gibi) uygun önlemlerin alınmasını sağlamak adına doğrulama prosedürleri de uygulanmalıdır.

Bir veri sorumlusu veya veri işleyen tarafından öngörülen güvenlik seviyesini arttırmaya yönelik önlemler arasında; veri koruma görevlileri, çalışanların güvenlik eğitimi, düzenli denetimler, etki testleri ve kalite mühürleri bulunur.

Örnek: I/Finlandiya davasında,[440] başvuru sahibi, kendi sağlık kayıtlarına çalıştığı hastanenin diğer çalışanları tarafından hukuka aykırı bir şekilde erişildiğini ispatlayamamıştır. Bu nedenle, veri koruma hakkının ihlal edildiğine ilişkin iddiası, yerel mahkemeler tarafından reddedilmiştir. AİHM, AİHS'in 8. maddesinin ihlal edildiğine karar vermiştir, nitekim hastanenin sağlık dosyalarına ilişkin kayıt sisteminin "yalnızca son beş başvuruyu ortaya koyması sebebiyle hasta kayıtlarının kullanımını geriye dönük olarak netleştirmek mümkün olmamıştır ve bu bilgiler, dosya arşive geri gönderildikten sonra silinmiştir". Yerel mahkemeler tarafından gereken ağırlık verilmemiş olmasına karşın; Mahkeme, hastanede bulunan kayıt sisteminin, iç hukukta yer alan gereksinimlere uygun olmadığını açıkça tespit etmiştir.

AB, siber güvenlik konusunda AB genelinde uygulanan ilk yasal araç olan ağ ve bilgi sistemlerinin güvenliği hakkındaki Direktif'i (NIS Direktifi)[441] yürürlüğe koymuştur. Direktif, bir yandan siber güvenliği ulusal düzeyde iyileştirmeyi ve diğer yandan AB içindeki iş birliği seviyesini artırmayı amaçlamaktadır. Ayrıca, risklerin yönetilmesi, ağlarının ve bilgi sistemlerinin güvenliğinin sağlanması ve güvenlik olaylarını raporlanması adına (enerji, sağlık, bankacılık, ulaştırma, dijital altyapı vb. sektörlerdeki işletmeciler de dahil olmak üzere) temel hizmet sağlayıcılar ve dijital hizmet sağlayıcılara yükümlülükler getirmektedir.

[440] AİHM, I/Finlandiya, No. 20511/03, 17 Temmuz 2008.
[441] Birlik genelinde ağ ve bilgi sistemlerinin yüksek güvenlik seviyesine ilişkin tedbirler hakkında Avrupa Parlamentosu ve Konseyinin 6 Temmuz 2016 tarih ve (AB) 2016/1148 sayılı Direktifi.

Görünüm

Eylül 2017'de, Avrupa Komisyonu, kurumun NIS Direktifi kapsamındaki yeni yetkinlikleri ve sorumluluklarını göz önünde bulundurarak ENISA'nın yetkilerini yeniden düzenlemeyi amaçlayan bir taslak düzenleme önerisinde bulunmuştur. Taslak düzenlemenin amacı, ENISA'nın görevlerini geliştirmek ve "AB siber güvenlik ekosistemindeki esas nokta" rolünü sağlamlaştırmaktır.[442] Teklif edilen düzenleme, GDPR prensiplerine halel getirilmemeli ve Avrupa siber güvenlik sertifikasyon programlarını oluşturan gerekli unsurları netleştirerek kişisel verilerin güvenliğini de güçlendirmelidir. Buna paralel olarak, Eylül 2017'de, Avrupa Komisyonu, NIS Direktifi'nin 16(8) maddesinde talep edildiği şekilde, dijital servis sağlayıcılarının ağlarının ve bilgi sistemlerinin güvenli olmasını sağlamak için göz önünde bulundurması gereken unsurları belirten bir taslak uygulama düzenlemesi teklifinde bulunmuştur. El kitabının taslağı hazırlanırken, bu iki teklifle ilgili tartışmalar devam etmekteydi.

4.2.2. Gizlilik

AB hukuku uyarınca, GDPR, kişisel verilerin gizliliğini genel bir ilkenin parçası olarak kabul etmektedir.[443] Kamuya açık elektronik iletişim hizmetleri sağlayıcılarının gizliliği sağlamaları gerekir. Ayrıca, ilgili hizmet sağlayıcıları sağladıkları hizmetin güvenliğini korumakla da yükümlüdür.[444]

Örnek: Bir sigorta şirketinin bir çalışanı, müşteri olduğunu söyleyen ve sigorta sözleşmesiyle ilgili bilgi talep eden birinden işyerinde bir telefon alır. Müşterilerin verilerini gizli tutma görevi, çalışanın kişisel verileri açıklamadan önce en az asgari güvenlik önlemlerini almasını gerektirir. Bu, örneğin aramayı müşterinin dosyasında yazılı bir telefon numarasına yönlendirmeyi teklif ederek yapılabilir.

Madde 5 (1) (f) uyarınca, kişisel veriler, yetkisiz veya hukuka aykırı şekilde işlenmeye, verilerin kaybına, imhasına veya zarara uğramasına karşı ('bütünlük ve gizlilik') uygun teknik veya organizasyonel tedbirler kullanılarak korunmasını sağlayacak şekilde işlenmelidir.

Madde 32 uyarınca, veri sorumlusu ve veri işleyen, yüksek güvenlik düzeyini tesis etmek amacıyla teknik ve organizasyonel önlemler almak zorundadır. Bu tür önlemler arasında, diğerlerinin yanı sıra kişisel verilerin maskelenmesi ve şifrelenmesi, devam eden gizlilik, bütünlük, işlemenin mevcudiyeti ve esnekliğini sağlama yeteneği, önlemlerin etkinliğinin değerlendirilmesi ve test edilmesi ve fiziksel veya teknik bir olay durumunda işlemi geri yükleme yeteneği sayılabilecektir. Ek olarak, onaylanmış bir davranış kuralı veya onaylanmış bir sertifikasyon mekanizması ile uyumluluk; bağlılık, bütünlük ve gizlilik ilkelerinin sağlanması için bir unsur olarak kullanılabilir. Bunun yanında, GDPR'nin 28. maddesine göre, veri sorumlusu ile veri işleyen arasındaki sözleşme kapsamında, veri işleyenin organizasyonu dahilinde kişisel verileri işlemeye yetkili kişilerin gizlilik taahhüdünde bulunduğunu veya yasal olarak kendilerine uygulanabilir bir gizlilik yükümlülüğü altında bulunduğu temin edilmelidir.

Gizlilik yükümlülüğü, bir veri sorumlusu veya veri işleyenin bir çalışanı olarak değil, özel bir

[442] Avrupa Parlamentosu ve Konseyi'nin ENISA, "AB Siber Güvenlik Ajansı" ve yürürlükteki 526/2013 sayılı Regülasyonu ve Bilgi ve İletişim Teknolojileri siber güvenlik sertifikasını (Siber Güvenlik Yasası) yürürlükten kaldırmasına ilişkin Teklif, COM(2017)477, 13 September 2017, p. 6.
[443] Avrupa Genel Veri Koruma Regülasyonu, Md. 5 (1) (f).
[444] Gizlilik ve elektronik haberleşme hakkında Direktif, Md. 5 (1).

kişi olarak kendi yetkisi dahilinde kişisel verilerin elde edildiği durumlarını kapsamaz. Bu durumda, GDPR'nin 32 ve 28'inci maddeleri geçerli olmayacaktır, nitekim kişisel verilerin özel kişilerce kullanımı, bu tür bir kullanımın aynı konut muafiyeti olarak adlandırılan istisna halinin sınırları içerisinde olduğu durumlarda, düzenlemenin kapsamından tamamen muaftır.[445] Aynı konut muafiyeti, kişisel verilerin "tamamen kişisel ya da aynı konut içerisindeki faaliyetleri sırasında gerçek bir kişi tarafından" kullanılmasını teşkil etmektedir.[446] Bununla birlikte, ABAD'nin Bodil Lindqvist[447] davasında verdiği karar uyarınca, bu muafiyetin, özellikle verilerin aktarılması ile ilgili olarak dar yorumlanması gerekir. Özellikle, aynı konut muafiyetinin kapsamı, kişisel verilerin internet üzerindeki sınırsız sayıda alıcıya yayınlanmasına veya profesyonel veya ticari yönleri olan işleme faaliyetlerine kadar genişlemeyecektir (dava hakkında daha fazla bilgi için, Bölüm 2.1.2, 2.2.2 ve 2.3.1'e bakınız).

"İletişimin gizliliği", özel kanuni düzenleyeme tabi olan, bir başka gizlilik başlığıdır. E-Gizlilik Direktifi kapsamında, elektronik haberleşmenin gizliliğinin sağlanması için öngörülen özel kurallar, Üye Ülkeler'in, kullanıcılar dışındaki kişilerin veya kullanıcıların rızası olmaksızın, iletişimlerini ve ilgili meta verileri dinlemelerine, kaydetmelerine, saklamalarına veya başka şekillerde müdahale etmelerine veya takip edilmesine izin vermelerini yasaklar.[448] İç hukuk düzenlemeleri, yalnızca ulusal güvenlik, savunma, suçların önlenmesi veya tespit edilmesi sebepleriyle ve bu gibi tedbirlerin izlenen amaçlar için gerekli ve orantılı olması kaydıyla bu prensibe istisnalar getirebilir.[449] Bu kurallar, ileride yürürlüğe girecek olan e-Gizlilik Regülasyonu kapsamında da geçerli olacaktır, ancak e-Gizlilik ile ilgili yasal düzenlemenin kapsamı, kamuya açık elektronik iletişim hizmetlerinin yanı sıra, OTT hizmetleri (örneğin; mobil uygulamalar) aracılığıyla yapılan iletişimleri de kapsayacak şekilde genişletilecektir.

Avrupa Konseyi Hukuku uyarınca, gizlilik yükümlülüğü, Modernize Edilmiş Sözleşme 108'in veri güvenliğine ilişkin 7 (1) maddesinde tanımlanan veri güvenliği kavramında belirtilmiştir.

Veri işleyenler için gizlilik, verilerin yetkilendirme olmaksızın üçüncü kişilere veya diğer alıcılara aktarılmaması anlamına gelmektedir. Veri sorumlusu veya veri işleyenin çalışanları için gizlilik ise, kişisel verileri yalnızca yetkili üstlerinin talimatları doğrultusunda kullanmalarını gerektirir.

Gizlilik yükümlülüğü, veri sorumluları ve bunlar adına veri işleyenler arasındaki tüm sözleşmelere dahil edilmelidir. Ek olarak, veri sorumluları ve veri işleyenler, genellikle ilgi çalışanlar ile tesis edilecek olan iş sözleşmelerine gizlilik yükümlülüğüne ilişkin hükümler eklemek suretiyle çalışanları için yasal bir gizlilik yükümlülüğü oluşturarak özel önlemler almak zorunda kalacaklardır.

Mesleki gizlilik yükümlülüğünün ihlali, birçok AB Üye Ülkesinde ve 108 Sayılı Sözleşme'ye Taraf Devletlerde ceza hukuku kapsamında cezalandırılabilir.

4.2.3. Kişisel veri ihlali bildirimleri

Kişisel veri ihlali, kişisel verilerin kazayla veya yasadışı bir şekilde tahrip edilmesine, kaybedilmesine, değiştirilmesine veya yetkisiz olarak ifşa edilmesine veya işlenmiş kişisel

[445] Avrupa Genel Veri Koruma Regülasyonu, Md. 2 (2) (c).
[446] *Age*.
[447] ABAD, C-101/01, Bodil Lindqvist'e karşı cezai kovuşturma, 6 Kasım 2003.
[448] Gizlilik ve elektronik haberleşme hakkında Direktif, Md. 5 (1).
[449] *Age*., Md. 15 (1).

verilere erişimine yol açan bir güvenlik ihlali anlamına gelir.[450] Şifreleme gibi yeni teknolojilerinin artık veri işleme güvenliğini sağlamak için daha fazla olanak sunmasına rağmen, veri ihlalleri hala yaygın bir olgudur. Veri ihlallerinin nedenleri, bir kuruluş içinde çalışan kişiler tarafından yapılan hatalardan, bilgisayar korsanları ve siber suç örgütleri gibi dış tehditlere kadar değişebilir.

Veri ihlalleri, ihlal sonucunda kişisel verileri üzerindeki kontrollerini kaybeden kişilerin mahremiyetine ve veri koruma haklarına zarar verebilir. İhlaller kimlik hırsızlığı veya dolandırıcılığa, finansal kayıplara veya maddi zararlara, mesleki gizlilikle korunan kişisel verilerin gizliliğinin kaybolmasına ve veri sahiplerinin itibar kaybına neden olabilir. 2016/679 sayılı Tüzük uyarınca Kişisel veri ihlali bildirimi ile ilgili Kılavuzunda, Madde 29 Çalışma Grubu, ihlallerin kişisel veriler üzerinde üç tür etkisinin olabileceğini belirtmektedir: ifşa, kayıp ve/veya değişiklik.[451] Bölüm 4.2'de açıklandığı gibi veri işleme güvenliğini sağlamak için önlemler alma yükümlülüğüne ek olarak, ihlaller meydana geldiğinde, veri sorumlularının bunları gereği gibi ve zamanında ele almaları da aynı derecede önemlidir.

Denetim otoriteleri ve bireyler çoğu zaman bir veri ihlalinin yaşandığından haberdar değildir ve bu, bireylerin kendilerini ihlalin sonuçlardan korumak için gerekli adımları atmalarını engellemektedir. Bireylerin haklarını korumak ve veri ihlallerinin etkilerini sınırlandırmak için, AB ve Avrupa Konseyi bazı durumlarda veri sorumlularına bildirimde bulunma zorunluluğu getirmektedir.

Avrupa Konseyi Modernize Edilmiş Sözleşme 108 uyarınca, Sözleşmenin Tarafları, asgari olarak, veri sorumlularını, veri sahiplerinin haklarına ciddi şekilde etki edebilecek veri ihlallerini yetkili denetim otoritesine bildirmekle zorunlu tutmaktadır. Bu bildirim "gecikmeksizin" yapılmalıdır.[452]

AB hukuku, bildirimlerin zamanlamasını ve içeriğini düzenleyen ayrıntılı bir prosedür barındırmaktadır.[453] Buna göre, veri sorumluları, belirli veri ihlallerini gecikmeksizin ve her halde ihlalden haberdar olunmasından sonraki 72 saat içinde denetleme makamlarına bildirmelidir. 72 saatlik süre aşılırsa, bildirim, gecikme için bir açıklama eşliğinde yapılmalıdır. Veri sorumluları yalnızca, ihlalin ilgili kişilerin hak ve özgürlükleri üzerine bir risk oluşma ihtimalinin bulunmadığını kanıtlayabildikleri durumlarda bildirim yapma yükümlülüğünden muaf tutulacaktır.

Düzenleme, denetim otoritesinin gerekli önlemleri alabilmesi adına bildirim sırasında sunulacak asgari bilgileri belirlemektedir.[454] Bildirimde, asgari olarak veri ihlalinin ve kategorilerin niteliğinin bir tanımı ve etkilenen veri sahiplerinin yaklaşık sayısı, ihlalin olası sonuçları ve veri sorumlusunun bu sonuçları kontrol edebilmek ve hafifletmek için aldığı önlemleri içermelidir. Ek olarak, yetkili denetim otoritesinin olası ilave bilgi taleplerini iletebilmesi adına, veri koruma görevlisinin veya başka bir irtibat noktasının adı ve iletişim bilgileri sağlanmalıdır.

---

[450] Avrupa Genel Veri Koruma Regülasyonu, Md. 4 (12). Ayrıca bakınız, Madde 29 Çalışma Grubu (2017), 2016/679 sayılı Tüzük uyarınca Kişisel veri ihlali bildirimi ile ilgili kurallar, WP250, 3 Ekim 2017, s. 8.
[451] Madde 29 Çalışma Grubu (2017), 2016/679 sayılı Tüzük uyarınca Kişisel veri ihlali bildirimi ile ilgili kurallar, WP250, 3 Ekim 2017, s. 6.
[452] Modernize Edilmiş Sözlşeme 108, Md. 7 (2); Modernize Edilmiş Sözleşme 108 Açıklayıcı Raporu, paras. 64-66.
[453] Avrupa Genel Veri Koruma Regülasyonu, Md. 33 ve 34.
[454] *Age*. Md. 33 (3).

Bir veri ihlalinin bireylerin hak ve özgürlükleri için yüksek risk oluşturması muhtemel ise, veri sorumluları ihlale uğrayan bireyleri (veri sahiplerini) gecikmeksizin bilgilendirmelidir.[455] Veri ihlaline ilişkin açıklamalar da dahil olmak üzere, veri sahiplerine yapılacak bilgilendirmeler açık ve sade bir dille hazırlanmalı ve denetleme makamlarına yapılacak bildirimler için gerekenlere benzer bilgiler içermelidir. Bazı durumlarda, veri sorumluları bu tür ihlalleri veri sahiplerine bildirme yükümlülüğünden muaf tutulabilirler. Muafiyetler özellikle şifreleme gibi yöntemlerle ihlalden etkilenen verilerin bu verilere erişme yetkisi bulunmayan kişilere anlaşılmaz kılınmış olması gibi veri sorumlusunun uygun teknik ve organizasyonel koruma önlemleri aldığı durumlarda uygulanır. Veri sahiplerinin haklarına gelebilecek zararların önüne geçmek adına ihlalden sonra veri sorumlusu tarafından önlem alınması da, veri sorumlusunu, veri sahiplerini bilgilendirme yükümlülüğünden muafiyetini sağlayabilir. Son olarak, bildirimin yapılması veri sorumlusu için orantısız bir çaba gerektiriyorsa, kamuya açık duyurular veya benzeri yöntemler gibi diğer yollarla da veri sahiplerine ihlallere ilişkin bilgi verilebilir.[456]

Veri ihlallerini denetleme otoritelerine ve veri sahiplerine bildirme yükümlülüğünün veri sorumluları üzerinde olacağı düzenlenmiştir. Ancak, veri işlemesinin bir veri sorumlusu veya veri işleyen tarafından yapılmasından bağımsız olarak veri ihlalleri meydana gelebilir. Bu nedenle, veri işleyenlerin de veri ihlallerini bildirmelerini sağlamak esastır. Bu durumda, veri işleyenler veri ihlallerini gecikmeksizin veri sorumlusuna bildirmelidirler.[457] Bunun üzerine veri sorumlusu, yukarıda belirtilen kurallara ve zaman sınırlamaları dahilinde, denetim otoritelerini ve etkilenen veri sahiplerine bildirim yükümlülüğünü yerine getirecektir.

4.3. Hesap verilebilirliğe ve uyumluluğu arttırmaya ilişkin kurallar

Kilit noktalar

- Kişisel verilerin işlenmesinde hesap verilebilirliği sağlamak için, veri sorumluları ve veri işleyenler kendi sorumlulukları altında yürütülen işleme faaliyetlerinin kayıtlarını tutmalı ve istendiğinde bunları denetleyici otoritelere sunmalıdır.

- Avrupa Genel Veri Koruma Regülasyonu, uyumluluğu artırmak için çeşitli araçlar sunmaktadır:

    - belirli durumlarda veri koruma görevlilerinin atanması;

    - bireylerin hak ve özgürlükleri için yüksek risk oluşturacak olan veri işleme faaliyetlerinin başlamasından önce bir etki değerlendirmesinin yapılması;

    - etki değerlendirmesinde, veri işlemenin azaltılması mümkün olmayan riskler oluşturacağı tespit edilirse önceden ilgili denetim otoritesine danışılması;

    - GDPR'nin çeşitli sektörlerdeki kişisel veri işleme faaliyetlerine uygulanmasını belirleyen veri sorumluları ve veri işleyenler için davranış kuralları;

    - mühür ve işaretler gibi sertifikasyon mekanizmaları.

[455] *Age*., Md. 34.
[456] *Age*., Md. 34 (3) (c).
[457] *Age*., Md. 33 (2) (2).

- Avrupa Konseyi yasası, Modernize Edilmiş Sözleşme 108'ye uyumu sağlamak için benzer enstrümanlar içermektedir.

Hesap verilebilirlik prensibi, Avrupa'da veri koruma kurallarının uyumu sağlamak adına özellikle önemlidir. Veri sorumlusu, veri koruma kurallarına uyulmasından sorumludur ve bu uygunluğu kanıtlayabilmelidir. Hesap verilebilirlik, yalnızca bir ihlal gerçekleştikten sonra devreye girmemelidir. Aksine, veri sorumluları, veri işlemenin tüm aşamalarında yeterli veri yönetimi politikalarını takip etmek için proaktif bir yükümlülüğe sahiptir. Avrupa veri koruma hukuku, veri sorumlularına, veri işlemenin yasaya uygun olarak gerçekleştirilmesini sağlamak ve uygunluğun sağlandığını kanıtlayabilmek için teknik ve organizasyonel önlemleri almasını zorunlu tutmaktadır. Bu önlemler arasında veri koruma görevlilerinin atanması, veri işlemeye ilişkin kayıtların ve belgelerin saklanması ve gizlilik etki değerlendirmelerinin yapılması yer almaktadır.

4.3.1. Veri koruma görevlileri

Veri Koruma Görevlileri (DPO'lar), kişisel veri işleme faaliyetleri yürüten kuruluşlarda veri koruma kurallarına uygunluk hususunda tavsiyelerde bulunan kişilerdir. Bu kişiler, uyuma destek oldukları için 'hesap verilebilirliğin temel taşlarından biridir', aynı zamanda denetim otoriteleri, veri sahipleri ve atandıkları kuruluş arasında aracı görevi görürler.

Avrupa Konseyi hukuku uyarınca, Modernize Edilmiş Sözleşme 108'in 10 (1) maddesi, veri sorumluları ve veri işleyenler hakkında genel bir hesap verilebilirlik sorumluluğu getirmektedir. Bu, veri sorumlularının ve veri işleyenlerin sözleşmede öngörülen veri koruma kurallarına uymak için gerekli tüm önlemleri almalarını ve kontrolleri altında gerçekleşen verilerin işlenmesi sırasında sözleşmenin hükümlerine uygun hareket edildiğin kanıtlayabilmelerini gerektirir. Sözleşme, veri sorumlularının ve veri işleyenlerin alması gereken önlemleri açıkça belirlemese de Modernize Edilmiş Sözleşme 108'in Açıklayıcı Raporu, DPO atanmasının, uyuma yardımcı olacak bir önlem olacağını değerlendirmektedir. DPO'lara görevlerini yerine getirmeleri için gerekli tüm araçlar sağlanmalıdır.[458]

Avrupa Konseyi yasalarının aksine, AB'de bir DPO atanması her zaman veri sorumlularının ve veri işleyenlerin takdirine bağlı değildir, belirli koşullarda zorunlu tutulmuştur. GDPR, DPO'nun yeni yönetişim sisteminde kilit bir rol oynadığını kabul etmekte ve DPO'nun atanması, pozisyonu, görevleri ve vazifeleri ile ilgili ayrıntılı hükümler içermektedir.[459]

GDPR, üç özel durumda bir DPO'nun atanmasını zorunlu kılmaktadır: veri işlemesini bir kamu otoritesinin veya organının gerçekleştirdiği durumlarda; veri sorumlusunun veya veri işleyenin temel faaliyetlerinin, veri sahiplerinin büyük ölçekte düzenli ve sistematik olarak izlenmesini gerektiren veri işleme faaliyetlerinden oluştuğu durumlarda veya temel faaliyetlerin, ceza mahkumiyeti ve suçlarıyla ilgili özel kategorili verilerin veya kişisel verilerin büyük çapta işlenmesinden oluştuğu durumlarda.[460] "Büyük ölçekte sistematik izleme" ve "temel faaliyetler" gibi terimler yönetmelikte tanımlanmamış olsa da, Madde 29 Çalışma Grubu bunların nasıl yorumlanmaları gerektiğine dair kılavuzlar yayınlamıştır.[461]

[458] Modernize Edilmiş Sözleşme 108 Açıklayıcı Raporu, para. 87.
[459] Avrupa Genel Veri Koruma Regülasyonu, Md. 37-39.
[460] *Age*., Md. 37 (1).
[461] Madde 29 Çalışma Grubu (2017), Veri Koruma Görevlileri ("DPO'lar") hakkında Kılavuzlar, WP 243 rev.01, en son 5 Nisan 2017 tarihinde revize edilmiş ve uygulanmıştır.

Örnek: Sosyal medya şirketleri ve arama motorları, veri sahiplerini düzenli ve sistematik bir şekilde izlerken genellikle veri sorumlusu olarak değerlendirilecektir. Bu tür şirketlerin iş modeli, çok miktarda kişisel verinin işlenmesine dayanır ve hedefli reklamcılık hizmetlerini sunarak ve şirketlerin sitelerde reklam vermelerini sağlar ve bu yolla önemli gelir elde ederler. Hedefli reklamcılık, demografiye ve tüketicilerin önceki satın alma geçmişine veya davranışlarına dayanarak reklamlar yerleştirmenin bir yoludur. Bu nedenle, veri sahiplerinin çevrimiçi alışkanlıklarının ve davranışlarının sistematik olarak izlenmesini gerektirmektedir.

Örnek: Hastaneler ve sağlık sigorta şirketleri, faaliyetleri özel nitelikli kişisel verilerin işlenmesinden oluşan tipik veri sorumlusu örnekleridir. Bir bireyin sağlığına ilişkin bilgileri ve verileri, hem Avrupa Konseyi hem de AB hukuku uyarınca özel nitelikli kişisel veridir ve daha gelişmiş koruma gerektirmektedir. AB hukuku ayrıca genetik ve biyometrik verileri özel nitelikli kişisel veri olarak kabul etmektedir. Sağlık kuruluşları ve sigorta şirketleri büyük çapta bu tür verileri işlediklerinden, GDPR kapsamında bir veri koruma görevlisi atamaları gerekmektedir.

Ek olarak, GDPR'nin 37. maddesinin 4. fıkrası uyarınca öngörülen üç tane zorunluluk dışında kalan durumlarda, veri sorumlusu, veri işleyen veya veri sorumluları ya da veri işleyen kategorilerini temsil eden diğer birlik veya kurumların, AB veya Üye Devlet yasalarının gerektirdiği durumlarda zorunlu olmak üzere veri koruma görevlisi belirleyebilirler. [462]

Diğer tüm kuruluşlar yasal olarak DPO tayin etmek zorunda değildirler. Bununla birlikte GDPR, hem veri sorumlularının ve veri işleyenlerin bir DPO'yu gönüllü olarak seçmelerine izin verir, hem de Üye Devlet'lerin DPO atanması zorunluluğunu öngörülen düzenlemelerden daha fazla kuruluş için getirmesini engellememektedir.

Veri sorumlusu bir DPO'yu atadığında, kuruluş içinde "kişisel verilerin korunmasına ilişkin tüm konulara, zamanında ve doğru şekilde dahil olması"nı sağlamalıdır.[463] Örneğin, DPO'lar veri koruma etki değerlendirmelerini gerçekleştirme konusunda tavsiyede bulunmaya ve bir kuruluştaki veri işleme faaliyetlerinin kayıtlarını oluşturmaya ve muhafaza etmeye dahil edilmelidir. DPO'ların görevlerini etkin bir şekilde yerine getirebilmeleri için, veri sorumluları ve veri işleyenler onlara finansal kaynak, altyapı ve ekipman dahil gerekli kaynakları sağlamalıdırlar. DPO'lara fonksiyonlarını yerine getirmeleri için yeterli zamanın sağlanmasını ve uzmanlıklarını geliştirmelerini sağlayacak devamlı eğitimler vermesini ve veri koruma hukukundaki tüm gelişmeleri takip edip uygulamalarını sağlaması gibi ek gereklilikler içermektedir. [464]

GDPR, DPO'ların bağımsız bir şekilde hareket etmesini sağlamak için bazı garantiler ön görmüştür. Veri sorumluları ve veri işleyenler, verilerin korunması ile ilgili görevlerini yerine getirirken, DPO'ların şirketten en yüksek seviyeye sahip kişiler de dahil olmak üzere herhangi bir talimat almadıklarından emin olması gerekmektedir. [465] Örneğin; DPO'nun veri sorumlularına veya veri işleyenlere veri koruma etki değerlendirmesi yapılmasını tavsiye ettiği durumlarda sebep, verilerin işlenmesinin veri sahipleri için yüksek risk ile sonuçlanabileceğini düşünüyor olmasıdır. Şirket, DPO'nun tavsiyelerine katılmayabilir, doğru olduğunu düşünmüyor ve sonuç olarak etki değerlendirmesine devam etmemeye karar verebilir. Şirket tavsiyeyi görmezden gelebilir ancak DPO'yu görevden alamaz ve cezalandıramaz.

[462] Avrupa Birliği Genel Veri Koruma Regülasyonu, Madde 37/f.3 ve 4
[463] A,e.g., Madde 38/f.1
[464] Madde 29 Çalışma Grubu (WP 29) (2017), Veri Koruma Görevlisi Hakkında Rehber (DPO's), WP 243 rev.01, son revize edilme ve kabul edilme tarihi 5 Nisan 2017, para. 3.1
[465] Avrupa Birliği Genel Veri Korum Tüzüğü, Madde 38F.2 ve 3

Son olarak, DPO'ların görevleri ve yapması gerekenler GDPR'nin 39. maddesinde ayrıntılı olarak açıklanmıştır. Bunlara mevzuat uyarınca yükümlülüklerini yerine getiren şirketleri ve çalışanları bilgilendirmek, tavsiyede bulunmak ve veri işleme faaliyetlerinde yer alan denetim ve eğitim personeli aracılığıyla AB ve yerel veri koruma kurallarına uyumu sağlamak için gözlem yapmak da dahildir. DPO'lar ayrıca denetim otoriteleri ile iş birliği yapmalı ve örneğin veri ihlali gibi verilerin işlenmesi ile ilgili konularda otoriteler için temas noktası olarak hareket etmelidirler.

AB kurumları ve otoriteleri tarafından, işlenen kişisel veriler ile ilgili olarak 45/2001 sayılı Tüzük, her Birlik kurumunun ve kuruluşunun DPO ataması gerektiğini öngörmektedir. DPO'lar, bahsi geçen düzenlemedeki hükümlerin AB kurum ve kuruluşlarında doğru şekilde uygulanmasını ve hem veri sahiplerinin hem de veri sorumlularının hakları ve yükümlülükleri hakkında bilgi verilmesini sağlamakla görevlendirilmiştir.[466] DPO'lar ayrıca EDPS'den gelen taleplere cevap vermek ve gerektiğinde onlarla iş birliği yapmakta sorumludur. GDPR'a benzer şekilde, 45/2001 sayılı Tüzük, DPO'ların görevlerini yerine getirirken bağımsız olmaları ile ilgili ve gerekli personel ve kaynakların sağlanması ihtiyacına ilişkin hükümler içermektedir.[467] AB kurumu veya kuruluşu (veya bu kuruluşların bölümleri) herhangi bir işlem gerçekleştirmeden önce DPO'ya bunu bildirmeli ve tüm verilerin işlenmesi faaliyetinin bildirimlerinin kaydını tutmaları gerekmektedir. [468]

4.3.2 Veri İşleme Faaliyetlerinin Kayıtları

Uyumluluğun sağlanması ve hesap verilebilirlik için şirketlerin yasal olarak faaliyetlerini belgelemesi ve kaydetmesi gerekir. Şirketlerin uyum gösterebildiğini ispat etmesi ve hesap verebilmesi için hukuka uygun olarak faaliyetlerini belgelemesi ve kaydetmesi gerekir. Önemli bir örnek ise, vergi hukuku ve denetimler gereği tüm şirketlerin kapsamlı dokümantasyon yapması ve kayıt tutmalarının zorunlu olmasıdır. Diğer hukuk alanlarında özellikle kişisel verilerin korunması hukuku kapsamında kayıt tutmak veri koruma kurallarına uyumu sağlamak için önemlidir. Bu nedenle AB hukuku veri sorumlularının veya onların temsilcilerinin kendi sorumlulukları altında yürüttükleri işleme faaliyetlerinin kaydını tutması gerektiğini belirtir.[469] Bu yükümlülük denetleyici otoritelerin gerektiğinde işlemlerin hukuka uygunluğunu onaylamaları için gerekli belgelere sahip olmalarını için düzenlenmiştir.

Belgelenen bilgiler aşağıdakileri içermelidir;

- Veri sorumlusunun ve uygun olan hallerde ortak veri sorumlularının, veri temsilcisinin, Veri Koruma Görevlisi'nin (DPO) adı ve iletişim bilgileri

- Veri işleme amacı

- Veri sahibi ve veri işleme ile ilgili olan kişisel verilerin kategorilerinin açıklaması

- Kişisel verilerin paylaşıldığı veya ileride paylaşılabilecek olan taraflar

- Kişisel verilerin üçüncü bir ülkeye veya uluslararası kuruluşa aktarımının olması veya aktarılacak olmasının bilgisi

[466] Bkz. Madde 24/f.1
[467] 45/2001 (EC) sayılı Tüzük, Madde 24/f.6 ve 7
[468] A.e.g., Madde 25 ve 26
[469] Avrupa Birliği Genel Veri Koruma Regülasyonu.

- Mümkün olduğu durumlarda, farklı kategorilerdeki verilerin silinmesi için öngörülen süre sınırları ve veri işlemenin güvenliğini sağlamak için alınan teknik tedbirlere yönelik genel açıklama[470]

GDPR kapsamında veri işleme faaliyetlerinin kayıt altına alınması yükümlülüğü veri sorumlusu ile aynı zamanda veri işleyenle de ilgilidir. Bu gelişme önemlidir çünkü düzenlemenin kabul edilmesinden önce veri sorumlusu ile veri işleyen arasında imzalanan sözleşmenin öncelikli olarak veri işleyenin sorumlulukları belirtilmektedir. Onların kayıt tutma yükümlülükleri artık kanunla öngörülmektedir.

GDPR bu yükümlülüğe istisna getirmiştir. Kayıt tutma zorunluluğu 250 kişiden daha az kişiyi istihdam eden bir işletme veya kuruluş (veri sorumlusu veya veri işleyen) için geçerli değildir. Ancak istisna ilgili kuruluşun veri sahibinin hak ve özgürlüklerine risk teşkil edecek veri işleme faaliyeti gerçekleştirmemesi, veri işlemenin nadiren gerçekleşmesi ve Madde 9 (1)'de belirtilen özel nitelikli kişisel verileri içermemesi veya Madde 10'da belirtilen mahkumiyet kararı ve ceza gerektiren suçlara ilişkin kişisel veri olmaması şartına tabidir.

Veri işleme faaliyetinin kayıtlarının tutulması veri sorumlularının ve veri işleyenlerin düzenlemeye uygun şekilde hareket edildiğini kanıtlamalarını sağlamaktadır. Ayrıca denetim otoritelerinin veri işlemenin hukuka uygun gerçekleştiğini gözlemleyebilmelerini sağlamalıdır. Bir denetim otoritesinin bu kayıtlara erişimi talep etmesi halinde, veri sorumlusu ve veri işleyen bu kişilerle iş birliği yapmak ve kayıtları erişilebilir hale getirmekle yükümlüdür.

4.3.3 Veri Koruma Etki Değerlendirmesi ve Ön İnceleme

Veri işleme faaliyeti doğası gereği kişilerin haklarına karşı risk oluşturmaktadır. Kişisel veriler kaybolabilir, yetkisiz kişilere açıklanabilir veya hukuka aykırı işlenebilir. Doğal olarak, bu riskler veri işlemenin niteliğine ve kapsamına bağlı olarak değişir. Özel nitelikli kişisel verilerin işlenmesini içeren geniş çaplı faaliyetler, örneğin küçük bir şirket çalışanlarının adreslerinin ve şahsi telefon numaralarının işlenmesi faaliyetinin potansiyel riskleri ile karşılaştırıldığında, veri sahibine yönelik çok daha yüksek bir risk oluşturmaktadır.

Yeni teknolojilerin ortaya çıkması ve veri işlemenin gittikçe karmaşık hale gelmesi ile, veri sorumluları veri işleme faaliyetine başlamadan önce amaçlanan işlemin olası etkisini inceleyerek bu riskleri dikkate almalıdır. Bu, kuruluşların riskleri önceden belirlemesini, dikkate almasını ve azaltmasını sağlar ve veri işlemenin sonucunda kişiler üzerindeki olumsuz etki olması olasılığını önemli ölçüde sınırlandırır.

Veri koruma etki değerlendirmeleri hem Avrupa Konseyi hem de AB hukuku uyarınca öngörülmüştür. Avrupa Konseyi'nin yasal çerçevesinden, Modernize Edilmiş 108 sayılı Sözleşme'nin 10.maddesini 2. Fıkrası ile veri sorunlularının ve veri işleyenlerin "amaçlanan veri işlemenin 108 sayılı Sözleşme'nin bu tür veri işleme faaliyetine başlamasından önce veri sahiplerinin temel hak ve özgürlükleri üzerinde oluşabilecek muhtemel etkisini inceleme"nin ve değerlendirmenin ardından, veri işlenme faaliyetini bu veri işlemesine bağlı riskleri önleyecek veya bu riskleri en aza indirecek şekilde tasarlanmaları gerektiği belirtilmiştir.

AB hukuku, GDPR'nin kapsamına giren veri sorumlularına benzer olarak daha ayrıntılı bir yükümlülük getirmiştir. Madde 35 uyarınca veri işlenmesi bireylerin hak ve özgürlükleri için yüksek bir risk oluşturabileceği durumlarda etki değerlenmesi yapılması gerekmektedir. Tüzük,

[470] a.g.e, DPO'ların görevlerinin tüm listesi için 45/2001 (EC) sayılı Tüzük, Madde 30/f.1

risk olasılığının nasıl değerlendirileceğini tanımlamamıştır daha ziyade bu risklerin neler olabileceğini göstermiştir.[471] Yüksek riskli olarak kabul edilen ve bunun için önceden bir etki değerlendirmesinin gerekli olduğu durumlar aşağıdadır:

- kişisel veriler, bireylerle ilgili şahsi yönlerin sistematik ve kapsamlı şekilde değerlendirilmesinin ardından, gerçek kişilerle ilgili kararlar almak için işlenmesi (profilleme);

- ceza mahkumiyeti ve güvenlik tedbirleri ile ilgili olan verilerin veya hassas verilerin geniş kapsamlı işlenmesi

- halka açık alanlarda geniş kapsamlı, sistematik şekilde izlenmeyi içeren veri işleme faaliyetleri.

Denetim otoriterleri, etki değerlendirmelerinin gerekli olduğu veri işleme faaliyetlerinin bir listesini çıkarmalı ve yayınlamalıdır. Ayrıca bu zorunluluktan muaf tutulan veri işleme faaliyetlerinin de bir listesi oluşturulabilir. [472]

Etki değerlendirmesinin gerekli olduğu durumlarda, veri sorumluları veri işlemenin gerekliliğini, orantılılığını ve bireylerin hakları üzerinde oluşabilecek riskleri değerlendirmelidir. Etki değerlendirmesi ayrıca tespit edilen riskler için planlanan güvenlik tedbirlerini de içermelidir. Listeleri oluşturmak için, Üye Devletler'in denetim otoritelerinin birbirleriyle ve Avrupa Veri Koruma Kurulu ile iş birliği yapmaları gerekmektedir. Bu AB genelindeki etki değerlendirmesi gerektiren faaliyetlere tutarlı bir yaklaşımı sağlayacaktır ve veri sorumluları bulundukları konuma bakılmaksızın benzer şartlarla karşılaşacaklardır.

Etki değerlendirmesini takiben, veri işlemenin bireylerin hakları üzerinde yüksek risk oluşturacağı ve riski azaltmak için herhangi bir tedbir alınmadığı ortaya çıkarsa, veri sorumlusu veri işleme faaliyetine başlamadan önce ilgili denetim otoritesine başvurması gerekir. [473]

Madde 29 Çalışma Grubu, veri koruma etki değerlendirmeleri ve veri işlemenin yüksek riskle sonuçlanıp sonuçlanmayacağının nasıl belirleneceğine dair rehberler yayınlamıştır. [474] Belirli bir durumda veri koruma etki değerlendirmesinin gerekli olup olmadığını tespit etmeye yardımcı olmak için dokuz kriter geliştirilmiştir: [475] (1) değerlendirme veya puanlama; (2) yasal veya benzeri önemli etkiye sahip otomatik karar verme; (3) sistematik izleme; (4) hassas veri; (5) geniş kapsamda işlenmiş veri; (6) eşleşen veya birleştirilmiş veri setleri; (7) veri sahibine ilişkin hassas veriler; (8) yenilikçi kullanım veya teknolojik veya kurumsal çözümler uygulamak; (9) veri işlemenin kendi içinde "veri sahibinin bir hakkını kullanmasını veya bir hizmeti kullanmasını veya sözleşme yapmasını" önlediğinde. Madde 29 Çalışma Grubu, iki kriterden daha azını karşılayan veri işleme faaliyetlerinin düşük risk seviyesi oluşturduğunu ve veri koruma değerlendirmesinin gerekmediğini ancak, iki veya daha fazla kriteri karşılayanların böyle bir değerlendirme gerektireceği konusunda genel bir kural getirmiştir. Bir veri koruma

[471] GDPR, Giriş, Recital 75
[472] a.g.e, Madde 35/f.4 ve 5
[473] a.g.e, Madde 36/f.1; Madde 29 Çalışma Grubu (Art. 29 WP) (2017), Veri Koruma Etki Değerlendirmesi (DPIA) Rehberleri ve 2016/679, WP 248 rev.01, Brüksel, 4 Ekim 2017 tarihli Yönetmelik uyarınca veri işlemenin "yüksek risk ile sonuçlanma olasılığı" olup olmadığı belirlemek.
[474] Madde 29 Çalışma Grubu (Art. 29 WP) (2017), Veri Koruma Etki Değerlendirmesi (DPIA) Rehberleri ve 2016/679, WP 248 rev.01, Brüksel, 4 Ekim 2017 tarihli Yönetmelik uyarınca veri işlemenin "yüksek risk ile sonuçlanma olasılığı" olup olmadığı belirlemek.
[475] a.g.e ss. 9-11

etki değerlendirmesinin gerekli olup olmadığının net olmadığı durumlarda, Madde 29 Çalışma Grubu böyle bir değerlemenin yapılmasını önermektedir çünkü "veri sorumlularının veri koruma kanunlarına uymasına yardımcı olan yararlı bir araçtır". [476] Yeni bir veri işleme teknolojisi kullanıldığında, veri koruma etkisi değerlendirmesinin yapılması önemlidir. [477]

4.3.4 Davranış Kuralları

Davranış kuralları, çeşitli endüstri sektörlerinde kendi sektörlerine özgün olarak GDPR'nin uygulanmasını ana hatlarıyla göstermek ve belirtmek için kullanılmasını ifade eder. Kişisel verileri işleyenler ve veri sorumluları için bu tür kuralları oluşturmak AB veri koruma kurallarının uygulanmasını geliştirir ve bu veri koruma kurallarına uyumluluğu büyük ölçüde artırır. Sektör üyelerinin uzmanlıkları sayesinde pratik ve takip edilmesi muhtemel çözümler bulunacaktır. Bu tür kuralların veri koruma kanununun etkin uygulanmasındaki önemini onaylayan GDPR, Üye Devler'e, denetim otoritelerine, Komisyon'a ve Avrupa Veri Koruma Kurulu'na düzenlemenin AB genelinde doğru uygulanmasına katkıda bulunmayı amaçlayan davranış kurallarının oluşturulmasını teşvik etmek için çağrıda bulunmaktadır. [478] Bu kurallar; kişisel verilerin toplanması, veri sahiplerine ve kamuya sağlanacak bilgiler ve veri sahiplerinin haklarının kullanılması gibi konular da dahil olmak üzere, belirli sektörlerde bu düzenlemenin uygulamasını belirleyebilir.

Davranış kurallarının, GDPR uyarınca belirlenen kurallarla uyumlu olmaları için, bu kurallar kabul edilmeden önce yetkili denetim otoritesine sunulması gerekmektedir. Denetim otoritesi daha sonra taslak kuralların düzenlemelere uygunluk sağlayıp sağlamadığına dair bir görüş verir ve kuralın uygun koruma sağladığını düşünürse kuralı onaylar. [479] Denetim otoriteleri onaylanmış davranış kurallarını ve onaylarının dayandığı kriterleri yayınlamalıdır. Bu taslak davranış kuralları birkaç Üye Devlet'teki veri işleme faaliyetleri ile ilgili olduğu durumlarda yetkili denetim otoritesi, taslak kuralı, değişikliği veya eklemeyi onaylanmadan önce Avrupa Veri Koruma Kurulu'na ibraz ederken bu kuralın GDPR ile uyumluluğuna dair bir görüş sunmalıdır. Komisyon, yasaları uygulayarak kendisine sunulan onaylanmış davranış kurallarını Birlik içinde genel geçerliliği olduğuna karar verebilir.

Davranış kuralına bağlılık hem veri sahipleri hem de veri sorumluları ve veri işleyenlere önemli faydalar sunar. Bu tür kurallar, belirli sektörlere yasal zorunluluk ve veri işleme faaliyetlerinin şeffaflığını artıran ayrıntılı rehberlik sağlar. Veri sorumluları ve veri işleyenler aynı zamanda, bu kuralları AB yasalarına uyumluluğunun ispatı mümkün kanıt ve faaliyetlerinde veri korumayı önceliklendiren ve taahhüt eden bir kuruluş olarak toplumsal imajını güçlendirmenin bir aracı olarak kullanabilirler. Onaylanmış davranış kuralları, bağlayıcı ve uygulanabilir yükümlülüklerle birlikte, kişisel verileri üçüncü ülkelere aktarmak için uygun güvenlik tedbirleri olarak kullanılabilir. Davranış kuralları ile bağlı olan kuruluşların gerçekten bu kurallara uymasını sağlamak için, uyumluluğu sağlamak ve gözlemlemek adına özel bir kurum (ilgili denetim otoritesi tarafından onaylanmış) oluşturulabilir. Kurumun görevlerini etkin bir şekilde yerine getirmek için, bağımsız olması, davranış kurallarına göre düzenlenen konularda uzmanlığının kanıtlanmış olması ve kuralların ihlaliyle ilgili şikâyetlerin ele alınmasını sağlayacak şeffaf prosedürlere ve yapıya sahip olması gerekir. [480]

Avrupa Konseyi yasalarına göre, Modernize Edilmiş 108 sayılı Sözleşme, ulusal yasalarla

[476] a.g.e. s.9
[477] a.g.e
[478] Avrupa Birliği Genel Veri Koruma Regülasyonu (GDPR), Madde 40/f.1
[479] a.g.e., Madde 41/f.1 ve f.2
[480] a.g.e, Madde 41/f.1 ve f.2

garanti altına alınan veri koruma seviyesinin, doğru uygulama kuralları veya mesleki davranış kuralları gibi ihtiyari düzenleme önlemleriyle faydalı bir şekilde güçlendirilmesini sağlamaktadır. Bununla birlikle, bunlar yalnızca Modernize Edilmiş 108 sayılı Sözleşme uyarınca ihtiyari tedbirleri teşkil eder: bu tür tedbiri almak için her ne kadar tavsiye edilse de herhangi bir yasal zorunluluk yoktur ve bu tür tedbirler sözleşmeye tam olarak uyulmasını sağlamak için yeterli değildir.[481]

4.3.5 Belgelendirme

Davranış kurallarına ek olarak, belgelendirme mekanizmaları ve veri koruma mühürleri ve işaretleri, veri sorumlularının ve işleyenlerin GDPR'a uyumluluğunu gösterebileceği başka yollardır. Bu amaçla, Tüzük bazı kurumların veya denetim otoritelerinin belge verebileceği ihtiyari bir belgelendirme sistemi sağlar. Belgelendirme mekanizmasına uygun hareket etmeyi seçen veri sorumluları ve veri işleyenlerin kullandığı belgeler, mühürler ve işaretler, veri sahiplerinin bir kuruluşun veri işleme için koruma düzeyini hızlı bir şekilde değerlendirmesini sağladığı için kurumlar daha fazla görünürlük ve güvenilirlik kazanabilir. Önemle belirtmek gerekir ki, bir veri sorumlusunun veya veri işleyenin böyle bir belgeye sahip olması, Tüzük'ün tüm şartlarına uyma sorumluluğunu ve yükümlülüklerini azaltmaz.

4.4 Tasarımdan İtibaren Veri Koruması ve Başlangıçtan İtibaren Veri Koruması

Tasarımdan itibaren veri koruması

AB hukuku, veri sorumlularının veri koruma ilkelerini etkin bir şekilde uygulaması için düzenlemelerin şartlarını yerine getirmesini ve veri sahiplerinin haklarını korumak için gerekli önemleri almasını öngörmüştür.[482] Bu tedbirler hem veri işleme sırasında hem de veri işleme yöntemini belirlerken uygulanmalıdır. Bu önemlerin uygulanmasında veri sorumlusunun en son teknolojiyi, uygulama maliyetlerini, kişisel veri işlemenin niteliğini, kapsamını ve amaçlarını ile veri sahibinin hak ve özgürlükleri üzerinde oluşacak riskleri ve zararı dikkate alması gerekir.[483]

Avrupa Konseyi hukuku, veri sorumlularının ve veri işleyenlerin, kişisel verilerin işlenmesi işleminin başlamasından önce bu işlemenin veri sahiplerinin hak ve özgürlükleri üzerindeki muhtemel etkisini değerlendirmeleri gerektiğini belirtir. Ek olarak, veri sorumluları ve veri işleyenler, veri işlerken bu hak ve özgürlükleri zedeleyebilecek herhangi bir riski önleyecek ve en aza indirecek şekilde veri işlenme faaliyetini tasarlamak ve veri işlemenin her aşamasında kişisel verileri koruma hakkının etkilerini dikkate alarak teknik ve idari tedbirleri uygulamakla yükümlüdür. [484]

Başlangıçtan İtibaren Veri Koruması

AB hukuku, veri sorumlularının başlangıçtan itibaren yalnızca veri işleme amacı için gerekli olan kişisel işlenmesini sağlamak için uygun tedbirlerin alınmasını gerektirir. Bu yükümlülük,

---

[481] Modernize Edilmiş 108 sayılı Sözleşmenin Açıklayıcı Raporu, prg.33
[482] Avrupa Birliği Genel Veri Koruma Regülasyonu, Madde 25/f.1
[483] Bkz. Madde 29 Çalışma Grubu (WP 29) (2017), Veri Koruma Etki Değerlendirmesi (DPIA) Kılavuzları ve veri işlemenin 2016/679, WP 248 rev.01, 4 Ekim 2017 tarihli amaçları için "yüksek risk doğurabilecek" olup olmadığının belirlenmesi. Ayrıca bkz. ENISA (2015), Tasarımdan İtibaren (plandan tekniğe kadar) Gizlilik ve Veri Koruması, 12 Ocak 2015
[484] Modernize Edilmiş 108 sayılı Sözleşme, Madde 10/f.2 ve f.3, 108 sayılı Sözleşme'nin Açıklayıcı Raporu, paragraf 89

toplanan kişisel verilerin miktarı, kişisel veri işlemenin kapsamı, verilerin saklama süresi ve erişilebilirlik için uygulanmalıdır.[485] Bu tür tedbirlere örnek vermek gerekirse; veri sorumlularının tüm çalışanlarının veri sahiplerinin kişisel verilerine erişememesi gerekir. EDPS tarafından daha fazla rehber olabilecek "Zorunlu Araçlar" dokümanı oluşturulmuştur.[486]

Avrupa Konseyi hukuku, veri sorumlularının ve veri işleyenlerin, kişisel verilerin korunması hakkının etkilerini göz önünde bulundurarak teknik ve idari tedbirleri almalarını ve kişisel verilerin işlendiği tüm aşamalarda teknik ve idari tedbirleri almalarını gerekir. [487]

2016 yılında, ENISA hali hazırda mevcuttaki gizlilik araç ve hizmetleri hakkında bir rapor yayınlamıştır. [488] Diğer değerlendirmeler ile karşılaştırma yapılacak olursa; bu değerlendirme iyi olan veya yetersiz olan gizlilik uygulamalarının göstergesi olan kriter ve parametre içeriği sunmaktadır. Bazı kriterler, maskeleme ve tasdik edilmiş belgelendirme mekanizması gibi doğrudan GDPR hükümleri ile ilgili olmasına karşın, tasarımdan itibaren ve başlangıçtan itibaren gizliliği sağlamak için yenilikçi çözümler sunmaktadır. Örnek vermek gerekirse; kullanılabilirlik kriteri, doğrudan gizlilikle ilgili olmamakla birlikte, bir gizlilik aracının veya hizmetinin daha geniş çapta benimsenmesini sağlayabildiğinden gizliliği artırabilir. Ek olarak, gizlilik araçlarının olgunluk ve istikrarlılık kriterleri yani bir aracın zaman içinde geliştiği ve gizlilikle ilgili mevcut veya yeni zorluklara cevap vermesi, çok önemlidir. Diğer gizlilikle ilgili geliştirilmiş teknolojiler, örnek vermek gerekirse; güvenli iletişim kapsamında, uçtan uca şifreleme (mesajları okuyabilen kişilerin yalnızca iletişim kuran kişiler olması durumundaki iletişim); alıcı-sunucu şifreleme (bir alıcı ile sunucu arasında kurulan işletim kanalını şifrelemek); kimlik doğrulama (iletişim kuran tarafların kimliklerini doğrulama); ve anonim iletişim (hiçbir üçüncü tarafın iletişim kuranları belirleyememesi) dahildir.

5. Bağımsız Denetim

[485] Avrupa Birliği Genel Veri Koruma Regülasyonu, Madde 35/f.2
[486] Avrupa Veri Koruma Denetçisi (EDPS), (2017), Necessity Toolkit, Brüksel, 11 Nisan 2017
[487] Modernize Edilmiş 108 sayılı Sözleşme, Madde 10/f.3, 108 sayılı Sözleşme'nin Açıklayıcı Raporu, paragraf 89
[488] ENISA, PET'in kontrol matrisi: Çevrimiçi ve mobil gizlilik araçlarını değerlendirmek için sistematik yaklaşım, 20 Aralık 2016

AB	Ele Alınan Konular	Avrupa Konseyi
Madde 8/f.3, Tablo Avrupa Birliği'nin İşleyişi Hakkında Antlaşma**, Madde 16/f.2** Avrupa Birliği Genel Veri Koruma Regülasyonu**, Madde 51-59** **ABAD, C-518/07**, Avrupa Komisyonu v. Almanya Federal Cumhuriyeti **[GC], 2010** **ABAD, C-614/10,** Avrupa Komisyonu v. Avusturya Cumhuriyeti **[GC], 2012** **ABAD, C-288/12,** Avrupa Komisyonu v. Macaristan **[GC], 2014** **ABAD, C-362/14,** Maximillian Schrems v. Veri Koruma Komisyonu **[GC], 2015**	**Denetim otoriteleri**	**Modernize Edilmiş 108 sayılı Sözleşme, Madde 15**
Avrupa Birliği Genel Veri Koruma Regülasyonu, Madde 60-67	**Denetim Otoriteleri Arasında İş birliği**	**Modernize Edilmiş 108 sayılı Sözleşme, Madde 16-21**
Avrupa Birliği Genel Veri Koruma Regülasyonu, Madde 68-76	**Avrupa Veri Koruma Kurulu**	

Bağımsız denetim Avrupa veri koruma hukuku için esaslı unsurdur. Hem AB hem de Avrupa Konseyi yasaları, bağımsız denetim otoritelerinin varlığını, bireylerin kişisel verilerinin işlenmesinde ilgili hak ve özgürlüklerinin etkin bir şekilde korunmasında vazgeçilmez olarak görmektedir. Veri işlemek şu anda ve her daim olacaktır ve bireylerin anlaması için giderek daha karmaşık halde geldiğinden, bu yetkililer dijital çağın gözlemcileridir. AB'de, bağımsız denetim otoritelerinin varlığı, AB'nin birincil hukukunda yer alan kişisel verilerin korunması hakkının en temel unsurlarından biri olarak kabul edilir. Avrupa Birliği Temel Haklar Bildirgesi'nin 8. maddesinin 3. fıkrası uyarınca TFEU'nun 16. maddesinin 2. fıkrası uyarınca kişisel verilerin korunmasının temel bir hak olarak kabul edilir ve veri koruma

kurallarına uymanın bağımsız bir otorite tarafından kontrol altına alınması gerektiği onaylanmaktadır.

Veri koruma yasası için bağımsız denetimin önemi, içtihat ile de kabul edilmiştir.

Örnek: Schrems Kararı'nda, ABAD, Edward Snowden'ın ABD Ulusal Güvenlik Otoritesi'nin kitlesel gözetim davranışlarına ilişkin açıklamaları ışığında, kişisel verilerin ilk EUSS Güvenli Liman Anlaşması'nda Amerika Birleşik Devletleri'ne (USA) aktarılmasının AB veri koruma yasasına uygun olup olmadığı konusunda endişe duyuyordu.

Kişisel verilerin ABD'ye aktarılması, 2000 yılında kabul edilen bir Avrupa Komisyonu kararı uyarınca kişisel verilerin AB'den ABD'ye temelinde kişisel verilerin yeterli düzeyde korunmasını sağlayan "the Safe Harbour (Güvenli Liman)" düzenlemesi kapsamında kendisini tasdik eden ABD kuruluşlarına aktarılmasına dayanmaktadır. Başvuranın Snowden'ın açıklamalarından sonraki veri aktarımlarının hukukiliği konusundaki şikayetinin incelenmesi istendiğinde İrlanda denetim otoritesi, Komisyon'un ABD veri koruma rejiminin yeterliliği konusundaki kararının Safe Harbour ilkelerine ("Güveli Liman Kararı") yansıyacağı gerekçesiyle şikayeti daha fazla incelemesini engellediğinden reddetmiştir. Bununla birlikte ABAD, yeterli düzeyde koruma sağlayan üçüncü ülkelere veri aktarımına izin veren bir Komisyon kararının olmasının ulusal denetim otoritelerinin yetkilerini ortadan kaldırmadığını veya azaltmadığını belirtmiştir. ABAD, bu otoritelerin veri koruma konusundaki AB kurallarına uyumu gözlemleme ve sağlama yetkilerinin AB'nin birincil hukukundan, özellikle Bildirge'nin m.8/f.3 ve TFEU'nın m.16/f.2 hükümlerinden kaynaklandığını belirtmiştir. "Bağımsız denetim otoritelerinin kurulması bu nedenle […] kişisel verilerin işlenmesi ile ilgili olarak bireylerin korunmasının temel unsurudur." [489]

Bu sebeple ABAD, kişisel verilerin aktarılmasının bir Komisyon'un vereceği yeterlilik kararına tabi olduğu durumlarda bile, bir şikayetin ulusal denetim otoritesine iletildiği durumlarda, otoritenin şikayeti titizlikle incelemesi gerektiğine karar vermiştir. Denetim otoritesi, şikayetin asılsız olduğunu tespit ederse şikayeti reddedebilir. Böyle bir durumda ABAD, etkili bir yargı yoluna başvurma hakkının; bireylerin Komisyon kararının geçerliliği ile ilgili ön karar için konuyu ABAD'a taşıyarak ulusal mahkemelerinden önce böyle bir karara itiraz edilebilmesi olduğunu belirtmiştir. Denetim otoritesinin şikayetin sağlam bir nedene dayandığını düşünmekte ise yasal işlemlerde bulunabilmeli ve konuyu ulusal mahkemelere sevk edebilmelidir. Ulusal mahkemeler, Komisyon'un yeterlilik kararının geçerliliğine karar verme yetkisine sahip olan tek organ olduğu için olayı ABAD'ye sevk edebilir. [490]

Ardından ABAD, aktarım sisteminin AB veri koruma kurallarına uygun olup olmadığını tespit etmek için Güvenli Liman Kararı'nın geçerliliğini incelemiştir. Güvenli Liman Kararı'nın 3. maddesi uyarınca ulusal denetim otoritelerinin (Veri Koruma Direktifi kapsamında izin verilen) ABD'deki kişisel verilerin yetersiz düzeyde korunması durumunda veri aktarımını önlemek için harekete geçme yetkisini sınırlandırdığını tespit edilmiştir. Bağımsız denetim otoritelerinin veri koruma yasalarına uyumluluğunun sağlanmasındaki önemine bakıldığında, ABAD, Veri Koruma Direktifi uyarınca ve Bildirge ışığında yorumlandığında Komisyon'un bu şekilde bağımsız denetim otoritelerinin yetkilerini sınırlamaya yetkisinin olmadığını belirtmiştir. Denetim otoritelerinin yetkilerinin sınırlandırılması, ABAD'ın Güvenli Liman Kararı'nı geçersiz kılmasının sebeplerinden biriydi.

Dolayısıyla Avrupa hukukuna göre etkili veri koruma sağlaması için önemli bir mekanizma olan bağımsız denetim gereklidir. Bağımsız denetim otoriteleri, gizlilik ihlali durumunda veri sahiplerinin ilk temas noktasıdır. [491] AB hukuku ve Avrupa Konseyi hukuku uyarınca, denetim otoritelerinin kurulması zorunludur. Her iki hukuki çerçeve de bu otoritelerin görevlerini ve yetkilerini GDPR'da yer alanlarla

[489] CJUE, C-362/14, Maximillian Schrems v. Veri Koruma Komisyonu [GC], 6 Ekim 2015, paragraf 41.
[490] a.g.e., paras. 53-66
[491] Avrupa Birliği Genel Veri Koruma Regülasyonu, Madde 13/f.2/d

aynı şekilde tanımlar. Kural olarak denetim otoriteleri, AB hukuku ve Avrupa Konseyi hukuku uyarınca aynı şekilde fonksiyonunu yerine getirmelidir. [492]

5.1 Bağımsızlık

AB hukuku ve Avrupa Konseyi hukuku uyarınca her bir denetim otoritesinin görevlerini ve yetkilerini yerine getirirken tamamen bağımsız hareket etmesi gerekir. [493] Denetim otoritesinin ve onların üyelerinin yanı sıra doğrudan veya dolaylı dışarıdan etkilenen personelin bağımsızlığı, veri korunması hakkındaki konularında karar verirken tarafsızlığın güvence altına alınmasında esastır. Yalnızca bir denetim otoritesinin oluşturulmasını sağlayan mevzuat altındaki özel hükümler değil, aynı zamanda otoritenin örgütsel yapısının da bağımsızlığını desteklemesi gerekir. 2010 yılında ABAD – ilk defa – veri koruma denetim otoritelerinin hangi ölçüde bağımsız olmaları gerektiğini incelemiştir. Önemle vurgulanan örneklerde ABAD'ın nasıl "tam bağımsızlığın" anlamını tanımlandığı yer almaktadır.

Örnek: Avrupa Komisyonu v. Federal Almanya Cumhuriyeti,[494] kararında Avrupa Komisyonu, ABAD'dan Almanya'nın verilerin korunmasını sağlamaktan sorumlu denetim otoritelerinin "tam bağımsızlığı" gerekliliğini yanlış bir şekilde kendi hukukuna aktardığını ve dolayısıyla Veri Koruma Direktifi'nin madde 28/f.1 uyarınca yükümlülüklerini yerine getirmediğinin tespit edilmesini istemiştir. Komisyon'un görüşüne göre, Almanya'nın veri koruma yasalarına uyumun sağlanması için farklı federal eyaletlerde (Länder(ülke)) kişisel veri işlemlerini gözlemleyen denetim otoritelerini bulundurması bağımsızlık şartını ihlal etmiştir.

ABAD, "tam bağımsızlığa sahip" sözcüklerinin, gerçek lafzına, AB Veri Koruma hukukunun amaçlarına ve düzenine dayanarak yorumlanması gerektiğini vurgulamıştır. [495]ABAD, denetim otoritelerinin kişisel veri işlemeyle ilgili hakların "koruyucuları" olduğunu vurgulamıştır. Dolayısıyla, onların Üye Devlet'lerdeki kuruluşları, "kişisel verilerin işlenmesi konusunda bireylerin korunmasının temel unsuru" olarak değerlendirilmektedir. [496]ABAD, "denetim otoritelerinin yükümlülüklerini yerine getirirken objektif ve tarafsız davranması gerekmektedir. Bu amaçla, kamu yetkililerinin doğrudan veya dolaylı etkisi de dahil olmak üzere herhangi bir dış etkenden uzak durmaları gerekmektedir." sonucuna varmıştır. [497]

ABAD ayrıca "tam bağımsızlık" anlamının, AB Kurumları Veri Koruma Regülasyonu'nde tanımlandığı şekilde EDPS'nin bağımsızlığı ışında yorumlanması gerektiğini belirtmiştir. Bu düzenlemede bağımsızlık kavramı uyarınca EDPS kimseden ne emir ne de talimat alabilir. Buna göre, ABAD Almanya'daki denetim otoritelerinin-kamu otoritelerinin gözetiminden dolayı- AB veri koruma hukuku anlamında tamamen bağımsız olmadığını belirtmiştir.

Örnek: Avrupa Komisyonu v. Avusturya Cumhuriyeti kararında[498] ABAD, Avusturya Veri Koruma İdaresi Başkanlığı'nın (DSK) bazı üyelerinin ve personelinin bağımsızlığı ile ilgili benzer problemlerin altını çizmiştir. ABAD, Federal Yüksek Mahkeme'nin denetim otoritesine iş gücünü sağlanmasının, AB Veri Koruma mevzuatında belirtilen bağımsızlık şartına aykırı olduğu sonucuna varmıştır. ABAD ayrıca, denetim otoritesinin Yüksek Mahkeme'ye çalışmaları hakkında her zaman bilgi verme zorunluluğunun olmasından dolayı otoritenin tam bağımsızlığını reddetmektedir.

Örnek: Avrupa/Komisyonu v. Macaristan Kararı'nda, [499] işgücünün bağımsızlığını etkileyen benzer

[492] A.g.e, Madde 51; Modernize Edilmiş 108 sayılı Sözleşme, Madde 12 mükerrer
[493] Avrupa Birliği Genel Veri Koruma Regülasyonu, Madde 52/f.1; Modernize Edilmiş 108 sayılı Sözleşme, Madde 15/f.5
[494] ABAD, C-518/07, Avrupa Komisyonu/Fedaral Almanya Cumhuriyeti, [GC], 9 Mart 2010, para. 27.
[495] A.g.e, paras. 17 and 29
[496] A.g.e, para. 23
[497] A.g.e, para. 25
[498] ABAD, C-614/10, Avrupa Komisyonu/Avusturya Cumhuriyeti, [GC], 16 Ekim 2012, paras. 59 ve 63.
[499] ABAD, C-288/12 Avrupa Komisyonu/Macaristan [GC], 8 Nisan 2014, paras. 50 ve 67.

ulusal uygulamalar yasaklanmıştır. ABAD, "her denetim otoritesinin kendisine verilen görevleri tam olarak bağımsız bir şekilde Üye Devlet'in bu otoritenin görev süresinin tamamı boyunca yerine getirmesine izin verme [...] yükümlülükleri altında olduğunu" belirtmiştir. ABAD ayrıca, "kişisel verilerin korunması için olan denetim otoritesinin görev süresinin erken sona erdirilmesiyle, Macaristan'ın 95/46/EC sayılı Direktif uyarınca yükümlülüklerini yerine getirmediğini […]" belirtmiştir.

"Tam bağımsızlık" kavramı ve kriterleri, açıklanmış olan ABAD kararları ile oluşturulan ilkeleri içeren şekilde GDPR'da açıkça belirtilmiştir. Düzeleme uyarınca, görevlerini yerine getirirken ve yetkilerini kullanırken tam bağımsızlık şartları: [500]

- Her bir denetim otoritesinin üyeleri, dış etkenlerden uzak durmalı – doğrudan veya dolaylı – ve hiç kimseden talimat almamalıdır;
- Denetim otoritesinin üyeleri, çıkar çatışmalarını önlemek için görevleriyle uyuşmayan herhangi eylemden kaçınmalıdır;
- Üye Devlet'ler, her denetim otoritesine görevlerini etkin bir şekilde yerine getirilmeleri için gerekli insan, teknik ve finansal kaynakları ve altyapıyı sağlamalıdır;
- Üye Devlet'ler her denetim otoritesinin kendi personelini kendi seçmesini sağlamalıdır;
- Her denetim otoritesinin ulusal yasalara göre tabi tutulduğu mali kontrol, bağımsızlığını etkilememelidir. Denetim otoritelerinin uygun şekilde çalışabilmelerini sağlayan ayrı ve halka açık yıllık bütçeleri olmalıdır.

Denetim otoritelerinin bağımsızlığı, Avrupa Konseyi hukuku uyarınca da temel bir gereklilik olarak kabul edilmiştir. Modernize Edilmiş 108 sayılı Sözleşme, denetim otoritelerinin talimat almadan veya kabul etmeden "görevlerini yerine getirme ve yetkilerini kullanma konusunda tam bağımsız ve tarafsız olarak hareket etmek" şartını aramaktadır. [501] Böylelikle, bu düzenleme uyarınca otoritelerin işlevlerini tam bağımsız olarak yerine getirmedikleri sürece veri işleme ile ilgili bireylerin hak ve özgürlüklerini etkin bir şekilde koruyamadıkları değerlendirilmiştir. Modernize Edilmiş 108 sayılı Sözleşme'nin Açıklayıcı Raporu, bu bağımsızlığın korunmasına katkıda bulunan birkaç unsur ortaya koymaktadır. Bu unsurlar, denetim otoritelerinin kendi personelini işe alma ve dış müdahaleye maruz kalmadan kararlar alabilmenin yanı sıra, işlevlerini yerine getirme süreleri ve işlevlerini durdurabilecekleri koşulları ile ilgili etkenleri de içerir.[502]

5.2 Görev ve Yetki

AB hukuku uyarınca GDPR, denetim otoritelerinin yetkilerini ve organizasyon yapısını ana hatlarıyla belirtir ayrıca yetkili olmalarını ve düzenleme uyarınca zorunlu olan görevleri yerine getirmelerini zorunlu tutmuştur.

Denetim otoritesi, AB Veri Koruma mevzuatına uyumu sağlayan ulusal hukuktaki başlıca organdır. Denetim otoriteleri proaktif ve önleyici denetim faaliyetlerini içeren, gözlemlemenin de ötesinde daha kapsamlı görevler ve yetkiler listesine sahiptir. Denetim otoriteleri bu görevlerini yerine getirmek için aşağıdakiler dahil, GDPR'nin 58. maddesinde belirtilen uygun araştırma, düzeltme ve öneride bulunma yetkilerine sahip olmalıdır: [503]

[500] Avrupa Birliği Genel Veri Koruma Regülasyonu, Madde 69
[501] Modernize Edilmiş 108 sayılı Sözleşme, Madde 15/f.5
[502] Moderne Edilmiş 108 sayılı Sözleşme'nin Açıklayıcı Raporu
[503] Avrupa Birliği Genel Veri Koruma Regülasyonu, Madde 58. 108 sayılı Sözleşme'de de ayrıca göreceğiniz üzere, Ek Protokol Madde 1

- tüm veri koruma ile ilgili konularda veri sahiplerine ve veri sorumlularına tavsiyelerde bulunmak;
- standart sözleşme maddelerini, bağlayıcı şirket kurallarını veya idari düzenlemeleri düzenlemek;
- veri işleme faaliyetlerini araştırmak ve bu faaliyete müdahale etmek;
- denetleyici faaliyetleri teftişi ile ilgili herhangi bir bilginin sunulmasının gerekmesi;
- veri sorumlularını uyarmak veya kınamak ve veri sahiplerine kişisel veri ihlalinin bildirilmesini sağlamak;
- verilerin düzeltilmesini, işlenmesinin engellenmesini, silmesini veya imha edilmesini emretmek;
- verilerin işlenmesini geçici olarak ya da devamlı şekilde yasaklamak ya da idari para cezaları kesmek;
- bir konuyu mahkemeye sevk etmek;

Bir denetim otoritesinin işlevlerini yerine getirebilmesi için, bir inceleme için gerekli olan tüm kişisel verilere ve bilgilere erişiminin yanı sıra, veri sorumlusunun bilgileri elinde tuttuğu yere de erişiminin olması gerekir. ABAD uyarınca, denetim otoritesinin yetkileri AB'deki veri sahiplerine yönelik veri korunmasının tam anlamıyla etkin olmasını sağlamak için geniş şekilde yorumlanması gerekmektedir.

Örnek: Schrems Kararı'nda ABAD, Edward Snowden tarafından yapılan açıklamalar ışığında, ilk AB-ABD Güvenli Liman Antlaşması uyarınca kişisel verilerin ABD'ye aktarılmasının AB veri koruma mevzuatına uygun olup olmadığı konusunda değerlendirmelerde bulunmuştur. ABAD'ın gerekçe olarak, ulusal denetim otoritelerinin-veri sorumluları tarafından veri işleme faaliyetinin bağımsız gözlemcileri olarak hareket etmek-yeterlilik kararına rağmen yeterli korumayı üçüncü ülkenin garanti etmediğine dair makul bir kanıt varsa, kişisel üçüncü bir ülkeye aktarılmasını engelleyebileceğini ileri sürmüştür. [504]

Her bir denetim otoritesi, kendi inceleme alanındaki soruşturma yetki ve yetkilerini kullanma yetkinliğine sahiptir. Ancak, veri sorumlularının ve veri işleyenlerin faaliyeti çoğu zaman sınır ötesi olduğundan ve veri işleme birden fazla Üye Devlet'te bulunan veri sahiplerini etkilediğinde farklı denetim otoriteleri arasında yetki ile ilgili sorun ortaya çıkmaktadır. ABAD, Weltimmo davasında bu konuyu inceleme fırsatı bulmuştur.

Örnek: Weltimmo Kararı uyarınca[505], ABAD ulusal denetim otoritelerinin kendi yetki alanlarında kurulmamış kuruluşları içeren meseleleri ele almasını incelemiştir. Slovakya'ya kayıtlı bir şirket olan Weltimmo, Macar mülkleri için bir internet sitesi işletmektedir. Reklamcılar, Macar veri koruma mevzuatını ihlal ettikleri için Macar veri koruma denetim otoritesine şikayette bulunmuşlardır ve otorite Weltimmo için para cezasına hükmetmiştir. Şirket, ulusal mahkemeler nezdinde cezaya itiraz etmiştir ve dava, AB Veri Koruma Direktifi'nin bir Üye Devlet'in denetim otoritelerinin ulusal veri koruma hukukunun başka bir Üye Devlet'e kayıtlı bir şirkete uygulamalarına izin verip vermediğini tespit etmek için ABAD'a sevk etmiştir.

ABAD, "ilgili veri sorumlusunun, Üye Devlet'in yetki alanında devamlı şekilde faaliyet gösterdiği sürece ve bu işlemenin gerçekleştirilmesi kapsamında gerçek ve etkili bir – en az bir bile olsa - faaliyet olması halinde" Veri Koruma Direktifi'nin 4. maddesinin 1. fıkrası uyarınca, veri sorumlusunun kayıtlı olduğu Üye Devlet'ten başka bir Üye Devlet'in veri koruma yasasının uygulanmasına izin vermiştir. ABAD, önceki bilgilere dayanarak, Weltimmo'nun Macaristan'da bir Macar adresi ve

[504] ABAD, C-362/14, Maximilian Schrems v. Veri Koruma Komisyonu [GC], 6 Ekim 2015, paras. 26–36 ve 40–41.
[505] ABAD, C-230/14, Weltimmo s.r. o. v. Nemzeti Adatvédelmi és Információszabadság Hatóság, 1 Ekim 2015.

Slovak banka hesabı ve posta kutusu ile birlikte Slovak şirketlerinde kayıtlı bir temsilcisinin Macaristan'da bulunması ayrıca Macarca yazılmış Macaristan'da faaliyetlerini sürdürmesi nedeniyle şirketin Macaristan'da gerçek ve etkili bir faaliyette bulunduğunu gözlemlemiştir. Bu bilgi bir yerleşik kuruluşun var olduğunu göstermiştir ve Weltimmo'nun faaliyetleri Macar veri koruma hukukuna tabi kılınacak ve Macar denetim otoritesinin yetki alanına girecektir. Fakat, ABAD bu bilgilerin doğrulanmasını ve Weltimmo'nun gerçekten Macaristan'da bir kuruluşunun olduğunun kabul edilip edilmeyeceğinin kararını ulusal mahkemeye bırakmıştır.

Karar verme yetkisi bırakılan mahkeme Weltimmo'nun Macaristan'da bir kuruluşu olduğunu tespit ederse, Macar denetim otoritesinin para cezasına hükmetme yetkisi olacaktır. Bununla birlikte, eğer ulusal mahkeme aksine karar verirse, bu demektir ki Weltimmo'nun Macaristan'da bir kuruluşu olmadığına o zaman uygulanabilir olan hukuk şirketin kayıtlı olduğu Üye Devlet (ler)'in hukuku olacaktır. Bu durumda denetim otoritelerinin yetkilerinin diğer Üye Devlet'lerin bölgesel egemenliğine uygun olarak kullanılması gerektiğinden, Macar otoritesi cezaya hükmedemez. Ayrıca Veri Koruma Direktifi denetim otoriteleri için bir iş birliği yükümlülüğü içerdiğinden, Macar otoritesi, Slovak meslektaşından konuyu incelmesini, Slovak hukukuna aykırı davranışın olup olmadığını tespit etmesini ve Slovak hukuku uyarınca verilen cezaların uygulanması talep edebilecektir.

GDPR'nin kabul edilmesiyle beraber, sınır ötesi davalarda denetim otoritelerinin yetkisi ile ilgili kurallar mevcuttur. Bu düzenleme, "tek otoriteye bağlı olunması"nı oluşturur ve farklı denetim otoriteleri arasında iş birliğini zorunlu kılacak hükümleri içerir. Sınır ötesi davalarda etkin bir iş birliği için GDPR, veri sorumlusunun veya veri işleyenin ana kuruluşunun veya tek kuruluşunun denetim otoritesi olarak kurulacak lider denetim otoritesine ihtiyaç duyulduğunu belirtmiştir. [506] Lider denetim otoritesi sınır ötesi davalardan sorumludur, veri sorumlusunun ve veri işleyenin tek muhatabıdır ve fikir birliğinin sağlanması için diğer denetim otoriteleriyle iş birliğini koordine etmektedir. Bu iş birliği, bilgi alışverişini, bağlayıcı kararların gözlemlenmesine, incelenmesine ve benimsenmesine karşılıklı olarak yardımcı olmayı içermektedir. [507]

Avrupa Konseyi hukukunda, denetim otoritelerinin görevleri ve yetkileri Modernize Edilmiş 108 sayılı Sözleşme'nin 15. maddesinde yer almaktadır. Bu yetkiler, soruşturma ve müdahale etme yetkileri, karar verme ve sözleşme hükümlerinin ihlaliyle ilgili idari yaptırımlara hükmetme ve hukuki işlemlerde bulunma yetkileri de dahil olmak üzere, AB hukuku altındaki denetim otoritelerine tekabül etmektedir. Bağımsız denetim otoriteleri ayrıca veri sahiplerinin taleplerini ve şikayetlerini ele alma, veri koruma mevzuatı hakkında kamuoyunda farkındalığı artırma ve kişisel veri işlemeyi sağlayan herhangi bir hukuki veya idari tedbir için ulusal düzey karar verenlere tavsiyede bulunma yetkisine sahiptir.

5.3 İş birliği

GDPR, denetim otoriteleri arasındaki iş birliği için genel hatlarıyla bir çerçeve oluşturur ve denetim otoritelerinin sınır ötesi veri işleme faaliyetlerinde iş birliği konusunda daha spesifik kurallar sağlar.

GDPR uyarınca denetim otoriteleri birbirlerine karşılıklı yardım sağlar ve düzenlemeyi tutarlı bir şekilde uygulamak için ilgili bilgileri paylaşır ve düzenlemeyi tutarlı bir şekilde uygular. [508] Bu durum, denetim otoritelerinin müzakere etmesini, teftiş yapmasını ve soruşturma yürütmesini de kapsamaktadır. Denetim otoriteleri, tüm denetim otoritelerinin personelinin dahil olduğu ortak soruşturmalar ve ortak yaptırım tedbirleri de dahil olmak üzere ortak işlemler yapabilirler. [509]

[506] Avrupa Birliği Genel Veri Koruma Regülasyonu, Madde 56/f.1
[507] A.e.g., Madde 60
[508] A.e.g, Madde 61/f.1-3 ve m. 62/f.1
[509] A.e.g., Madde 62/f.1

AB'de veri sorumluları ve veri işleyenler gittikçe daha fazla uluslararası faaliyet göstermektedirler. Bu demektir ki; kişisel veri işleme faaliyetinin, GDPR şartlarına uygun olmasını sağlamak için Üye Devlet'lerdeki yetkili denetim otoriteleri ile arasındaki yakın iş birliğini gerektirir. Düzenlemenin "tek otoriteye bağlı olunması" mekanizmasına göre; bir veri sorumlusunun veya veri işleyenin birkaç Üye Devlet'te tek bir veya birden çok kuruluşu varsa, ancak veri işleme faaliyetleri birden fazla Üye Devlet'teki veri sahiplerini etkiliyorsa, ana (veya tek) kuruluşun denetim otoritesi veri sorumlusunun veya veri işleyenin sınır ötesi faaliyetlerinin lider otoritesidir. Lider otoriteler veri sorumlusuna veya veri işleyene karşı yaptırım uygulama yetkisine sahiptirler. Tek otoriteye bağlı olunması mekanizması, uyumlaştırmayı ve AB veri koruma hukukunun farklı Üye Devlet'ler arasında aynı şekilde uygulanmasını geliştirmeyi amaçlar. Ayrıca birkaç denetim otoritesinin yerine sadece bir lider otorite ile ilgilenmeleri gerektiğinden işlemeler için de faydalıdır. Bu konu, işletmeler için hukuki öngörülebilirliği artırmaktadır ve uygulamada kararların daha hızlı alındığı ve işletmelerin kendileri ile çelişen zorunluluklar getiren farklı denetim otoriteleri ile karşı karşıya olmadığı anlamına gelmektedir.

Lider otoritenin belirlenmesi, AB'de bir işletmenin ana kuruluşunun yerini tespit etmeyi gerektirir. "Ana kuruluş"un tanımı GDPR'da yer almaktadır. Eklemek gerekir ki; Madde 29 Çalışma Grubu (WP 29), ana kuruluşun belirlenmesi için kriterlerin yer aldığı, veri sorumlusunun veya veri işleyenin lider otoritesinin belirlenmesi için bir rehber yayınlamıştır. [510] AB genelinde yüksek düzeyde veri koruması sağlamak için, lider denetim otoritesi tek başına hareket edemez. Mutabakata varmak ve uyum sağlamak için veri sorumluları ve veri işleyenler tarafından kişisel veri işlemeye dair karar almak için ilgili diğer denetim otoriteleriyle iş birliği yapmalıdır. İlgili denetim otoriteleri arasında iş birliği; karşılıklı bilgi alışverişinde bulunmayı, yardım etmeyi, ortak incelemeler yapmayı ve faaliyetleri gözlemlemeyi içerir.[511]

Denetim otoriteleri birbirlerine karşılıklı yardım ederlerken diğer denetim otoriteleri tarafından yapılan bilgi taleplerini doğru bir şekilde ele almalı ve örneğin veri işleme faaliyetleri, denetimleri ve soruşturmaları hakkında veri sorumlusuna önceden yetki vermek ve onlarla müzakere etmek gibi yasal tedbirlre almalıdır. Diğer Üye Devlet'lerdeki denetim otoriteleri ile karşılıklı yardımlaşma talep üzerine en kısa zamanda ve en geç talep alındıktan 1 ay sonra olmalıdır. [512]

Veri sorumlusunun birden fazla Üye Devlet'te kuruluşu olduğu yerlerde, denetim otoriteleri, diğer Üye Devlet'lerin denetim otoritelerinin personelinin dahil olduğu soruşturma ve yasal tedbirler dahil ortak işlemler yapabilirler. [513] Farklı denetim otoriteleri arasındaki iş birliği, Avrupa Konseyi hukukunda da önemli bir gerekliliktir. Modernize Edilmiş 108 sayılı Sözleşme uyarınca denetim otoritelerinin görevlerini yerini getirmek için gerekli olduğu ölçüde birbirleriyle iş birliği yapmalıdırlar. [514] Örneğin birbirleriyle ilgili ve faydalı bilgiler sağlayarak, araştırmaları koordine ederek ve ortak eylemlerde bulunarak yapılmalıdır.

5.4. Avrupa Veri Koruma Kurulu

Bağımsız denetim otoritelerinin önemi ve Avrupa veri koruma mevzuatı uyarınca sahip oldukları başlıca yetkiler bu bölümde daha önceden açıklanmıştır. Avrupa Veri Koruma Kurulu (EDPB) veri koruma kurallarını AB genelinde etkin ve tutarlı şekilde uygulanmasını sağlamakta önemli bir etkendir. GDPR uyarınca EDBP tüzel kişiliğe sahip bir AB organı olarak kurulmuştur. [515]

Bireylerin kişisel verilerinin işlenmesi ve mahremiyetle ilgili haklarını etkileyen herhangi bir AB tedbiri

[510] Madde 29 Çalışma Grubu (WP 29) (2016), Veri sorumlusunun veya veri işleyenin lider otoritesinin belirlenmesi için rehber, WP 244, 13 Aralık 2016, 5 Aralık 2017'de güncellenmiştir
[511] Avrupa Birliği Genel Veri Koruma Regülasyonu, Madde 60/f.1-3
[512] A.e.g., Madde 61/f.1 ve f.2
[513] A.e.g., Madde 62/f.1
[514] Modernize Edilmiş 108 sayılı Sözleşme, Madde 16 ve m.17
[515] Avrupa Birliği Genel Veri Koruma Regülasyonu, Madde 68

hakkında Komisyon'a tavsiyede bulunmak üzere Veri Koruma Direktifi tarafından oluşturulan, Direktif'in yeknesak şekilde uygulanmasını sağlamak ve verilerin korunması ile ilgili konularda Komisyon'a uzman görüşü vermek için Madde 19 Çalışma Grubu'nun[516] (WP 29) halefidir. Madde 29 Çalışma Grubu (WP 29), Komisyon ve EDPS ile birlikte AB Üye Devlet denetim otoritelerinin temsilcilerinden oluşmaktadır.

Çalışma Grubu'na (WP 29) benzer şekilde EDPB, her Üye Devlet'in ve EDPS'nin denetim otoritelerinin başkanlarından veya bu kişilerin temsilcilerinden oluşmaktadır. [517] EDPS, uyuşmazlıkların çözümü ile ilgili durumlar haricinde, yalnızca GDPR'nin maddeleri uyarınca AB kurumlarına uygulanan ilke ve kurallarla ilgili kararlara oy verebileceği durumlarda eşit oy hakkına sahiptir. Komisyon, EDPB'nin faaliyetlerine ve toplantılarına katılma hakkına sahiptir ancak oy hakkına sahip değildir. [518] Kurul, beş yıllık bir süre için salt çoğunluk ile bir Başkan (temsilcisine emanet edilebilen) ve iki Başkan Yardımcısı seçer. Ayrıca, EDPB'nin, EDPS'nin Kurul'un analitik, idari ve lojistik desteğine sahip olmasını sağladığı bir sekreterlik vardır. [519]

EDPB'nin görevleri GDPR'nin 64, 65 ve 70. maddelerinde ayrıntılı olarak yer almaktadır ve üç ana faaliyete ayrılabilecek kapsamlı görevler içermektedir:

- **Tutarlılık:** EDPB, üç durumda yasal olarak bağlayıcı kararlar alabilir: bir denetim otoritesinin tek otoriteye bağlı olunması durumunda, denetleyici otoritelerin hangisinin "lider" olduğu konusunda ihtilaflı görüşlerin bulunduğu ve bir itirazda bulunan yetkili denetim otoritesinin EDPS'nin görüşünü sormaması veya bu görüşü uygulamaması durumunda. [520] EDPB'nin temel sorumluluğu, GDPR'nin AB'de tutarlı bir şekilde uygulanmasını sağlamak ve Bölüm 5.5'te açıklandığı gibi tutarlılık mekanizmasında kilit rol oynamaktır.

- **Danışma:** EDPB'nin görevleri arasında Komisyon'a, Avrupa Birliği'ndeki GDPR değişiklikleri gibi kişisel verilerin işlenmesi ile ilgili ve AB veri koruma kuralları ile çelişkili olabilecek AB mevzuatındaki değişikliklerle ilgili konularda bilgi vermeyi içerir veya kişisel verilerin üçüncü bir ülkeye veya uluslararası bir kuruluşa aktarılmasını sağlayan Komisyon yeterlilik kararlarının verilmesi yer almaktadır.

- **Rehber:** Kurul ayrıca, düzenlemenin tutarlı bir şekilde uygulanmasını teşvik etmek için rehberler, tavsiyeler ve en iyi uygulamaları yayınlar ve denetim otoriteleri arasındaki iş birliğini ve bilgi alışverişini teşvik eder. Ek olarak, veri sorumlularını ve veri işleyenleri kendi kurumlarında davranış kurallarını oluşturmaya ve veri koruma belgelendirme mekanizmasını kurmaya ve mühür edinmeye teşvik etmelidir.

EDPB kararlarına ABAD karşısında itiraz edilebilir.

5.5 GDPR'nin Tutarlılık Mekanizması

GDPR, düzenlemenin Üye Devletler genelinde tutarlı bir şekilde uygulanmasını sağlamak için bir tutarlılık mekanizması oluşturmuştur, bu sayede denetim otoriteleri birbirleriyle ve ilgili olan durumlarda Komisyon ile iş birliği yapmaktadır. Tutarlılık mekanizması iki durumda kullanılmaktadır. Birincisi; yetkili bir denetim otoritesini bir Veri Koruma Etki Değerlendirmesi (DPIA) gerektiren veri işleme faaliyetlerinin bir liste gibi veya standardize edilmiş sözleşme hükümlerini belirlemek gibi

[516] 95/46/EC sayılı Direktif uyarınca, Madde 29 Çalışma Grubu (WP 29), Komisyon'a kişisel verilerin işlenmesi ve mahremiyete ilişkin bireylerin haklarını etkileyen AB tedbirleri hakkında Direktif'in yeknesak şekilde uygulanmasını teşvik etmek ve uzmanlık sağlamak için Komisyon'a verilerin korunması ile ilgili konularda görüş vermektedir.
[517] Avrupa Birliği Genel Veri Koruma Regülasyonu, Madde 68/f.3
[518] A.e.g., Madde 68/f.4 ve f.5
[519] A.e.g., Madde 73 ve 75
[520] A.e.g., Madde 65

tedbirleri almak istediği durumlarda EDPB'nin görüşleri ile ilgilidir. İkincisi; tek otoriteye bağlı olunması durumlarında yetkilileri denetlemek için ve denetim otoritesinin EDPB'den bir görüş istemediği veya bu görüşe uyulmadığı durumlarda EDBP'nin bağlayıcı kararlarıyla ilgilidir.

6. Veri sahibinin hakları ve bu hakların kullanılması

AB	Ele Alınan Konular	Avrupa Konseyi
Bilgi edinme hakkı		
Avrupa Birliği Genel Veri Koruma Regülasyonu, Madde 12 ABAD, C-473/12, Institut professionnel des agents immobiliers (IPI) v. Englebert, 2013 ABAD, C-201/14, Smaranda Bara and Others v. Casa Naţională de Asigurări de Sănătate and Others, 2015	Bilginin şeffaflığı	Modernize Edilmiş 108 sayılı Sözleşme, Madde 8
Avrupa Birliği Genel Veri Koruma Regülasyonu, Madde 13/f.1 ve f.2 Madde 14/f.1 ve f.2	Bilginin içeriği	Modernize Edilmiş 108 sayılı Sözleşme, Madde 8/f.1
Avrupa Birliği Genel Veri Koruma Regülasyonu, Madde 13/f.1 Madde 14/f.3	Bilgiyi edinme süresi	Modernize Edilmiş 108 sayılı Sözleşme, Madde 9/f.1/b
Avrupa Birliği Genel Veri Koruma Regülasyonu, Madde 12/f.1,5 ve 7	Bilgiye erişmenin anlamı	Modernize Edilmiş 108 sayılı Sözleşme, Madde 9/f.1/b
Avrupa Birliği Genel Veri Koruma Regülasyonu, Madde 13/f.2/d Madde 14/f.2/e Madde 77, 78 ve 79	Denetim otoritesine şikayette bulunma hakkı	Modernize Edilmiş 108 sayılı Sözleşme, Madde 9/f.1/f
Erişim hakkı		
Avrupa Birliği Genel Veri Koruma Regülasyonu, Madde 15/f.1 ABAD, C-553/07, College van burgemeester en wethouders van Rotterdam v. M. E. E. Rijkeboer, 2009 ABAD, Ortak dava C-141/12 ve C-372/12, YS v. Minister voor Immigratie, Integratie en Asiel and Minister voor Immigratie,	Veri sahibinin kendi verisine erişim hakkı	Modernize Edilmiş 108 sayılı Sözleşme, Madde 9/f.1/b ECtHR, Leander v. Sweden, No. 9248/81, 1987

Genel olarak hukuk kuralları etkililiği ve özellikle de veri sahiplerinin hakları ve bu hakları uygulamak için uygun mekanizmaların varlığına büyük ölçüde bağlıdır. Dijital çağda, verilerin işlenmesi her yerde gerçekleşmektedir ve bireylerin bunu anlaması gittikçe zorlaşmaktadır.

Veri sahipleri ve veri sorumluları arasındaki güç dengesizliklerini azaltmak için bireylere kişisel bilgilerinin işlenmesini üzerinde daha fazla kontrol etme hakları konusunda belirli haklar verilmiştir. Kişinin kendi kişisel verilerine erişim hakkı ve düzeltme hakkı, AB birincil mevzuatını oluşturan ve AB hukuk düzeninde büyük öneme sahip bir belge olan AB Temel Haklar Bildirgesi'nin 8. maddesini 2. fırkasında yer almaktadır. AB ikincil mevzuatı – özellikle Avrupa Birliği Genel Veri Koruma Regülasyonu – veri sorumlularıyla ilgili haklar oluşturarak veri sahiplerini güçlendiren tutarlı bir yasal çerçeve oluşturmuştur. GDPR, erişim ve düzeltme hakların ek olarak, silme hakkı ("unutulma hakkı"), itiraz etme hakkı veya verilerin işlenmesini sınırlandırma hakkı, profilleme ve otomatik karar vermeyle ilgili haklar gibi birçok başka hakkı da tanımıştır. Veri sahiplerinin kendi verileri üzerinde etkili kontrol etmelerini sağlamak için benzer güvenlik önlemleri de Modernize Edilmiş 108 sayılı Sözleşme'ye dahil edilmiştir. Madde 9, bireylerin kişisel verilerinin işlenmesiyle ilgili olarak kullanabilecekleri hakları listeler. Taraf ülkeler, bu hakların kendi yetki alanları dahilindeki her veri sahibinin kullanımına olanak ve veri sahiplerinin kullanmalarına olanak sağlamak için etkili yasal ve pratik yollar sağlamalıdırlar.

Bireylere bu tür hakların sağlanmasının yanı sıra, veri sahiplerinin haklarının ihlal edilmesini önleme, veri sorumlularını sorumlu tutma ve veri sorumlularından tazminat talep etme mekanizmaları oluşturmak da aynı derecede önemlidir. AİHS ve Bildirge kapsamında güvence altına alındığı gibi, etkili bir hukuk yoluna başvurma hakkını ve hukuk yollarının herkes için erişilebilir olmasını gerektirir.

6.1. Veri sahiplerinin hakları

Kilit Noktalar

- Her veri sahibi, herhangi bir veri sorumlusunun, sınırlı istisnalar uyarınca kişisel verilerinin işlenmesi hakkında bilgi edinme hakkına sahiptir.

- Veri sahipleri aşağıdaki haklara sahip olmalıdır:

  - kendi verilerine erişmek ve verilerin işlenmesi hakkında kesin bilgi edinmek;

  - verilerin yanlış/hatalı olması durumunda verileri işleyen veri sorumlusu tarafından verilerin düzetilmesini sağlamak;

  - veri sorumlusunun veya veri işleyenin verileri hukuka aykırı işlemesi durumunda, veri sorumlusunun bu verileri uygun şekilde silmesini sağlamak;

  - veri işleme faaliyetini geçici olarak sınırlama hakkına sahiptir;

  - belli koşullar altında verilerinin başka bir veri sorumlusuna aktarılmasını sağlamak;

- Ek olarak veri sahiplerinin aşağıdaki haklar uyarınca verilerin işlenmesine itiraz etme hakkı vardır:
  - özel durumuyla ilgili gerekçelerle verilerinin işlenmesi,

  - verilerin doğrudan pazarlama amacıyla kullanılması

- Veri sahipleri profilleme, yasal etkileri olan veya kendisini önemli ölçüde etkileyen otomatik işlemeye dayanan kararlara tabi olmama hakkına sahiptir. Veri sahipleri ayrıca:

    - veri sorumlusu tarafından insan müdahalesi almak

    - görüşlerini ifade etme ve otomatik işlemeye dayanan karara itiraz etmek

6.1.1. Bilgi edinme hakkı

Avrupa Konseyi Hukuku ve AB hukukuna göre, veri işleme faaliyetlerinin veri sorumluları, amaçlanan işlemle ilgili kişisel veriler toplandığı zamanda veri sahibini bilgilendirmek zorundadır. Bu yükümlülük, veri sahiplerinin talebine bağlı değildir, veri sahibinin bilgiye ilgi gösterip göstermediğine bakılmaksızın veri sorumlusunun proaktif olarak bu yükümlülüğü yerine getirmesi gerekir.

Avrupa Konseyi hukuku uyarınca, Modernize Edilmiş 108 sayılı Sözleşme'nin 8. maddesi uyarınca, Taraf Ülkeler; veri sorumlularının veri sahiplerine kimlik ve mutad meskenleri hakkında, veri işlemenin yasal dayanağını ve amacını, işlenen kişisel veri kategorilerini, paylaşım yapılan tarafları (eğer varsa) ve erişim, düzeltme ve hukuki çözüm yollarını içeren 9. maddeye göre haklarını nasıl kullanabileceklerinin bilgisinin verilmesini sağlamaktadır. Adil ve şeffaf bir şekilde kişisel verilerin işlenmesinin sağlanması için gerekli görülen diğer tüm bilgiler de veri sahiplerine iletilmelidir. Modernize Edilmiş 108 sayılı Sözleşmesi'nin Açıklayıcı Raporu'nda veri sahiplerine yapılan bilgilendirmenin "kolayca erişilebilir, okunaklı, anlaşılır ve ilgili veri sahiplerine uyarlanabilir olması" gerektiğini açıkça belirtmiştir. [521]

AB hukukuna göre, şeffaflık ilkesi; herhangi bir kişisel verinin işlenmesinde genellikle bireylere karşı şeffaf olunmasını gerektirmektedir. Bireyler, hangi kişisel verilerin nasıl ve ne şekilde toplandığını, kullandığını veya işlendiğini bilmelerinin yanı sıra risklerden, önlemlerden ve verinin işlenmesi hakkındaki haklarından haberdar olma hakkına sahiptirler.[522] Böylece GDPR'ın 12. maddesi, veri sorumluları için şeffaf bilgilendirme yükümlülüğü ve/veya veri sahiplerinin haklarını nasıl kullanabileceklerini açıklama konusunda geniş kapsamlı bir yükümlülük getirmektedir.[523] Bilgilendirme(aydınlatma) net ve sade bir dil kullanarak özlü, şeffaf, anlaşılır ve kolay erişilebilir olmalıdır. Bilgilendirme uygun olduğu hallerde elektronik yollar da dahil olmak üzere yazılı olarak sunulmalıdır. Veri sahibinin kimliğinin herhangi bir şüpheye mahal bırakmadığı hallerde bilgilendirme sözel olarak da yapılabilecektir. Bilgilendirme gecikmeden ve herhangi bir masraf talep edilmeden yapılmalıdır. [524]

GDPR'ın 13. maddesi ve 14. maddesi kişisel verilerin, doğrudan veri sahiplerinden toplandığı durumlarda veya verilerin veri sahiplerinden alınmadığı durumlarda veri sahiplerinin bilgi alma hakkını ele almaktadır.

Bilgi edinme hakkının kapsamı ve AB hukuku kapsamındaki sınırlamaları ABAD hukukunda açıklığa kavuşturulmuştur.

---

[521] Modernize Edilmiş 108 sayılı Sözleşmesi'nin Açıklayıcı Raporu, para. 68
[522] Avrupa Birliği Genel Veri Koruma Regülasyonu, Gerekçe 39
[523] A.e.g., Madde 13 ve 14; Modernize Edilmiş 108 sayılı Sözleşme, Madde 8/1/b
[524] Avrupa Birliği Genel Veri Koruma Regülasyonu, Madde 12/f.5; Modernize Edilmiş 108 sayılı Sözleşme, Madde 9/1/b

Örnek: *In Institut professionnel des agents immobiliers (IPI) v. Engelbert Kararı'nda*[525], ABAD'dan 95/46 sayılı Direktif'in 13.maddesinin 1. fıkrasının yorumlanması istenmiştir. Bu madde, Üye Devlet'lere, veri sahibinin haklarının başkalarının hak ve özgürlüklerini korumak ve regüle edilmiş meslekler için suç ve etik ihlallerinin önlenmek ve soruşturmak için gerektiğinde bilgi edinme hakkını sınırlandırmada yasal tedbirleri kabul edip etmeme tercih hakkını vermiştir. IPI; Belçika'da emlakçılık mesleğinin doğru şekilde uygulanmasından sorumlu emlakçıların kurumsal kuruluşudur. Bir ulusal mahkemeden, sanıkların mesleki kuralları ihlal ettiğinin açıklaması ve emlak ajansının çeşitli faaliyetlerini durdurmalarının emredilmesi istenmiştir. Faaliyet, IPI'nin kullandığı özel dedektifler tarafından sağlanan kanıtlara dayanmaktadır.

Ulusal mahkeme, Belçika mevzuatının veri koruma şartlarına, özellikle de verileri toplamadan önce veri sahiplerine kişisel verilerin işlenmesi ile ilgili bilgilendirme yapma yükümlülüğüne uyulmaksızın verilerin elde edilme olasılığı göz önüne alındığında, dedektiflerin kanıtlarının değerine dair şüpheleri mevcuttur. ABAD, madde 13/f.1 uyarınca Üye Devlet'lerin, verilerin işlenmesi faaliyetiyle ilgili veri sahiplerini bilgilendirme yükümlülüğüne ilişkin istisnalar dışında kendi ulusal hukukları uyarınca "yapabileceklerini" ancak hiçbir zorunluluklarının bulunmadığını belirtmiştir. Madde 13/f.1; Üye Devlet'lerin bireylerin haklarını, IPI gibi bir kuruluşun faaliyetlerini ve kendi içinde faaliyet gösteren özel dedektifleri sınırlandırabilmenin gerekçesi olarak ceza gerektiren suçların veya etik ihlallerin önlenmesi, soruşturulması, tespit edilmesi ve kovuşturulması hükümlerine dayanmaktadır. Ancak, Üye Devlet böyle bir istisna kapsamına girmeyen durumlarda veri sahibini bilgilendirmelidir.

Örnek: *In Smaranda Bara ve Diğerleri v. Casa Naţională de Asigurări de Sănătate ve Diğerleri*[526] Kararı'nda ABAD, AB hukukunun ulusal bir kamu idari otoritesinin başka kamu idari otoritesine kişisel verileri daha sonra işlenmesi için aktarması konusunda hem aktarım hem de veri işlemesi hakkında veri sahiplerine bilgi verilmesinin engellenip engellenmeyeceğini açıklamıştır. Bu durumda, Ulusal İdare Kurumu başvuranlara veri aktarımdan önce kişisel verileri Ulusal Sağlık Sigortası Fonu'na aktardıklarının bilgisini vermemiştir.

ABAD, AB hukukuna göre kişisel verilerin işlenmesi hakkında veri sahibinin bilgilendirilmesi gerektiğini "çünkü veri sahiplerinin verilere erişim hakkının verileri düzeltme hakkını da etkilediğini, işlenmiş verilere […] ve bu verilerin işlenmesine itiraz hakkı olduğunu ve bunların hepsinden daha önemli olduğunu" belirtmiştir. Adil veri işleme ilkesi uyarınca daha sonraki veri işleme faaliyetleri için başka bir kamu kurumuna aktarımı hakkında veri sahibinin bilgilendirilmesi gerekmektedir.

[525] CJEU, C-473/12, Institut professionnel des agents immobiliers (IPI)/Geoffrey Englebert ve Diğerleri, 7 Kasım 2013

[526] CJEU, C-201/14, Smaranda Bara and Others v. Casa Naţională de Asigurări de Sănătate ve Diğerleri, 1 Ekim 2015.

95/46 sayılı Direktif'in 13. maddesinin 1. fıkrası uyarınca, Üye Devlet'ler vergilendirme konuları da dahil olmak üzere devletin önemli bir ekonomik çıkarını korumak için gerekli görmesi halinde bilgilendirme hakkını kısıtlayabilir. Ancak, bu tür kısıtlamalar yasal tedbirlerle yapılmalıdır. Ne veri aktarımının tanımı ve ne de aktarım için ayrıntılı düzenlemeler yasal bir çerçevede belirtilmediğinden, yalnızca iki kamu kurumu arasındaki bir protokolde AB kanunları uyarınca istisna koşulları yerine getirilmemiştir. Başvuranlara, verilerin Ulusal Sağlık Sigortası Fonu'na aktarılmasından ve bu kurumun bu verileri daha sonra işlenmesinden önce bilgilendirme yapılmış olması gerekmektedir.

Bilgilendirmenin İçeriği

Modernize Edilmiş 108 sayılı Sözleşme'nin 8. maddesinin 2. fıkrası uyarınca veri sorumlusunun, adil olarak ve şeffaf bir şekilde kişisel veri işlemeyi sağlayarak ve aşağıdakileri de dahil ederek veri sahibini bilgilendirmelidir:

- veri sorumlusunun kimliği ve mutad meskeni veya kuruluşu
- veri işleme amacının yasal dayanağı ve amacı
- işlenen kişisel veri kategorileri
- eğer varsa kişisel verilerin aktarılacağı taraflar veya alıcı kategorileri
- veri sahiplerinin kendi haklarını kullanma yolları

GDPR uyarınca, veri sahiplerinden kişisel verilerin toplandığında, veri sorumlusu kişisel verilerin elde edildiği tarihte aşağıda yer alan bilgileri veri sahibine sunmakla yükümlüdür:

- varsa Veri Koruma Görevlisi'nin bilgileri da dahil olmak üzere, veri sorumlusunun kimlik bilgisi ve iletişim bilgileri;
- veri işlemenin amacı ve hukuki temelinin ne olduğu, ör. sözleşmesel veya yasal zorunluluk;
- veri işlemesi için temel teşkil ediyorsa ver sorumlusunun meşru menfaati;
- kişisel verinin aktarıldığı taraflar veya aktarılan tarafların kategorileri;
- kişisel verilerin üçüncü bir ülkeye mi yoksa uluslararası bir kuruluşa mı aktarılacağının bilgisi ve bunun bir yeterlilik kararına mı dayandığı veya uygun tedbirlerin alınıp alınmadığı;
- kişisel verilerin saklanacağı süre ve bu sürenin belirlenmesi mümkün değilse, veri saklama süresini belirlemek için kullanılan kriterlerin neler olduğu;
- veri sahiplerinin erişim, düzeltme, silme veya veri işlemesini sınırlandırma veya verilerin işlenmesine itiraz etme hakları gibi verilerin işlenmesi ile ilgili haklar;
- kişisel verilerin edinilmesinin yasaların veya bir sözleşmenin gereği olup olmadığı, veri

sahibinin kişisel verilerini paylaşmasının zorunluluğunun olup olmadığı ayrıca veri sahibinin kişisel verilerini paylaşmaması halinde sonuçları;

- Profilleme dahil olmak üzere otomatik karar vermenin varlığı;
- Denetim otoritesine şikayet etme hakkı
- Verilen rızayı sonradan geri çekme hakkının varlığı;

Profilleme de dahil olmak üzere otomatik karar verme durumlarında, veri sahiplerinin profillemede yer alan mantığı, önemi ve işlemden kaynaklı öngörülen sonuçlar ile ilgili anlamlı bilgiler edinmelidir.

Kişisel verilerin doğrudan veri sahibinden elde edildiği durumlarda, veri sorumluları, bireye kişisel verilerin toplama kaynağı hakkında bilgi vermelidir. Her durumda, veri sorumlusu, diğer bilgilerin yanı sıra, profilleme dahil olmak üzere otomatik karar vermenin varlığı hakkında veri sahiplerini bilgilendirmelidir. [527] Son olarak, bir veri sorumlusunun kişisel verileri başlangıçta belirtilenden başka bir amaç uyarınca işlenmek istiyorsa, amaçta sınırlılık ve şeffaflık ilkelerine göre veri sorumlusunun bu konuyla ilgili bu yeni amaç hakkında bilgi vermesini gerektirir. Veri sorumluları daha sonraki verilerin işlenmesinden önce bilgilendirme yapmalıdır. Başka bir deyişle, veri sahibinin kişisel veri işlemesi için rıza verdiği durumlarda, veri işleme amacı değişirse veya veri işleme amacına başka amaçlar eklendiyse veri sorumlusunun veri sahibinin yenilenmiş rızasını almalıdır.

Bilgilendirme Zamanı

GDPR uyarınca, veri sorumlusunun veri sahibine bilgilendirme yapması gereken iki senaryo ile iki nokta arasında ayrım yapar:

- Kişisel verilerin doğrundan veri sahibinden elde edildiği durumlarda, veri sorumlusu verileri toplarken GDPR kapsamındaki tüm bilgiler ona sunulmalı ve hakları hakkında bilgilendirilmelidir.[528]
- Veri sorumlusu kişisel verileri farklı bir amaç için daha fazla veriyi işlemeyi planlıyorsa, veri sorumlusunun verileri işlemeden önce tüm ilgili bilgileri veri sahibine sunmalıdır.
- Kişisel verilerin doğrudan veri sahibinden elde edilmediği durumlarda veya veriler üçüncü bir tarafa aktarılmadan önce, veri sorumlusu "kişisel verileri elde ettikten sonra makul bir süre içerisinde ancak 1 (bir) ayı geçmeyecek kadar" veri sahibine veri işlenmesi konusunda bilgi vermekle yükümlüdür.

Modernize Edilmiş 108 sayılı Sözleşme Açıklayıcı Raporu uyarınca, veri işlemeye başlarken veri sahibini bilgilendirmesi mümkün değilse, veri sorumlusu herhangi bir nedenden dolayı veri sahibine temas etmesi gibi daha sonraki bir aşamada bilgilendirmenin yapılabileceği öngörülmektedir. [529]

Bilgilendirmenin farklı yollarla yapılması

[527] Avrupa Birliği Genel Veri Koruma Regülasyonu, Madde 13/f.2 ve m.14/2/f
[528] A.e.g., Madde 13/f.1 ve 2, Avrupa Birliği Genel Veri Koruma Regülasyonu'nun bilgilendirmenin yapılmasında "kişisel verilerin elde edildiği tarihte" uygulanması yükümlülüğü hakkındaki ifade ettiği önsözdür.
[529] Modernize Edilmiş 108 sayılı Sözleşme Açıklayıcı Raporu, para. 70

Hem Avrupa Konseyi hukuku hem de AB hukukuna göre, veri sorumlularının veri sahiplerine sağlaması gereken bilgiler az ve öz, şeffaf, anlaşılır ve kolay erişilebilir olmalıdır. Açık, sadece ve kolayca anlaşılabilir bir dil kullanılarak, yazılı olarak veya elektronik araçlar da dahil olmak üzere diğer yollarla yapılmalıdır. Veri sorumlusu bilgilendirmeyi kolayca görülebilir şekilde sunabilir ve anlaşılır şekilde yapmak için standardize edilmiş simgeleri kullanabilir.[530] Örnek vermek gerekirse; verilerin güvenli bir şekilde toplandığı ve/veya şifrelendiğini bildirmek için kilidi temsil eden bir simge kullanılabilir. Veri sahipleri sözlü yollarla bilgilendirmenin yapılmasını talep edebilir. Veri sahiplerinin istekleri açıkça temellendirilmemiş veya aşırı olmadıkça (tekrarlayıcı nitelikte) bilgilendirme ücretsiz olarak yapılmalıdır.[531] Bilgilendirmeye kolay erişim, veri sahibinin AB veri koruma mevzuatı kapsamında belirtilen haklarını kullanabilmesi için önemlidir.

dil işleme ilkesi, bu bilgilerin veri sahipleri tarafında kolayca anlaşılabiliyor olmasını gerektirir. Muhataplara uygun bir dil kullanılmalıdır. Kullanılan dilin seviyesi ve türü, hedeflenen kitlenin, örneğin bir yetişkin veya çocuk olması, halktan biri veya akademisyen olmasına bağlı olarak farklı olmalıdır. Anlaşılabilir bilgilendirmenin bu yönünün nasıl dengeleneceği sorusu Madde 29 Çalışma Grubu'nun Daha Fazla Uyumlaştırılmış Bilgilendirme Hükümleri Kararı'nda açıklanmıştır. Bu, söz konusu katmanlı bildirimler[532] fikrini destekleyen, verinin sahibinin hangi ayrıntı düzeyini tercih edeceğine karar vermesine olanak tanır. Bununla birlikte, bu bilgilendirme şekli veri sorumlusunun GDPR'ın 13. ve 14. maddeleri kapsamındaki yükümlülüğüne halel getirmez. Veri sorumlusunun hala tüm bilgilendirmeyi veri sorumlusuna yapması gerekmektedir.

Bilgilendirmenin en etkili yollarından biri internet sitesine gizlilik politikaları gibi veri sorumlusunun ana sayfasına uygun bilgi maddeleri yerleştirmektir. Bununla birlikte, interneti kullanmayan önemli ölçüde kitle de vardır ve bir şirketin veya kamu otoritesinin bilgilendirme politikasında (aydınlatma metninin) bu dikkate alınmalıdır.

İnternet sayfasındaki kişisel verilerin işlenmesiyle ilgili gizlilik metni aşağıdaki gibi görünebilir:

Biz kimiz?

Veri işleyen "veri sorumlusu" olan Bed and Breakfast C&U; [Address: xxx] mukimdir, Tel: xxx; Fax: xxx; Email at info@c&u.com; Veri Koruma Görevlisi iletişim bilgisi [xxx].

Kişisel veri aydınlatma metni, otel hizmetlerimizi düzenleyen şartların ve koşulların bir parçasını oluşturur.

[530] Avrupa Komisyonu ayrıca, temsilciler tarafından sunulacak bilgileri ve temsil edilen yasalar aracılığıyla standartlaştırılmış simgelerle bilgilendirme yapma prosedürlerini geliştirecektir: bkz. Avrupa Birliği Genel Veri Koruma Regülasyonu, Md. 12/f.8
[531] Avrupa Birliği Genel Veri Koruma Regülasyonu, Madde 12/f.1,5 ve 7 ve Modernize Edilmiş 108 sayılı Sözleşme, Madde 9/f.1/b
[532] Madde 29 Çalışma Grubu (2004), 10/2004 tarihli Daha Fazla Uyumlaştırılmış Bilgilendirme Hükümleri Kararı, WP 100, Brüksel, 25 Kasım 2004

Sizden hangi verileri topluyoruz?

Sizden aşağıdaki kişisel bilgileri toplamaktayız; adınız, posta adresiniz, telefon numaranız, e-posta adresiniz, konaklama bilgileriniz, kredi kartı ve banka kartı numaranız ve IP adresleriniz veya internet sitemize bağlanmak için kullandığınız bilgisayarların alan adı.

Neden verilerinizi topluyoruz?

Verilerinizi rızanızı temel alarak ve çekinceleri yerine getirmek, size sunduğumuz hizmetlerle ilgili sözleşmeleri kurmak ve ifa etmek, yasaların gerektirdiği gereklilikleri yerine getirmek için örneğin Yerel Harçlar Kanunu uyarınca konaklama için şehir vergisinin ödenmesini sağlamak adına kişisel verilerinizi toplamamız gerekir.

Kişisel verilerinizi nasıl işliyoruz?

Kişisel verileriniz üç aylık süre boyunca saklanacaktır. Verileriniz otomatik karar verme prosedürlerine tabi değildir.

Bed and Breakfast C&U, kişisel bilgilerinizin izniniz olmadan zarar görmemesi, imha edilmemesi veya üçüncü bir tarafa ifşa edilmemesi ve yetkisiz erişimin önlenmesi için sıkı güvenlik prosedürleri uygulamaktadır. Bilgileri depolayan bilgisayarlar, fiziksel erişimi kısıtlı ve güvenli ortamlarda tutulur. Elektronik erişimi kısıtlamak için güvenlik duvarları oluşturmakta ve diğer önlemleri almaktayız. Verilerin üçüncü bir tarafa aktarılması gerekiyorsa, kişisel verilerinizi korumak için benzer önlemleri almalarını gerekmektedir.

Topladığımız veya kaydettiğimiz tüm bilgiler ofislerimizde yer almaktadır. Sadece bu sözleşme kapsamındaki yükümlülüklerini yerine getirmek için bilgiye ihtiyaç duyan kişisele kişisel verilere erişim izni verilir. Sizi tanımlamak için bilgiye ihtiyaç duyduğumuzda size açıkça soracağız. Sizi bilgi vermeden önce güvenlik kontrollerimizle iş birliği yapmanızı isteyebiliriz. Bize verdiğiniz kişisel bilgileri istediğiniz zaman doğrudan bizimle işletişime geçerek güncelleyebilirsiniz.

Haklarınız nelerdir?

Verilerinize erişim, verilerinizin bir kopyasını alma, verilerin silinmesini veya düzeltilmesini talep etme veya verilerinizin başka bir veri sorumlusuna taşınmasını isteme hakkınız vardır.

İstekleriniz için info@c&u.com adresinden bizimle iletişime geçebilirsiniz. İsteğinizi bir ay içinde yanıtlayacağız ancak isteğiniz çok kapsamlı veya başka çok fazla istek alınması durumunda bu sürenin iki ay daha uzatılabileceğini bildireceğiz.

Kişisel verilerinize erişim

Talep veya istek üzerine, verinin temelini oluşturan veri işleme gerekçesinin bilgilendirmesini, silinmelerini veya düzeltilmelerini görüşlerinizi dikkate almadan tamamen otomatik bir karara tabi olmama hakkına sahip olacaksınız. İstekleriniz için info@c&u.com adresinden bizimle iletişime geçebilirsiniz. Ayrıca, verilerinizin işlenmesine itiraz etme, rızanızı geri çekme ve ulusal denetim otoritesine şikayette bulunma hakkınıza sahipsiniz, bu veri işleme faaliyetinin hukuka aykırı olduğunu düşünüyorsanız ve hukuk aykırı işlemlerin sonucu olarak ortaya çıkan zarar için tazminat talebinde bulunabilirsiniz.

Şikayette bulunma hakkı

GDPR kişisel veri ihlali durumlarında yerel hukuk ve AB hukuku kapsamındaki icra mekanizmaları hakkında veri sorumlusunun veri sahiplerini bilgilendirmesi gerektiğini belirtmiştir. Veri sorumlularının veri sahiplerini denetim otoritesine ve gerekirse bir yerel mahkemeye yapılan kişisel veri ihlaliyle ilgili şikayette bulunma hakları hakkında bilgilendirmesi gerekir.[533] Avrupa Konseyi hukuku ayrıca, veri sahiplerinin madde 9 fıkra 1'de belirtilen bir kanun yoluna başvurma hakkı da dahil olmak üzere haklarını kullanma konusunda bilgilendirilme hakkını belirtir.

Bilgilendirme yükümlülüğünün istisnaları

GDPR, bilgilendirme yükümlülüğüne istisna getirmektedir. GDPR'ın 13. maddesinin 4. fıkrası ve 14. maddesinin 5. fıkrası uyarınca, eğer veri sahibi zaten ilgili bilgilerin tümüne sahipse, veri sahibini bilgilendirme yükümlülüğü ortadan kalkar.[534] Ek olarak, kişisel verilerin veri sahibinden elde edilmesi durumlarında, bilgilendirme yapılması imkansız veya orantısız ise, özellikle kişisel verilerin kamu yararı, bilimsel çalışma veya tarihi araştırma amacıyla arşivleme için işlendiği durumlarda, bilgilendirme yapma yükümlülüğü uygulanmayacaktır.[535]

Ayrıca, Üye Devletler, demokratik toplumda, örneğin ulusal düzeyde ve kamusal güvenlik, savunma, adli soruşturmaları ve kovuşturmaları veya ekonomik ve finansal çıkarları korumak

[533] Avrupa Birliği Genel Veri Koruma Regülasyonu, Madde 13/f.2/d ve 14/2/e, Modernize Edilmiş 108 sayılı Sözleşme, Mdde 8/f.1/f
[534] A.e.g., Madde 13/f.4 ve 14/5/a
[535] A.e.g., Madde 14/f.5/b-e

için gerekli ve orantılı bir önlem alması durumunda, bu düzenleme uyarınca bireylerin yükümlülükleri ve haklarını kısıtlamak için GDPR uyarınca takdir yetkisine sahiptir. Herhangi bir muafiyet veya kısıtlama demokratik toplumda gerekli ve uyulması gereken amaçla orantılı olmalı.

Çok istisnai durumlarda, örneğin tıbbi belirtiler nedeniyle, veri sahibinin korunması için şeffaflığın sınırlandırılması gerekebilir; bu özellikle her veri sahibinin erişim hakkının kısıtlanması ile ilgilidir.[536] Bununla birlikte, asgari bir koruma seviyesi olarak, yerel hukuk AB hukuku kapsamında korunan temel hak ve özgürlüklerin özüne saygı göstermelidir[537]. Bu yerel hukukun veri işlenmesinin amacını içerdiği kişisel veri kategorileri, güvenceleri ve diğer prosedür gereklerini açıklayan özel hükümler içermelidir.[538]

Verilerin, bilimsel veya tarihi araştırma amacıyla, istatiksel amaçlarla veya kamu yararı amacıyla arşivlemek için toplanması durumunda, Birlik ve Üye Devlet'ler hukuku uyarınca eğer ifa etmek imkansız hale geldiyse veya belirli amaçlarla ulaşılması halinde ciddi şekilde zarar görmesinin muhtemel olup olmadığını bildirme yükümlülüğünün istisnası olarak kabul edilebilir.[539]

Modernize Edilmiş 108 sayılı Sözleşme'nin 9. maddesi uyarınca veri sahiplerine verilen hakların katı koşullar altında, Modernize Edilmiş 108 sayılı Sözleşme'nin 11. maddesi uyarınca olası sınırlamalara tabi olabileceği gibi, Avrupa Konseyi hukukunda da benzer sınırlamalar varsın. Ayrıca, Modernize Edilmiş 108 sayılı Sözleşme'nin 8. maddesinin 2. fıkrasına göre veri sorumlusunun işlemin şeffaflığını sağlama yükümlülüğü, veri sahibinin bilgi sahibi olduğu durumlarda geçerli değildir.

Bireylerin kendi verilerine erişim hakkı

Avrupa Konseyi hukuku uyarınca, bireyim kendi verilerine erişim hakkı, Modernize Edilmiş 108 sayılı Sözleşme'nin 9. maddesinde açıkça belirtilmiştir. Her bireyin talep üzerine kendisiyle ilgili kişisel verilerin işlenmesi hakkında anlaşılır bir şekilde iletilmesi gereken bilgileri edinme hakkına sahip olmasını sağlar. Erişim hakkı sadece Modernize Edilmiş 108 sayılı Sözleşme hükümlerinde değil, aynı zamanda AİHM içtihatlarında da tanınmıştır. AİHM, birçok kez bireylerin kendi kişisel verileri hakkındaki bilgilere erişim hakkına sahip olduğunu ve bu hakkın özel hayata saygı duyulması ihtiyacından doğduğunu ileri sürmüştür.[540] Bununla birlikte, kamu kurumu veya özel kuruluşlar tarafından depolanan kişisel verilere erişim hakkı belirli durumlarda sınırlı olabilir. [541]

AB hukuku uyarınca, bir kişinin kendi verilerine erişim hakkı GDPR'ın 15. maddesinde açıkça belirtmiştir ve ayrıca AB Temel Haklar Bildirgesi'nin 8. maddesinin 2. fıkrası uyarınca kişisel verilerin korunmasına ilişkin temel hakların bir unsuru olarak belirtilmiştir.[542] Bireyin kendi

---

[536] Avrupa Birliği Genel Veri Koruma Regülasyonu, Madde 15
[537] Avrupa Birliği Genel Veri Koruma Regülasyonu, Madde 23/f.1
[538] A.e.g., Madde 23/f.2
[539] A.e.g., Madde 89/f.2 ve 3
[540] AİHM, Gaskin v. Birleşik Krallık, No. 10454/83, 7 Temmuz 1989; AİHM, Odièvre v. France [GC], No. 42326/98, 13 Şubat 2003; AİHM, K.H. and Others v. Slovakya, No. 32881/04, 28 Nisan 2009; AHİM, Godelli v. İtalya, No. 33783/09, 25 Eylül 2012
[541] AİHM, Leander v. İsveç, No. 9248/81, 26 March 1987
[542] Ayrıca bkz. CJEU, Ortak davalar C-141/12 ve C-372/12, YS v. Minister voor Immigratie, Integratie en Asiel ve Minister voor Immigratie, Integratie en Asiel v. M ve S, 17 Temmuz 2014; CJEU, C-615/13 P, ClientEarth, Pesticide Action Network Europe (PAN Europe) v. Avrupa Gıda Güvenliği Kurumu (EFSA), Avrupa Komisyon, 16 Temmuz 2015.

kişisel verilerine erişim hakkı, Avrupa veri koruma hukukunun kilit unsurlarından biridir.[543]

GDPR, her veri sahibinin kendi kişisel verilerine ve veri sorumlularının sağlaması gereken işleme hakkındaki bazı bilgilere erişme hakkı olmasını sağlamaktadır.[544] Özellikle, her veri sahibi kendisiyle ilgili verilerin işlenip işlenmediğine dair (veri sorumlusundan) rıza verme hakkına ve en azından aşağıdakilerle ilgili bilgilere sahip olmalıdır:

- Veri işleme amaçları;
- İlgili veri kategorileri;
- Verilerin paylaşıldığı taraflar veya taraf kategorileri;
- Verinin saklanması için öngörülen süre veya öngörülmesi mümkün değilse o süreyi belirlemek için kullanılan kriterler;
- Kişisel verileri düzeltme, silme veya kişisel veri işlemeyi sınırlandırma haklarının varlığı;
- Denetim otoritesine şikayette bulunma hakkı;
- Veri sahiplerinden veri toplanmazsa, işlenmekte olan verilerin toplandığı kaynak hakkında mevcut herhangi bir bilgi;
- Otomatik karar verme durumunda herhangi bir otomatik veri işlemesinin temelinde olan mantık

Veri sorumluları, veri sahibine işlenen kişisel verilerin bir kopyasını temin etmelidir. Veri sahibine iletilen her türlü bilginin anlaşılır bir şekilde sunulması gerekmektedir; bu veri sorumlusunun veri sahibine yaptığı bilgilendirmenin veri sahibinin anlayabilmesini sağlaması gerektiği anlamına gelmektedir. Örneğin, teknik kısaltmalar veya kodlanmış terimler dahil, bu terimlerin anlamı açıklanmadıkça genellikle bir erişim talebine verilen cevap yeterli olamayacaktır. Profilleme de dahil olmak üzere, otomatik karar vermenin gerçekleştirildiği yerlerde, otomatik karar verme sürecinin genel mantığını veri sahibini değerlendirirken dikkate alınan kriterler de dahil olmak açıklanması gerekecektir. Avrupa Konseyi hukukunda da benzer koşullar vardır. [545]

Örnek: Veri sahiplerinin kişisel verilerine erişmesi, verilerin doğru olup olmadığını tespit etmek için yardımcı olacaktır. Bu nedenle, veri sahibinin anlaşılır bir biçimde, yalnız şimdiye kadar işlenmekte olan gerçek kişisel veriler değil aynı zamanda isim, IP adresi, coğrafi konum koordinatları, kredi kartı numarası vb. gibi kişisel verilerin işlendiği kategoriler hakkında da bilgilendirilmesi germektedir.

Veri toplama kaynağı hakkında bilgi – verilerin veri sahibinden toplanmadığı durumlarda -, bu bilgilere erişildiği sürece erişim talebine cevap verilmesi gerekmektedir. Bu hükmün adil,

[543] CJEU, Ortak davalar C-141/12 and C-372/12, YS v. Minister voor Immigratie, Integratie en Asiel ve Minister voor Immigratie, Integratie en Asiel v. M ve S, 17 Temmuz 2014.
[544] Avrupa Birliği Genel Veri Koruması Regülasyonu, Madde 15/f.1
[545] Modernize Edilmiş 108 sayılı Sözleşme, Madde 8/1/c

şeffaflık ve hesap verilebilirlik ilkeleri bağlamında anlaşılması gerekmektedir. Veri sorumlularının talep cevap verme sorumluluğundan muaf tutulmaları için verilerin toplama kaynağı hakkındaki bilgileri tahrip edemez – erişim talebine alınmasına rağmen silme gerçekleşmemişse - ve yine de genel "hesap verilebilirlik" şartlarına uyması gerekir.

ABAD içtihat hukukunda belirtildiği gibi, kişisel verilere erişim hakkı zaman sınırlaması ile kısıtlanamaz. Veri sahiplerine, geçmişte gerçekleşen verilerin işlenmesi faaliyetleri hakkında bilgi edinmeleri için de uygun fırsat verilmelidir.

Örnek: *Rijkeboer Kararı'nda*[546] ABAD'dan, bireyin kişisel verilerinin paylaşım yapıldığı tarafları veya bu taraf kategoriyle ilgili verilere erişim hakkının ve verilerin içeriğine erişimi istediği tarihten bir yıl öncesine kadar sınırlı olup olmayacağını belirlemesi istenmiştir.

AB mevzuatının böyle bir süreye izin verip vermeyeceğinin belirlenmesi için, ABAD, 12. maddenin, Direktif'in amaçları doğrultusunda yorumlanmasına karar vermiştir. ABAD, ilk olarak veri sorumlusunun veri sahibinin düzeltme, silme veya erişimini engelleme kullanması için veya düzeltme yapılması, silinmesi veya erişimin engellenmesi için paylaşım yapılan üçüncü taraflara bildirim yapmasının veri sahibinin erişim hakkının gerekli olduğunu belirtmiştir. Veri sahiplerinin kişisel verilerinin işlenmesine itiraz etme haklarını veya şikayette bulunma ve tazminat talep etme haklarını kullanabilmelerini sağlamak için etkin bir erişim hakkı da gerekmektedir. [547]

Veri sahiplerine verilerin haklarının pratik etkilerini sağlamak için, ABAD "hakkın geçmişse bağlı olması gerektiğini belirtmiştir. Durum böyle olmasaydı, veri sahipleri kanuna aykırı veya yanlış olduğu düşünülen, silinmiş veya engellenmiş veriye sahip olma veya yasal işlemler yapma ve zarardan dolayı tazminat alma hakkını etkin bir şekilde kullanmayacaktı."

6.1.2 Düzeltme Hakkı

AB hukuku ve Avrupa Konseyi hukuku uyarınca, veri sahipleri kendi kişisel verilerini düzeltme hakkına sahiptir. Kişisel verilerin doğruluğu, veri sahipleri için yüksek düzeyde veri koruması için esastır.[548]

Örnek: *Ciubotaru v. Moldova Kararı'nda*[549] başvuran, talebini kanıtlayamadığı için etnik kökeninin resmi kayıtlarda Moldova'dan Romanya'lı olarak değiştiremediğini iddia etmiştir. AİHM, Devlet'lerin bireyin etnik kimliğini kaydederken nesnel kanıtlar talep etmesini kabul edilebilir olduğunu belirtmiştir. Böyle bir iddia tamamen öznel ve doğrulanmamış gerekçelere dayandığında yetkililer reddedebilirdi. Ancak başvuranın iddiası, kendi etnik kökeninin öznel bakış açısından daha fazlasına dayanıyor olmasıydı; Romen etnik grubu ile dil, isim, başkasıyla özdeşleştirme ve diğerleri ile objektif olarak doğrulanabilir bağlantılar sağlanabilmekteydi. Bununla birlikte, iç hukuk uyarınca başvuranın ailesinin Romen etnik grubuna ait olduğuna dair kanıt sağlanması istenmiştir. Moldova'nın tarihsel gerçekleri göz önüne alındığında böyle bir gereksinim, Sovyet otoritelerinin kişinin ailesi ile ilgili

[546] CJEU, C-553/07, College van burgemeester en wethouders van Rotterdam/M. E. E. Rijkeboer, 7 Mayıs 2009.
[547] Avrupa Birliği Genel Veri Koruma Regülasyonu, Madde 15/1/c ve f, 16,17/f.2 ve 21, ve Bölüm 8
[548] A.e.g Madde 16 ve Başlangıç Hükmü 65; Modernize Edilmiş 108 sayılı Sözleşme, Madde 9/1/e
[549] AİHM, Ciubotaru/Moldova, No. 27138/04, 27 Nisan 2010, paras. 51 ve 59.

kaydettiğinden başka bir etnik kimliğin kaydedilmesinde aşılamaz bir engel oluşturuyordu. Başvuranın iddiasını nesnel olarak doğrulanabilir kanıtlar ışığında incelemesini engellerken, Devlet başvuranın özel hayatına etkili bir şekilde saygı gösterilmesini sağlamak için aktif yükümlülüğünü yerine getirmekte başarısız olmuştur. Mahkeme, AİHS'in 8. maddesinin ihlal edildiğine karar vermiştir.

Bazı durumlarda, veri sahibinin örneğin bir adın yazılışını, bir adresin değişikliğini veya telefon numarasının basitçe düzeltilmesini talep etmesi yeterli olacaktır. AB ve Avrupa Konseyi hukukuna göre, hatalı kişisel veriler gereğinden fazla veya aşırı derece gecikme olmadan düzeltilmelidir. [550] Bununla birlikte, bu tür talepler veri sahibinin yasal kimliği veya yasal evrakların teslimi için doğru ikamet yeri gibi hukuki olarak önemli hususlarla bağlantılıysa, yalnızca düzeltme talepleri yeterli olmayabilir ve veri sorumlusunun iddia edilen yanlışlığın kanıtını talep etme hakkı mevcuttur. Bu tür talepler, veri sahibin makul olmayan ispat yüküne tabi tutulmamalı ve bu nedenle veri sahiplerinin verilerinin düzeltilmesi engellenmemelidir. [551]

Örnek: *Cemalettin Canlı v. Türkiye Kararı'nda*[552] AİHM ceza soruşturmasında hatalı polis raporunun olmasından dolayı AİHS'in 8. maddesinin ihlal edildiğine karar vermiştir. Başvuran yasadışı kuruluşlara üyelik iddiasıyla iki kez cezai davranışta bulunmuş ancak mahkum edilmemiştir. Başvuran tekrar tutuklanıp başka bir suç için yargılandığında, polis ceza mahkemesine başvuranın iki yasadışı örgütün üyesi olduğu söyleyen "ek suçlarla ilgili bilgi formu" başlıklı bir rapor sunmuştur. Başvuranın raporu ve polis kayıtlarını değiştirme isteği başarısız olmuştur. AİHM, polis raporunda yer alan bilgilerin AİHS m.8 kapsamına girdiği, otoriteler tarafından tutulan dosyalarda saklanan halka açık bilgilerin "özel hayata" girebileceğine karar vermiştir. Ayrıca, polis raporunun hazırlanması ve ceza mahkemesine sunulması da iç hukuka aykırıdır. Mahkeme madde 8'in ihlal edildiğine karar vermiştir.

Hukuk davası veya verinin doğru olup olmadığına karar vermek için bir kamu otoritesi nezdindeki işlemler sırasında, veri sahibi doğruluğa itiraz edildiğini ve resmi kararın beklediğini belirten bir maddenin koyulmasını veya notun alınmasını isteyebilir. [553] Bu süre zarfında, veri sorumlusunun verileri bu veriler doğruymuş gibi sunmamalı veya bu veriler değişikliğe uğramamalı, özellikle üçüncü taraflarla paylaşılmamalıdır.

6.1.3 Silme Hakkı ("unutulma hakkı")

Veri sahiplerine kendi verilerinin silinmesi hakkının verilmesi, veri koruma ilkelerinin etkili bir şekilde uygulanması için ve özellikle de verilerin en aza indirmesi (veri minimizasyonu (kişisel veriler, işlenme amacının gerektiği kadar ile sınırlı olmalıdır) ilkesi için çok önemlidir. Bu nedenle, silme hakkı hem Avrupa Konseyi hem de AB hukuki araçlarında bulunur. [554]

[550] Avrupa Birliği Genel Veri Koruma Regülasyonu, Madde 16; Modernize Edilmiş 108 sayılı Sözleşme, Madde 9/f.1
[551] AİHM, Rotaru/RomanYA [GC], No. 28341/95, 4 Mayıs 2000
[552] AİHM, Cemalettin Canli/TÜRKİYE, No. 22427/04, 18 Kasım 2008, paras. 33 ve 42–43; AİHM, Dalea/Fransa, No. 964/07, 2 Şubat 2010
[553] Avrupa Birliği Genel Veri Koruma Regülasyonu, Madde 16, ikinci cümlesi
[554] A.e.g, Madde 17

Örnek: *Segerstedt-Wiberg ve Diğerleri v. İsveç Kararı'ndaki*[555] başvuranlar belirli liberal ve komünist siyasi partilere üye olmuştur. Bu kişiler hakkındaki bilgilerin güvenliği sağlayan polis kayıtlarına girdiğinden şüpheleniyorlardı ve silinmesini istiyorlardı. AİHM, söz konusu verilerin saklanmasının yasal bir temeli olduğu ve meşru bir amaç izlediği konusunda ikna olmuştu. Bununla birlikte, AİHM bazı başvurucularla ilgili olarak, verilerin tutulmasının devam etmesinin özel hayatına orantısız bir müdahale olduğunu tespit etmiştir. Örneğin, bir başvurucunun durumunda yetkililer 1969'daki gösteriler sırasında polis kontrolüne şiddetli bir direnç gösterdiği iddia edilmiştir. AİHM, bu bilginin özellikle tarihi niteliği göz önünde alındığında, ilgili hiçbir ulusal güvenlik çıkarına sahip olamayacağını tespit etmiştir. Mahkeme, AİHM'in 8. maddesinin; beş başvurucudan dördünce ilişkin olarak, başvuruculların iddia ettiği eylemlerden bu yana uzun süre geçmesinden zaman aşımına uğraması nedeniyle verilerin saklı tutulmasına devam edilmesine gerek olmadığına ilişkin ihlal tespit etmiştir.

Örnek: *Brunet v. Fransa Kararı'nda*[556] başvuranlar, mahkum edilmiş kişiler, sanıklar ve mağdurlar hakkında bilgi içeren polis veri tabanında kişisel bilgilerinin saklanmasını istemektedir. Başvuranlar aleyhindeki kovuşturmalara son verilmiş olmasına rağmen, detayları veri tabanlarında yer almaktadır. AİHM, AİHS'in 8. maddesinin ihlal edildiğine karar vermiştir. Mahkeme karar verirken, uygulamada başvuruculların kişisel verilerinin veri tabanından silinmesinin mümkün olmadığına karar vermiştir. AİHM ayrıca veri tabanında yer alan bilgilerin niteliğini de göz önüne alarak veri sahibinin kimliğinin ve kişiliğinin ayrıntılarını içerdiği için başvurucunun mahremiyetine müdahale ettiği kabul etmiştir. Ayrıca, veri tabanında 20 yıl olan kişisel kayıtların tutulma süresinin, özellikle hiçbir mahkeme başvurucuyu mahkum etmemiş olması nedeniyle aşırı derecede uzundur.

Modernize Edilmiş 108 sayılı Sözleşme, her bireyin yanlış, hatalı veya yasadışı olarak işlenmiş verilerin silinmesi hakkına sahip olduğunu açıkça kabul etmiştir. [557]

AB hukukuna göre, GDPR'ın 17. maddesi, veri sahiplerinin verilerinin silinmesi veya silinmesini talep etmesini sağlar. Birinin kişisel verilerini gereğinden fazla gecikmeden silme hakkı aşağıdaki durumlarda geçerlidir:

- Kişisel veriler, toplandıkları veya işlendikleri başka amaçlar için artık gerekli değilse;
- Veri sahibinin veri işlenmesinin dayandığı veya işleme için başka bir yasal dayanağın bulunmadığı durumda rızasını geri çekerse;
- Veri sahibi verilerin işlenmesine itiraz etmiş ve verilerin işlenmesi için ağır basan bir meşru zemin yoksa;
- Kişisel veriler yasa dışı olarak işlenmişse;
- Kişisel verilerin, veri sorumlularının tabi olduğu Birlik veya Üye Devlet yasalarındaki hukuki bir zorunluluk ile uyumlu olması için silinmesi;

[555] CtHR, *Segerstedt-Wiberg and Others v. Sweden*, No. 62332/00, 6 June 2006, paras. 89 and 90; see also, for example, ECtHR, *M.K. v. France*, No. 19522/09, 18 April 2013
[556] AİHM, Brunet/Fransa, No. 21010/10, 18 Eylül 2014.
[557] Modernize Edilmiş 108 sayılı Sözleşme, Madde 9/1/e

- GDPR'ın 8. maddesi uyarınca çocuklardan bilgi toplumu hizmetlerinin sunulmasına ilişkin kişisel veriler toplanmışsa. [558]

Veri işlemenin meşru olduğunu ispat etme yükümlülüğü, işlemlerin yasal olmasından sorumlu oldukları için veri sorumluları üzerinde olacaktır. [559] Hesap verilebilirlik ilkesine göre, veri sorumlusu herhangi bir zamanda veri işlemenin sağlam yasal temele dayandığını gösterebilmelidir, aksi takdirde işlemin durdurulması gerekmektedir. [560] GDPR, aşağıdakiler için kişisel verilerin işlenmesinin gerekli olduğu durumlar da dahil olmak üzere, unutulma hakkına yönelik istisnalar belirtmiştir:

- İfade özgürlüğü ve bilgi edinme hakkını kullanmak;
- Veri sorumlusunun tabi olduğu Birlik veya Üye Devlet mevzuatlarının verilerin işlenmesini veya kamu yararını veya veri sorumlusuna verilen resmi makamın verdiği bir görevin yerine getirilmesini gerektiren yasal bir yükümlülüğe uyulması;
- Kamu sağlığı alanındaki kamu yararı nedenleri;
- Kamu yararına, bilimsel veya tarihi amaçlarına veya istatiksel amaçlara yönelik arşivleme amaçları;
- Hukuki hak taleplerin oluşturulması, kullanılması veya savunulması[561]

ABAD, yüksek düzeyde veri koruması sağlamak için silme hakkının önemini kabul etmiştir.

Örnek: *Google İspanya Kararı'nda*[562], ABAD'ın Google'ın, başvuran hakkındaki mali sıkıntısı ile ilgili eski bilgileri arama listesi sonuçlarından silmesi gerekip gerekmediğini değerlendirmiştir. Ayrıca, Google, yalnızca başvurucunun iflas olayı hakkında bir gazete bildirisi yayınlayanın, bilgiyi barındıranın internet sayfasına bir köprü rolünde olduğunu savunarak sorumluluğunun olmasına itiraz etmiştir.[563] Google, eski bir bilgiyi internet sayfasından silme isteğinin yalnızca haberin yer aldığı sayfaya bağlantı sağlayan Google'a değil, internet sayfasının ana bilgisayarına yapılması gerektiğini savunmuştur. ABAD, Google'ı eğer internette bilgi ve internet sayfalarını aradığında ve arama sonuçlarını sağlamak için içeriği dizine eklediğinde, AB yasaları uyarınca sorumlulukların ve yükümlülüklerin uygulanarak bir veri sorumlusu haline geldiği sonucuna varmıştır.

[558] Avrupa Birliği Genel Veri Koruma Regülasyonu, Madde 17/f.1
[559] A.e.g
[560] A.e.g., Madde 17/f.3
[561] A.e.g., Madde 17/f.3
[562] CJEU, C-131/12, Google İspanya SL, Google Inc./Agencia Española de Protección de Datos (AEPD), Mario Costeja González [GC], 13 May 2014, paras. 55–58.
[563]Google ayrıca, Goodle Inc.'nin ABD'de kurulmuş olması ve söz konusu kişisel verilerin işlenmesi durumunda ABD'de bu işlemin yapılması nedeniyle AB veri koruma kurallarının uygulanmasına da itiraz etmiştir. AB veri koruma hukuku uyarınca arama motorlarının, arama sonuçlarında görüntülenen veriler bakımından "veri sorumlusu" olarak kabul edilmemesi iddiasıyla ilgili ikinci bir argüman sunulmuş ve veriler hakkında bir bilgilerinin olmadığı veya bunlar üzerinde kontrol sahibi olmadıkları savunulmuştur. CJEU, her iki argümanı da reddetmiştir, 95/46/EC sayılı Direktif'in bu durumda uygulanabilir olduğunu ve özellikle kişisel verileri silme hakkının güvence altına alındığını incelemeye devam etmiştir.

ABAD, internet arama motorlarının ve kişisel veriye erişim sağlayan arama sonuçlarının, bir bireyin detaylı profilini oluşturabildiğini netleştirmiştir. [564] Arama motorları, böyle bir sonuç listesinde yer alan bilgileri her yerde yer alabilir. Potansiyel ciddiyetin ışığında, bu müdahale sadece böyle bir motorun operatörünün bu işlemdeki sahip olduğu ekonomik çıkarından haklı gösterilemez. Bilhassa internet kullanıcılarının, bilgiye erişimdeki meşru menfaatleri ile AB'nin Temel Haklar Bildirgesi'nin altındaki temel haklar ile arasında adil denge aranmalıdır. Giderek artan bir şekilde dijitalleşmiş bir toplumda, kişisel verilerin doğru olması ve gerekenin ötesinde geçememesi (ör. kamuya açık bilgiler için), bireylere yüksek düzeyde veri koruması sağlamak için esastır. "Verilerin işlenmesine ilişkin veri sorumlularının kendi sorumlulukları çerçevesinde, işlemlerin bu şartların yerine getirilmesini sağlayan yetkileri ve imkanı" sağlamalıdır, böylece oluşturulan hukuki garantilerin tam etkili olması gerekir. [565]

Bu, işlemin eski olduğu ve artık gerekli olmadığı durumlarda kişisel verilerinin silinme hakkının aynı zamanda bilgileri kopyalayan veri sorumlularını da kapsadığı anlamına gelmektedir. [566]

Google'ın başvuran ile ilgili bağlantıları kaldırmanın gerekli olup olmadığını değerlendiren ABAD, belirli koşullar altında kişinin kişisel verilerinin silinmesini isteme hakkına sahip olduğunu belirtmiştir. Bu hak, bir bireye ilişkin bilgilerin verilerin işlenmesi amaçları için hatalı, yetersiz, ilgisi olmayan veya orantısız olduğu durumlarda kullanılabilir. ABAD bu hakkın mutlak olmadığını diğer haklarla ve çıkarlarla, özellikle de haklın belirli bilgilere erişimi olan isteği ile dengelenmesi gerektiğini kabul etmiştir. Her bir silme talebi, kişisel verinin korunmasına ilişkin temel haklar ile veri sahibinin özel hayatı arasındaki temel hakları ve yaylayanlar da dahil olmak üzere tüm internet kullanıcılarının meşru menfaatleri arasında bir denge kurulması için olay üzerinde değerlendirilmelidir. ABAD, bu dengeleme çalışması sırasında göz önünde bulundurulacak kriterler hakkında rehberlik sağlamıştır. Aksine, eğer veri sahibi kamuya mal olmuş birin var olması veya bilginin kamuya açık olmasını haklı kılacak nitelikte olması durumunda, daha sonra genel halkın bilgiye erişimdeki üstün yararı, veri sahibinin veri koruma ve gizlilik konuları ile ilgili temel haklarına yapılan müdahaleyi haklı kılabilir.

Bu kararı takiben, Madde 29 Çalışma Grubu, ABAD Kararı'nı uygulamak için ilgili rehberleri kabul etmiştir.[567] Rehberler, denetim otoritelerinin, kişilerin silme talepleriyle ilgili şikayetleri ele alınırken kullanacakları kriterlerin, silme hakkının neleri içerdiğini açıklamak ve bu hakları dengelerken kullanacakları yolu gösteren ortak kriterlerin bir listesini içerir. Rehberler, yapılan değerlendirmelerin olay özelinde yapılması gerektiğini yinelemiştir. Unutulma hakkı mutlak

[564] A.e.g., paras. 36, 38, 80–81 ve 97
[565] A.e.g., paras 81-83
[566] CJEU, C-131/12, Google Spain SL, Google Inc. v. Agencia Española de Protección de Datos (AEPD), Mario Costeja González [GC], 13 Mayıs 2014, para. 88. Ayrıca bkz. Madde 29 Çalışma Grubu (WP29) (2014),"Google Spain and Inc v. Agencia Española de Protección de Datos (AEPD) and Mario Costeja González" CJEU Kararının uygulanması hakkında Rehber, C-131/12, WP 225, Brüksel, 26 Kasım 2014 ve CM/Rec 2012(3), Bakanlar Kurulu, üyelerine arama motorları bakımından insan haklarının korunmasına ilişkin Tavsiye Kararı, 4 Nisan 2012.

[567] Madde 29 Çalışma Grubu (WP 29) (2014), CJEU'nin "Google Spain and Inc v. Agencia Española de Protección de Datos (AEPD) and Mario Costeja González" Kararı'nın uygulanması hakkında Rehber, C-131/12, WP 225, Brussels, 26 Kasım 2014.

olmadığı için, bir talebin sonucu, söz konusu davaya bağlı olarak değişebilir. Bu aynı zamanda Google'dan sonra ABAD'ın içtihatlarında da belirtilmiştir.

Örnek: *Camera di Commercio di Lecce v. Manni Kararı'nda*,[568] CJEU, bir şirketin ticari varlığı sona erdiğinde, bir Ticaret Sicili Odası'ndan yayınlanan kişisel verilerinin silinme hakkına sahip olup olmadığını incelemesi gerekmiştir. Bay Manni, Lecce Ticaret Odası'ndan kişisel verilerinin sicilden silinmesini istemiş, potansiyel müşterilerin sicile bakacağını ve on yıldan daha fazla bir süre önce iflas ettiğini ilan eden bir şirketin yöneticisi olduğunu görmüştür. Başvurucu bu bilginin potansiyel müşterileri vazgeçirebileceğine inanmaktadır.

Manni'nin kişisel verilerinin korunma hakkını, kamunun bilgiye erişmedeki genel kamu yararı ile dengelemekle beraber, ABAD ilk önce kamu kayıtlarının tutulmasındaki amacı incelemiştir. Bilgilendirmenin kanuna uygun şekilde ve özellikle şirket bilgilerinin üçüncü şahıslar için daha kolay erişilebilir olmasını hedefleyen bir AB Direktif'i ile sağlandığına dikkat çekmiştir. Bu nedenle üçüncü taraflar, bir şirketin temel belgelerini ve "özellikle şirketi bağlayıcı yetkilere sahip olan kişilerin ayrıntılarını" ile ilgili şirket hakkındaki diğer bilgilere erişebilmeli ve bunları inceleyebilmelidirler. Bahsi geçen açıklamanın amacı, üçüncü tarafların AB'deki şirketler hakkındaki tüm ilgili bilgilere erişebilmelerini sağlayarak, Üye Devlet'ler arasındaki yoğun ticaret açısından yasal kesinliği sağlamaktır.

ABAD ayrıca, zaman geçtikten sonra ve hatta bir şirket dağıldıktan sonra bile, şirkete ilişkin hakların ve yasal yükümlülüklerin devam ettiğini belirtmiştir. Fesihle ilgili anlaşmazlıklar uzun sürebilir ve bir şirket yöneticileri ve tasfiye memurları ile ilgili sorular bir şirketin varlığının sonra ermeden yıllar sonra ortaya çıkabilir. ABAD, olası senaryoların kapsamı ve her Üye Devlet'te yapılan sınırlama sürelerindeki farklılıklar göz önüne alındığında "bir şirketin dağılmasından itibaren, tek bir zaman sınırının belirtilmesinin imkansız olduğunu, bu verilerin kayıt defterine dahil edilmesinin ve açıklanmasının artık gerekmeyecek" demiştir. Bilgilendirmenin meşru amacı ve üçüncü şahısların çıkarlarına zarar vermeden kişisel verilerin sicilden silinebileceği bir dönemin kurulmasındaki zorluklar nedeniyle ABAD, AB veri koruma kurallarından kişisel verileri silme hakkını Bay Manni'nin durumundaki kişiler için garanti etmediğini tespit etmiştir.

Veri sorumlusunun kişisel verileri herkese açık hale getirdiği ve bilgileri silmesi gerektiğinde verileri silmesinin zorunlu olduğu ve aynı verileri işleyen diğer sorumlularının da veri sahibinin silme isteği hakkında bilgi vermek için "makul" adımlar atmak zorundadır. Veri sahibinin verilerin silinmesi faaliyetinde mevcut teknolojileri ve uygulama maliyetini dikkate alınmalıdır.[569]

6.1.4. Düzeltme hakkı

GDPR'ın 18. maddesi, veri sorumlusunun kişisel verileri işlemesini geçici olarak kısıtlaması için veri sahiplerine güç vermektedir. Veri sahipleri veri sorumlularından aşağıdaki hallerde verilerinin işlenmesinin kısıtlanmasını isteyebilir:

---

[568] CJEU, C-398/15, *Camera di Commercio, Industria, Artigianato e Agricoltura di Lecce v. Salvatore Manni*, 9 March 2017

[569] Avrupa Birliği Genel Veri Koruma Regülasyonu, Madde 17/f.2 ve Başlangıç Hükmü 66

- Kişisel verilerin doğruluğuna itiraz edildiğinde;
- Verilerin işlenmesi hukuka aykırı olduğunda ve veri sahibinin kişisel verilerinin silinmesi yerine kısıtlanmasını talep ettiğinde;
- Yasal iddiaların sunulabilmesi veya savunulması için veriler saklanmalıdır;
- Veri sorumlusunun meşru menfaatinin veri sahibinin çıkarlarından veri sahibinin çıkarlarından üstün olduğu duruma ilişkin bir karar bekleniyor olması;[570]

Veri sorumlusunun kişisel verilerin işlenmesini kısıtlayabileceği yöntemler, örneğin seçilen verilerin başka işletim sistemine geçici olarak taşınmasını, verilerin kullanıcılar tarafından kullanılmamasını veya kişisel verilerin geçici olarak kaldırımını içerir.[571] Veri sorumlusu, kısıtlamanın kaldırılmasından önce veri sahibini bilgilendirmelidir. [572]

Kişisel verilerin düzeltilmesi veya silinmesi veya işlem kısıtlaması yapılması hakkında bildirimde bulunma yükümlülüğü

Veri sorumlusunun, kişisel verilerin paylaşıldığı her bir tarafa kişisel verinin herhangi bir şekilde düzeltilmesi veya silinmesi veya herhangi bir işlemin kısıtlanması hakkında eğer imkansız veya orantısız değil ise bildirimde bulunma yükümlülüğü vardır.[573] Veri sahibi bu paylaşım yapılan taraflar hakkında bilgi isterse, veri sorunlusu veri sahibine bu bilgileri sağlamalıdır.

6.1.5 Veri Taşınabilirliği Hakkı

GDPR uyarınca, veri sahipleri veri sorumlusuna sunduğu kişisel verilerin rıza esasına göre otomatik yollarla elde edildiği durumlarda veya sözleşmenin yerine getirilmesi için gerekli olduğu ve otomatik yollarla gerçekleştirildiği durumlarda, kişisel verilerin işlenmesinin gerekli olduğu durumlarda veri taşınabilirliği hakkına sahiptir. Veri taşınabilirliği hakkının, kişisel veri işlemenin rıza veya sözleşmeden başka bir yasal temele dayandığı durumlarda geçerli olamadığı anlamına gelir. [574]

Veri taşınabilirliği hakkı uygulanabilirse, veri sahipleri kişisel verilerinin teknik olarak mümkünse doğrudan bir veri sorumlusundan diğer veri sorumlusuna aktarılmasını sağlama hakkı verilir. [575] Bunu kolaylaştırmak için, veri sorumlusu veri sahipleri için veri taşınabilirliğini sağlayan birlikte çalışılabilir formatlar geliştirmelidir.[576] GDPR, birlikte çalışabilirliği kolaylaştırmak için bu formatların yapılandırılması, yaygın olarak kullanılması ve makine tarafından okunması gerektiğini belirtir. [577] Birlikte çalışabilirlik, geniş anlamda, bilgi sistemlerinin veri alışverişinde bulunma ve bilgi paylaşımını sağlama yeteneği olarak tanımlanabilir.[578] Kullanılan formatların amacı birlikte çalışabilirliği sağlamak olsa da GDPR

[570] Avrupa Birliği Genel Veri Koruma Regülasyonu, Madde 18/f.1
[571] A.e.g., Başlangıç Hükmü 67
[572] A.e.g., Başlangıç Hükmü 67
[573] Ad hoc Committee on Data Protection (CAHDATA), Kişisel Verilerin Otomatik Olarak İşlenmesi İle İlgili Bireylerin Korunmasına İlişkin Modernize Edilmiş 108 sayılı Sözleşme'nin Açıklayıcı Raporu,para. 79.
[574] A.e.g., Başlangıç Hükmü 68 ve Madde 20/f.1
[575] A.e.g., Madde 20/f.2
[576] A.e.g., Başlangıç Hükmü 68 ve Madde 20/f.1
[577] A.e.g., Başlangıç Hükmü 68
[578] Avrupa Komisyonu, sınırlar ve güvenlik için daha güçlü ve daha akıllı bilgi sistemleri üzerine iletişimi hakkında Tebliğ, COM(2016) 205 son hali, 2 Nisan 2016

sağlanacak olan format hakkında özel tavsiyeler vermemektedir: formatlar sektörler arasında farklılık gösterebilmektedir. [579]

Madde 29 Çalışma Grubu rehberler uyarınca, veri sahiplerinin kendi kişisel verileri üzerinde kontrol vermeyi amaçlayan "taşınabilirliğin seçilmesi, kullanıcı kontrolü ve kullanıcı yetkilendirmesini destekleme" hakkı vardır. [580] Rehberler aşağıdakileri içeren veri taşınabilirliğinin ana unsurlarını belirtir:

- Veri sahibinin veri sorumlusu tarafından yapılandırılmış, yaygın olarak kullanılan, makine tarafından okunabilir ve birlikte çalışabilir bir biçimde işlenen kendi kişisel verilerini alma hakkı;

- Eğer teknik olarak mümkünse, kişisel verileri bir veri sorumlusundan diğer veri sorumlusuna engelle karşılaşmadan iletme hakkı;

- Veri sorumluluğu rejimi – veri sorumlusu veri taşınabilirliği talebine cevap verdiğinde, veri sahibinin talimatlarını yerine getirir, veri sahibinin kime veri taşındığına karar vermesi koşuluyla paylaşım yapılan tarafın veri koruma yasasına uymasından sorumlu olmadıkları anlamına gelir;

- Veri taşınabilirliği hakkının kullanılması, GDPR'ın diğer haklarında olduğu gibi, herhangi bir diğer hakka halel getirmez.

6.1.6 İtiraz etme hakkı

Ver sahipleri, kendi durumlarına ilişkin gerekçelerle kişisel veri işlemeye itiraz etme hakkını kullanabilir ve doğrudan pazarlama amacıyla işlenen verilere itiraz edebilir. İtiraz etme hakkı otomatik yollarla kullanılabilir.

Veri sahiplerinin belirli durumlarıyla ilgili gerekçelerle itiraz etme hakkı

Veri sahiplerinin verilerinin işlenmesine genel itiraz etme hakkı yoktur.[581] GDPR'ın 21. maddesinin 1. fıkrası uyarınca, işlemlerin yasal dayanağının veri sorumlusunun kamu yararı için gerçekleştirilen bir görevi yerine getirmesi durumunda veya işlemin veri sorumlusunun meşru menfaatine dayandığı yerde veri sahibine kendi durumlarına ilişkin itirazları güçlendirme hakkı verilir.[582] İtiraz hakkı profilleme aktiviteleri için de geçerlidir. Benzer bir hak Modernize Edilmiş 108 sayılı Sözleşme'de kabul edilmiştir. [583]

Veri sahibinin özel durumuyla ilgili gerekçelerle itiraz etme hakkı, veri sahibinin veri koruma hakları ile diğer kişilerin verilerinin işlenmesindeki meşru hakları arasında doğru dengenin kurulmasını amaçlamaktadır. Bununla birlikte ABAD, veri sahibinin haklarının, "söz konusu bilginin niteliği ve veri sahibinin özel hayatına ve bu bilgiye sahip olma konusunda halkın ilgisine olan duyarlılığı bağlı olarak" 'genel bir kural olarak' bir veri sorumlusunun ekonomik

[579] Madde 29 Çalışma Grubu (2016), Veri taşınabilirliği hakkında Rehber, WP 242, 13 Aralık 2016 ve 5 Nisan 2017 tarihinde revize edilmiş, sayfa 13
[580] A.e.g
[581] Ayrıca bkz. AİHM, M.S./İsveç, No. 20837/92, 27 Ağustos1997 (sağlık verilerinin rıza veya itiraz etme imkanı olmadan iletildiği yerler) AİHM, Leander v. İsveç, No. 9248/81, 26 Mart 1987; AİHM, Mosley/Birleşik Krallık, No. 48009/08, 10 May 2011.
[582] Avrupa Birliği Genel Veri Koruma Regülasyonu, Başlangıç Hükmü 69; Madde 6/f.1/e ve f
[583] Modernize Edilmiş 108 sayılı Sözleşme, Madde 9/f.1/d; Profilleme Hakkında Tavsiye Kararı, Madde 5/f.3

çıkarlarından üstün olduğunu açıkça belirtmiştir. [584] GDPR uyarınca, ispat yükümlülüğü, verilerin işlenmesine devam etmek için gerekli zeminleri göstermesi gereken veri sorumlularına aittir. Benzer şekilde, Modernize Edilmiş 108 sayılı Sözleşme'nin Açıklayıcı Raporu, veri işleme konusundaki meşru gerekçelerin (veri sahiplerinin itiraz etme hakkından daha üstün olan) olay özelinde açıklanması gerektiğini açıklamaktadır.

Örnek: *Manni Kararı'nda*,[585] ABAD, kişisel verilerin ticaret sicilindeki ifşa edilmesinin meşru amacı nedeniyle, özellikle üçüncü tarafın çıkarlarını koruma ve yasal olarak kesinliği sağlama gereği nedeniyle, kural olarak Bay Manni'nin ticaret sicilinden kişisel verilerinin silinmesi hakkına sahip olmadığına karar vermiştir. Ancak, veri işlenmesine itiraz hakkının var olduğunu kabul ederek "hariç tutulamayacağını belirterek […], ilgili kişinin özel durumunun üstün olması ve meşru sebeplerin, sicile kaydedilen kişisel verilere erişimin sınırlı olduğunu haklı çıkaran özel durumlar olabilir, yeterince uzun bir sürenin bitiminde […] başvurularını açıklayabilecek özel menfaati olan üçüncü taraflarla sınırlıdır." şeklinde belirtmiştir.

ABAD, bireyin tüm ilgili durumunu ve üçüncü kişilerin şirket sicilinde bulunan kişisel verilere kısıtlı erişimin istisnai şekilde haklı çıkaracak meşru ve geçersiz kılma nedenleri olup olmadığını dikkate alarak. her davayı değerlendirmenin yerel mahkemelerin sorumluluğunda olduğunu düşünmüştür. Bununla birlikte, Manni Kararı'nda, Bay Manni kişisel verilerinin sicilde ifşa edildiğinden dolayı müşterilerinin etkilediği iddia edildiğinde, böyle meşru ve üstün kılan nedenlere sebep olarak değerlendirilemeyeceği açıklığa kavuşturulmuştur. Bay Manni'nin potansiyel müşterilerinin, Bay Manni'nin eski şirketinin iflasıyla ilgili bilgilere erişme konusunda meşru menfaatleri vardır.

Başarılı bir itirazın etkisi, veri sorumlularının söz konusu verileri artık işleyememesidir. Ancak itiraz öncesi veri sahiplerinin verileri üzerinde gerçekleştirilen işleme faaliyetleri meşru kalır.

Doğrudan pazarlama amacıyla verilerin işlenmesine itiraz etme hakkı

GDPR madde 21 fıkra 2 uyarınca, doğrudan pazarlama amacıyla kişisel verilerin kullanımına itiraz etme hakkını açıklamış ve e-Gizlilik Direktifi'nin 13. Maddesi de daha fazla açıklık getirmiştir. Bu tür bir hak Modernize Edilmiş 108 sayılı Sözleşme'nin ve Avrupa Konseyi'nin Doğrudan Pazarlama Tavsiye Kararı'nda belirtilmiştir. [586] Modernize Edilmiş 108 sayılı Sözleşme'nin Açıklayıcı Raporu, doğrudan pazarlama amaçlı verilerin işlenmesine itirazların, söz konusu kişisel verilerin neden koşulsuz olarak silinmesinin veya kaldırılmasının gerektiğini açıklığa kavuşturmaktadır. [587]

Veri sahibi, kişisel verilerinin doğrudan pazarlama amacıyla herhangi bir zamanda ve ücretsiz olarak kullanılmasına itiraz etme hakkına sahiptir. Veri sahipleri bu hak, diğer bilgilerden ayrı olarak açık bir şekilde bilgilendirilmelidir.

[584] CJEU, C-131/12, Google Spain SL, Google Inc./Agencia Española de Protección de Datos (AEPD), Mario Costeja González [GC], 13 Mayıs 2014 para. 81.
[585] CJEU, C-398/15, Camera di Commercio, Industria, Artigianato e Agricoltura di Lecce/Salvatore Manni, 9 Mart 2017, paras. 47 ve 60.
[586] Avrupa Konseyi, Bakanlar Kurulu (1985), doğrudan pazarlama amacıyla kullanılan kişisel verilerin korunması konusunda üye devlere Tavsiye Kararı (85)20, 25 Ekim 1985, Md. 4/f.1.
[587] Modernize Edilmiş 108 sayılı Sözleşme'nin Açıklama Raporu, para.79

Otomatik yolla olan kişisel verilerin işlenmesine itiraz hakkı

Kişisel bilgilerinin, bilgi toplumu hizmetleri için kullanıldığı ve işlendiği yerlerde, veri sahibinin kişisel verilerinin otomatik yollarla kişisel verilerinin işlenmesine itiraz etme hakkını kullanabilir. Bilgi toplumu hizmetleri, kural olarak ücret karşılığında elektronik olarak ve bir hizmet alan kişinin bireysel talebi üzerine sağlanan herhangi bir hizmet olarak tanımlanmaktadır. [588]

Bilgi toplumu hizmetleri sunan veri sorumluları, otomatik yollarla veri işlenmesine itiraz etme hakkının etkin bir şekilde kullanılmasını sağlamak için uygun teknik düzenlemelere ve prosedürlere sahip olmalıdır.[589] Örneğin; bu düzenlemeler internet sayfalarındaki çerezleri engellemeyi veya internet taramasının izlenmesini kapatmayı içerebilir.

Bilimsel veya tarihi araştırma amaçlı istatiksel amaçlar için itiraz hakkı

AB hukuku uyarınca, bilimsel araştırmalar geniş yorumlanmalıdır, örneğin teknolojik gelişmeler ve göstergeler, temel araştırmalar, uygulamalı araştırmalar ve özel olarak finanse edilen araştırmalar da dahildir. [590] Tüzük'ün ölen kişilere uygulanmaması gerektiği dikkate alarak, tarihi araştırmalar soyağacı amaçlı araştırmaları da içermektedir. [591] İstatiksel amaçlar, herhangi bir toplama işlemi ve istatistiksel araştırmalar için veya istatistiksel sonuçların üretimi için gerekli kişisel verilerin işlenmesi anlamına gelir.[592] Tekrarlamak gerekirse, bir veri sahibinin özel durumu, araştırma amacıyla kişisel verilerin işlenmesine itiraz etme hakkına ilişkin yasal dayanaktır. [593]

Bunun tek istisnası, kamu yararı nedeniyle yapılan bir görevin yerine getirilmesi için verilerin işlenmesinin gerekliliğidir. Ancak silme hakkı, bilimsel ya da tarihi araştırma amaçlı ya da istatistiksel amaçlarla verilerin işlenmesi (kamu yararı nedenleriyle ya da yararı olmadan) gerekli olduğunda uygulanamaz. [594]

GDPR, bilimsel, istatistiksel veya tarihi araştırmanın gerekliliklerini veya veri sahiplerinin 89. maddede belirtilen özel korumalarla ve istisnalarla haklarını dengelemektedir. Bu nedenle, Birlik veya Üye Devlet hukuku, araştırma hakkının gerçekleştirilmesini imkansız veya ciddi şekilde engelleyen ve bu amaçların yerine getirilmesi için gerekli olduğu takdirde, bu hakkın ihlal edilme ihtimalinin yüksek olduğu durumlarda, itiraz etme hakkına istisna oluşturabilir.

Avrupa Konseyi hukuku uyarınca, Modernize Edilmiş 108 sayılı Sözleşmenin 9. maddesinin 2. fıkrası, veri sahiplerinin temel hak ve özgürlüklerinin ihlal edilmesi riskinin bilinmesinin mümkün olmadığı durumlarda kamu yararı, bilimsel veya tarihi araştırmalarla arşivleme amacıyla verilerin işlenmesi ile ilgili veri koruma yasası dahil olmak üzere, veri sahiplerinin itiraz hakkı da dahil olmak üzere haklarına ilişkin kısıtlamalar getirilebileceğini belirtmektedir.

6.1.7. Profilleme dahil, otomatik bireysel karar alma

Otomatik kararlar, işlenen kişisel verilerin herhangi bir insani müdahale olmadan sadece

[588] 98/48 /EC sayılı Direktif ile değiştirilen 98/34/EC sayılı Direktif, teknik standartlar ve yönetmelikler alanında bilgi sağlanması için prosedür düzenler, Md. 1/f.2
[589] Avrupa Birliği Genel Veri Koruma Regülasyonu, Md. 21/f.5
[590] A.e.g., Başlangıç Hükmü 159
[591] A.e.g., Başlangıç Hükmü 160
[592] A.e.g., Başlangıç Hükmü 162
[593] A.e.g., Madde 21/f.6
[594] A.e.g., Madde 17/f.3/d

otomatik vasıtalar kullanılarak alınan kararlardır. AB hukuku altında, veri sahipleri hukuki etkileri olan ya da benzer ehemmiyette sonuçlar doğuran otomatik kararlara maruz bırakılmamalıdır. Şayet söz konusu kararların örneğin kredibiliteyle, online işe alımla, işteki performansla ya da davranış ya da güvenilirliğin analiz edilmesiyle bağlantılı olması nedeniyle kişilerin hayatında mühim etkileri olması muhtemelse, olumsuz etkilerin önlenmesi amacıyla özel koruma gerektirmektedir. Otomatik karar alma "bir gerçek kişiye ait, özellikle veri sahibinin işteki performansı, ekonomik durumu, sağlığı, kişisel tercih ve ilgi alanları, güvenilirliği ya da davranışı, konumu ya da hareketleriyle ilgili kişisel özelliklerin analiz edilmesi amacıyla" değerlendirilmesini ifade eden profillemeyi de içermektedir.[595]

Madde 29 Çalışma Grubu'na göre, veri sahiplerine yönelik hukuki etkiler doğurabilecek ya da önemli biçimde etkileyebilecek münhasıran otomatik işlemelere dayalı kararlara maruz kalmama hakkı genel bir yasağa eşittir ve veri sahibinin proaktif biçimde ilgili karara yönelik itirazda bulunmasını gerektirmez.[596]

Halbuki, GDPR'a göre, hukuki etkileri olan ya da ilgili kişiyi önemli biçimde etkileyen otomatik karar alma faaliyetleri veri sorumlusu ile veri sahibi arasında bir sözleşmenin kurulması ya da ifası için gerekliyse ya da veri sahibi açık rıza verdiyse kabul edilebilecektir. Keza otomatik karar alma, kanunlar tarafından izin verildiği hallerde ve veri sahibinin hakları, özgürlükleri ve meşru menfaatleri uygun önlemlerle korunduğu takdirde de kabul edilebilecektir.[597]

GDPR, ayrıca veri sorumlusunun kişisel verilerin toplandığı hallerde mevcut olan aydınlatma yükümlülüğüne yönelik, veri sahiplerinin profilleme dahil olmak üzere otomatik karar almanın olduğu hallerde bu hususta bilgilendirilmesi gerektiğini düzenlemektedir.[598] Veri sorumlusu tarafından işlenen kişisel verilere ulaşma hakkına halel gelmemektedir.[599] Aydınlatma sadece profillemenin yapılacağını belirtmekle kalmamalı, ayrıca profillemede yer alan mantığı ve ilgili kişilere yönelik öngörülen sonuçları da içermelidir.[600] Örneğin, başvurularda otomatik karar almadan yararlanan bir sağlık sigortası şirketi veri sahiplerine algoritmanın nasıl çalıştığına yönelik genel bilgi sağlamalı ve algoritmanın sigorta ücretlerini belirlemek için hangi faktörleri kullandığını belirtmelidir. Benzer şekilde, "erişim hakkı"nı kullanırken veri sahipleri veri sorumlusundan otomatik karar almanın varlığı ve mantığına dair anlamlı bilgiler talep edebilecektir.[601]

Veri sahiplerine verilen bu bilgiler şeffaflığı sağlama ve veri sahiplerinin bilgilendirilmiş şekilde rıza, eğer durum bu şekildeyse, vermesini mümkün kılma ya da insan müdahalesini sağlama amacı taşımaktadır. Veri sorumlusunun veri sahibinin haklarını, özgürlüklerini ve meşru menfaatlerini koruma amacıyla uygun önlemleri uygulama yükümlülüğü vardır.

Bu, en azından veri sorumlusu açısından insan müdahalesini temin etme hakkını ve veri sahibinin görüşünü iletme ve kişisel verilerinin otomatik işlenmesine karşı itirazda bulunabilme hakkını içermektedir.[602]

595 A.g.e., Başlangıç 71, Md. 4 (4) ve Md. 22.
596 Madde 29 Çalışma Grubu, 2016/679 sayılı Regülasyonun amaçları kapsamında Münhasıran Otomatik Karar-Alma ve Profilleme üzerine Rehber, WP 251, 3 Ekim 2017, sy. 15.
597 GDPR, Md. 22 (2).
598 A.g.e., Md. 12.
599 A.g.e., Md. 15.
600 A.g.e., Md. 13 (2) (f).
601 A.g.e., Md. 15 (1) (h).
602 A.g.e., Md. 22 (3).

Madde 29 Çalışma Grubu, GDPR kapsamında otomatik karar almanın kullanımı üzerine detaylı rehberler yayınlamıştır.[603]

Avrupa Konseyi hukuku altında, ilgili kişilerin kendilerini önemli biçimde etkileyecek ve münhasıran otomatik işlemeye dayalı bir karara görüşleri göz önüne alınmadan maruz kalmama hakkı vardır.[604] Kararların münhasıran otomatik işlemeye dayalı olduğu hallerde veri sahibinin görüşlerinin göz önüne alınması yükümlülüğü kişilerin bu tarz kararlara itiraz etme hakları olduğu ve veri sorumlusunun kullandığı kişisel verilerdeki hatalara karşı koyma ve kendilerine uygulanan profillerin ilintili olup olmadığına yönelik itirazda bulunabilme haklarının mevcut olduğu anlamına gelir.[605] Ancak ilgili kişi, otomatik kararın veri sorumlusunun tabi olduğu ve veri sahibinin haklarının, özgürlüklerinin ve meşru menfaatlerinin korunması adına uygun önlemlerin ortaya koyulduğu bir hukuktan kaynaklanması halinde bu hakkını kullanamayacaktır. İlaveten, veri sahiplerinin, talepleri üzerine, gerçekleştirilen veri işleme faaliyetlerinin arkasında yer alan muhakemeye dair bilgileri edinme hakları vardır.[606] Modernize Edilmiş Sözleşme 108'in Açıklayıcı Raporu kredi derecelendirme örneğini vermektedir. İlgili kişiler sadece pozitif ya da negatif derecelendirme kararını değil aynı zamanda söz konusu kararla sonuçlanan, kişisel verilerinin işlenmesini destekleyen mantığı da bilebilmelidir. "Bu unsurlara dair bilgi sahibi olunması itiraz etme hakkı ve yetkin bir otoriteye şikâyette bulunma hakkı gibi diğer esaslı korumaların etkili biçimde kullanılmasına katkı sağlamaktadır".[607]

Profilleme Tavsiyesi, hukuken bağlayıcı olmamasına karşın, profilleme bağlamında kişisel verilerin toplanması ve işlenmesine yönelik şartları belirtmektedir.[608] Profilleme bağlamındaki veri işlemenin adil, ölçülü ve belirlenmiş ve meşru amaçlara yönelik olmasının teminine yönelik hükümler içermektedir.

Ayrıca, veri sorumlularının veri sahiplerine sağlaması gereken bilgilere dair hükümler de içermektedir. Veri kalitesi prensibi – veri sorumlularına veri hataları unsurlarının düzeltilmesine, profillemenin yol açabileceği risk veya hataları sınırlandırmaya ve verilerin kalitesini ve kullanılan algoritmaları periyodik olarak değerlendirmeye yönelik tedbirler almayı şart koşan– de tavsiyede yer almaktadır.

6.2. Çözümler, yükümlülükler, cezalar ve tazminat

Kilit Noktalar

- Modernize Edilmiş Sözleşme 108'e göre, Sözleşmenin Taraflarının ulusal hukuku verilerin korunması hakkı ihlallerine karşı uygun çözüm ve yaptırımları belirlemek zorundadır.

- AB'de, GDPR veri sahiplerine haklarının ihlali durumunda çözümler sunmaktadır,

603 Madde 29 Çalışma Grubu (2017), 2016/679 sayılı Regülasyonun amaçları kapsamında Münhasıran Otomatik Karar-Alma ve Profilleme üzerine Rehber, WP 251, 3 Ekim 2017.
604 Modernize Edilmiş Sözleşme 108, Md. 9 (1) (a).
605 Modernize Edilmiş Sözleşme 108'in Açıklayıcı Raporu, para. 75.
606 Modernize Edilmiş Sözleşme 108, Md. 9 (1) (c).
607 Modernize Edilmiş Sözleşme 108'in Açıklayıcı Raporu, para. 77.
608 Avrupa Konseyi, Üye Devletlerin Bakanlar Komitesinin profilleme bağlamında otomatik veri işlemelere karşı kişilerin korunması hakkında Tavsiye CM/Rec(2010)13 Md. 5.

aynı zamanda regülasyonun hükümlerine uymayan veri sorumluları ve veri işleyenler için yaptırımlar belirlemektedir. Aynı zamanda tazminat hakkı ve yükümlülüğü düzenlemektedir.

- Veri sahiplerinin regülasyonu ihlalinin öne sürülmesi halinde denetleyici otoriteye başvurma hakkı vardır, ayrıca etkin adli çözüm ve tazminat elde etme hakları da mevcuttur.

- Etkin çözüm haklarının uygulamasında, ilgili kişiler veri koruma alanında aktif kâr amacı gütmeyen kuruluşlar tarafından temsil edilebilirler.

- Veri sorumlusu ya da veri işleyen ihlalden doğan tüm maddi ve maddi olmayan zararlardan sorumludur.

- Denetleyici otoritelerin regülasyonun ihlali halinde € 20,000,000'a kadar idari para cezası, ya da bir teşebbüs söz konusu olduğunda dünya çapındaki cirosunun %4'üne kadar idari para cezası uygulama yetkileri vardır – hangisi daha yüksekse

- Veri sahipleri veri koruma hukukuna yönelik ihlalleri son merci olarak ve belirli koşullar altında Avrupa İnsan Hakları Mahkemesi'nin önüne getirebilecektir.

- Bütün gerçek veya tüzel kişilerin Avrupa Veri Koruma Kurulu'nun kararlarının iptali için Anlaşmalarda belirtilen koşullar altında Avrupa Adalet Divanı'na başvurma hakkı vardır.

Yasal dokümanları kabul etmek Avrupa dahilinde kişisel verilerin korunmasını temin etmek için yeterli değildir. Avrupa veri koruma kurallarını etkin kılmak için, ilgili kişilerin ihlallere karşı çıkmalarına ve uğradıkları zararlara karşı tazminat talep etmelerine yarayacak mekanizmalar kurulması gerekmektedir.

Denetleyici otoritelerin somut ihlale yönelik etkili, caydırıcı ve ölçülü yaptırımlar uygulamaya yetkili olmaları da önem arz etmektedir.

Veri koruma hukuku altındaki haklar, hakları mevzubahis olan kişi tarafından kullanılacaktır; bu veri sahibi olan kişi olacaktır. Ne var ki, - ulusal hukuk kapsamındaki gerekli şartları yerine getiren – diğer kişiler de haklarının kullanılması hususunda veri sahiplerini temsil edebilir. Pek çok ulusal mevzuat kapsamında çocuklar ve akli engelleri bulunan kişiler vasileri tarafından temsil edilmelidir.[609] AB veri koruma hukuku altında, bir – hukuki amacı veri koruma haklarını desteklemek olan – kuruluş veri sahiplerini bir denetleyici otorite ya da mahkeme önünde temsil edebilir.[610]

6.2.1. Denetleyici otoriteye şikâyet arz etme hakkı

Hem Avrupa Konseyi hem de AB hukuku altında, ilgili kişilerin kişisel verilerine yönelik işleme faaliyetlerinin hukuka uygun biçimde yapılmadığını öne sürmeleri halinde yetkin denetleyici otoriteye talep ve şikayetleri arz etme hakları vardır.

609 FRA (2015), Çocukların haklarına dair Avrupa hukuku hakkında el kitabı, Lüksemburg, Yayınlar Bürosu; FRA (2013), Zihinsel engeli olan ve akıl sağlığı sorunu olan insanların hukuki ehliyeti, Lüksemburg, Yayınlar Bürosu.
610 GDPR, Md. 80. 622 Modernize Edilmiş Sözleşme 108, Md. 18.

Modernize Edilmiş Sözleşme 108 veri sahiplerinin uyruk ya da ikametlerinden bağımsız olarak sözleşme altındaki haklarını kullanmada bir denetleyici otoritenin yardımından yararlanma hakkını tanımaktadır. Yardım talebi ancak olağandışı durumlarda reddedilebilir ve veri sahipleri söz konusu yardıma yönelik masraf ve ücretleri ödememelidir.[611]

Benzer hükümler AB hukuk sisteminde bulunabilir. GDPR, denetleyici otoritelerin bir elektronik şikayet iletim formunun oluşturulması gibi şikayetlerin arz edilmesini kolaylaştıracak önlemleri benimsemesini şart koşmaktadır.[612] Veri sahibi arz edilecek şikayeti kendisinin mutat meskeninin bulunduğu, iş yerinin bulunduğu veya iddia edilen ihlalin meydana geldiği üye ülkedeki denetleyici otoriteye arz edebilecektir.[613]

Şikayetler araştırılmalıdır ve denetleyici otorite ilgili kişileri iddiaya yönelik işlemler konusunda bilgilendirmek zorundadır.[614]

AB kurum ve kuruluşları tarafından olası ihlaller Avrupa Veri Koruma Denetçisi'nin dikkatine sunulabilir.[615] EDPS'ten 6 ay içerisinde bir yanıt gelmemesi halinde, şikâyetin reddedildiği kabul edilecektir. EDPS kararlarına karşı başvurular AB kurum ve kuruluşlarına veri koruma kurallarına uymaları yönünde yükümlülükler getiren 45/2001 sayılı Regülasyon çerçevesinde Avrupa Adalet Divanı önüne getirebilecektir.

Ulusal veri koruma otoritesinin kararlarına yönelik mahkemelere başvuruda bulunma seçeneği mevcut olmalıdır. Bu durum veri sahiplerinin yanı sıra bir denetleyici otorite önünde yapılan işlemlere taraf olmuş veri sorumluları ve veri işleyenlere de uygulanır.

6.2.2. Etkin adli çözüm hakkı

Denetleyici otoriteye şikâyette bulunma hakkına ilaveten, ilgili kişiler etkin adli çözüm elde etme ve vakayı mahkeme önüne getirme haklarına sahip olmalıdır. Adli çözüm hakkı Avrupa hukuk geleneğinde yüceltilmiş bir haktır ve hem AB Temel Haklar Regülasyonu'nun 47. maddesinde hem de Avrupa İnsan Hakları Sözleşmesi'nin 13. maddesinde tanınmıştır.[616]

AB hukuku altında, veri sahiplerine haklarına yönelik ihlallerin söz konusu olduğu hallerde etkili hukuki çözümler sunulmasının önemi hem GDPR'ın hükümlerinde – denetleyici otoritelere, veri sorumlularına ve veri işleyenlere karşı etkin adli çözüm hakkı tesis etmektedir – hem de Avrupa Adalet Divanı içtihatlarında oldukça açıktır.

Örnek: Schrems davasında,[617] Avrupa Adalet Divanı, Safe Harbour Yeterlilik Kararı'nı geçersiz ilan etmiştir. Söz konusu karar AB'den ABD'de bulunan Safe Harbour tertibi altında onaylanmış kuruluşlara uluslararası veri aktarımlarına izin vermekteydi. Avrupa Adalet Divanı Safe Harbour tertibinin AB vatandaşlarının gizliliğinin korunması, kişisel verilerinin

611 A.g.e., Md. 16–17.
612 GDPR, Md. 57 (2).
613 A.g.e., Md. 77 (1).
614 A.g.e., Md. 77 (2).
615 Kişisel verilerinin Topluluğun kuruluş ve organları tarafından işlenmesine yönelik kişilerin korunması ve bu verilerin serbest dolaşımı hakkında 45/2001 sayılı 18 Aralık 2000 tarihli Avrupa Parlamentosu ve Konseyi Regülasyonu, OJ 2001 L 8.
616 Bkz: AİHM, Karabeyoğlu v. Türkiye, No. 30083/10, 7 Haziran 2016; AİHM, Mustafa Sezgin Tanrıkulu v. Türkiye, No. 27473/06, 18 Temmuz 2017.
617 CJEU, C-362/14, Maximillian Schrems v. Data Protection Commissioner [GC], 6 Ekim 2015.

korunması ve etkin adli çözüme yönelik temel haklarını tehlikeye atan birtakım eksiklikler içerdiğini göz önüne almıştır.

Gizlilik ve veri koruma haklarının ihlali açısından, Avrupa Adalet Divanı ABD mevzuatının belirli kamu otoritelerinin AB Üye Ülkelerinden ABD'ye aktarılan verilere orijinal aktarım amaçlarıyla uygun olmayan biçimde ve ulusal güvenliğin korunması noktasında gerekli ve ölçülü olmayan şekilde erişimine izin verdiğinin altını çizmiştir. Etkin çözüm hakkı açısından, kendilerine ait verilere erişim ve yok etme, silmeyi mümkün kılan veri sahiplerinin idari ya da adli tazmin araçlarına sahip olmadığını belirtmiştir. Avrupa Adalet Divanı kişisel verilere erişim, yok etme veya silmeye yönelik hukuki çözümler sunmayan mevzuatın "Tüzüğün 47. maddesinde yüceltilen etkin adli korumaya yönelik temel hakkın özüne saygı duymadığı" kanısına varmaktadır. Hukuk kurallarına uyumu garanti eden bir adli çözüm yolunun varlığının hukukun üstünlüğünün doğasında olduğunun altını çizmiştir.

Bir denetleyici otoritenin hukuken bağlayıcı kararına karşı çıkmak isteyen ilgili kişiler, veri sorumluları ve veri işleyenler yargılama yapılmak üzere mahkemenin önüne getirebilir.[618] "Karar" terimi denetleyici otoritenin şikayetin reddi dahil soruşturma, yaptırım ve yetkilendirme kuvvetlerinin uygulamasını kapsayacak şekilde geniş yorumlanmalıdır. Ancak, denetleyici otorite tarafından verilen görüş ya da tavsiyeler gibi hukuken bağlayıcı olmayan önlemler, mahkeme önüne getirilmek üzere konu olamazlar.[619]

Dava, ilgili denetleyici otoritenin kurulmuş olduğu Üye Ülkede yer alan mahkemelerde açılmalıdır.[620]

Bir veri sorumlusu ya da veri işleyenin veri sahibinin haklarını ihlal ettiği hallerde veri sahipleri mahkemeye şikâyette bulunma hakkına sahiptir.[621] Bir veri sorumlusu ya da veri işleyene karşı başlatılmış olan yargılamalarda ilgili kişilere davayı nerede açmak istediklerini seçme hakkının tanınması özellikle önem taşımaktadır. Bu kişiler gerek veri sorumlusu ya da veri işleyenin yerleşik olduğu Üye Ülkede gerekse veri sahibi olarak mutat meskenlerinin bulunduğu yerde davayı açabilirler.[622] İkinci seçenek ilgili kişilere yaşadıkları yerde ve aşina oldukları yargı yetkisi altında dava açma hakkı tanıması itibariyle haklarının kullanılmasını kolaylaştırmaktadır. Veri sorumluları ve veri işleyenlere karşı yapılacak yargılamalarda yargılama yerini bunların mukim olduğu yerle sınırlamak, diğer Üye Ülkelerde yerleşik olan veri sahiplerini seyahat ve diğer ilave masraflar dolayısıyla ve yargılamanın farklı bir dilde ve yargı yetkisinde yapılacak olması nedeniyle dava açmaktan caydırabilecektir. Tek istisna, veri sorumluları ya da veri işleyenlerin kamu kurumu olduğu hallerde veri işlemenin kamusal yetkilerin kullanımı sırasında gerçekleşmesidir. Bu durumda, sadece ilgili kamu kurumunun bulunduğu ülke mahkemeleri yetkilidir.[623]

Pek çok örnekte, veri koruma kurallarına dair davaların Üye Ülkelerin mahkemelerinde çözülecek olmasına karşın, bazı davalar Avrupa Adalet Divanı'na getirilebilecektir. İlk ihtimal bir veri sahibi, veri sorumlusu, veri işleyen ya da denetleyici otoritenin EPDB kararının iptalini talep etmesidir. Dava, öte yandan, TFEU'nun 263. Maddesindeki şartlara tabidir, dolayısıyla kabul edilebilmesi için ilgili kişi ve kurumların Kurul kararının kendilerini doğrudan ve bireysel olarak ilgilendirdiğini kanıtlamalıdır.

618 GDPR, Md. 78.
619 A.g.e., Başlangıç 143.
620 A.g.e., Md. 78 (223).
621 A.g.e., Md. 79.
622 A.g.e., Md. 79 (2).
623 A.g.e.

İkinci senaryo AB kurum ya da kuruluşlarının kişisel verileri hukuka aykırı olarak işlemesiyle ilgilidir. AB kuruluşlarının veri koruma hukukunu ihlal ettiği durumlarda, veri sahipleri taleplerini doğrudan AB Genel Mahkemesi (Genel Mahkeme Avrupa Adalet Divanı'nın bir parçasıdır) önüne getirebilecektir. Genel Mahkeme, ilk etapta, AB hukukunun AB kuruluşları tarafından ihlaline dair şikayetlerde yetkilidir.

Buna mukabil, EDPS hakkındaki şikayetler – bir AB kuruluşu olarak – Genel Mahkeme önüne getirilebilir.[624]

Örnek: Bavarian Lager davasında,[625] şirket Avrupa Komisyonu'ndan Komisyon'un şirketi ilgilendiren hukuki sorularla bağlantılı olarak yapmış olduğu iddia edilen toplantının tamamına erişim sağlanmasını talep etmiştir. Komisyon şirketin bu erişim talebini baskın veri koruma menfaatlerine dayanarak reddetmiştir.[626] Bavarian Lager, bu karara dair AB Kuruluşları Veri Koruma Regülasyonu'nun 32. maddesi altında, ilk derece mahkemesine (Genel Mahkeme'nin öncülü) şikâyette bulunmuştur. İlk derece mahkemesi kararında (dava T194/04, The Bavarian Lager Co. Ltd v. Commission of the European Communities), Komisyon'un kararını iptal etmiştir. Avrupa Komisyonu bu karara karşı Avrupa Adalet Divanı'na başvurmuştur.

Avrupa Adalet Divanı (Yüce Divan'da) ilk derece mahkemesinin kararını bir kenara koymak suretiyle Avrupa Komisyonu'nun toplantıdaki kişilerin kişisel verilerini korumaya yönelik toplantıya erişime dair ret kararını kabul etmiştir. Avrupa Adalet Divanı, katılımcıların kişisel verilerinin aktarılmasına yönelik rızalarını vermemiş olmamaları dolayısıyla söz konusu bilgilerin açıklanmasını reddetmekte Komisyonu haklı bulmuştur. İlaveten, Bavarian Lager söz konusu bilgilere erişilmesinin gerekliliğini kanıtlamamıştı.

Son olarak, veri sahipleri, denetleyici otoriteler, veri sorumluları veya veri işleyenler, yerel yargılamalar esnasında, ulusal mahkemeden, Avrupa Adalet Divanı'nın AB kurum, kuruluş, ofis ve bürolarının eylemlerinin yorumlaması ve geçerliliğine dair açıklık getirmesini talep etmesini isteyebilir. Söz konusu açıklamalar ön karar olarak bilinmektedir. Bu şikayetçi için doğrudan çözüm değildir, ancak ulusal mahkemelerin AB hukukunu doğru uygulamalarının temininin sağlanmasını mümkün kılar. Digital Rights Ireland ve Kärntner Landesregierung ve Diğerleri[627] ve Schrems[628] davaları gibi AB veri koruma hukukunun gelişimini önemli biçimde etkileyen yeni davaların Avrupa Adalet Divanı'na ulaşması bu ön karar mekanizması sayesinde olmuştur.

Örnek: Digital Rights Ireland ve Kärntner Landesregierung ve Diğerleri 641[629] İrlanda Yüksek Mahkemesi ve Avusturya Anayasa Mahkemesi tarafından başvurulan bir birleşmiş davadır ve 2006/24/EC sayılı Direktifin (Veri Saklama Direktifi) AB veri koruma hukukuyla

624 45/2001 sayılı Regülasyon (EC), Md. 32 (3).
625 CJEU, C-28/08 P, Avrupa Komisyonu v. The Bavarian Lager Co. Ltd [GC], 2010.
626 Argümanın analizi için bkz: EDPS (2011), Bavarian Lager kararı sonrası kişisel veri içeren dokümanlara kamu erişimi, Brüksel, EDPS.
627 CJEU, Müşterek davalar C-293/12 ve C-594/12, Digital Rights Ireland Ltd v. Minister for Communications, Marine ve Natural Resources ve Diğerleri ve Kärntner Landesregierung ve Diğerleri [GC], 8 Nisan 2014.
628 CJEU, C-362/14, Maximilian Schrems v. Data Protection Commissioner [GC], 6 Ekim 2015.
629 CJEU, Müşterek davalar C-293/12 ve C-594/12, Digital Rights Ireland Ltd v. Minister for Communications, Marine ve Natural Resources ve Diğerleri ve Kärntner Landesregierung ve Diğerleri [GC], 8 Nisan 2014.

uyumu ile ilgilidir. Avusturya Anayasa Mahkemesi Avrupa Adalet Divanı'na AB Temel Haklar Regülasyonu'nun 7,9 ve 11. Maddeleri ışığında Direktif Madde 3-9'un geçerliliğine dair sorular iletmiştir. Bu sorular, Veri Saklama Direktifi'nin yerine geçen Telekomünikasyon hakkındaki Avusturya Federal Kanunu'nun belirli hükümlerinin eski Veri Koruma Direktifi ve AB Kuruluşları Veri Koruma Regülasyonu ile uyumlu olup olmadığını da içermekteydi.

Kärntner Landesregierung ve Diğerleri davasında, Bay Seitlinger – Anayasa Mahkemesi yargılamasındaki müracaat sahiplerinden biri – telefon, internet ve e-postayı hem iş amacıyla hem de özel hayatında kullandığını söylemiştir. Bu nedenle, göndermiş ve almış olduğu bilgiler kamu telekomünikasyon şebekelerinden geçmiştir. 2003 tarihli Avusturya Telekomünikasyon Yasası altında, telekomünikasyon sağlayıcısı şebekeyi kullanımına dair verileri toplama ve muhafaza etmeye kanunen yükümlüydü. Bay Seitlinger, şebeke aracılığıyla bilgi gönderimi ve alımının teknik amaçları açısından kişisel verilerinin toplanması ve muhafazasının gerekli olmadığı inancındaydı. Ayrıca, söz konusu verilerin toplanması ve muhafaza edilmesi fatura edilmeye yönelik amaçlar açısından da gerekli değildi. Bay Seitlinger sadece 2003 tarihli Avusturya Telekomünikasyon Yasası dolayısıyla toplanan ve muhafaza edilen kişisel verilerinin bu şekilde kullanımına rıza göstermediğini ifade etmiştir.

Buna binaen, Bay Seitlinger Avusturya Anayasa Mahkemesi önünde dava açmış ve telekomünikasyon sağlayıcısının kanuni yükümlülüklerinin AB Temel Haklar Regülasyonu'nun 8. maddesi kapsamındaki temel haklarını ihlal ettiğini öne sürmüştür. Avusturya mevzuatının AB hukukunu (o zamanki Veri Saklama Direktifi) uyguladığını göz önüne alarak, Avusturya Anayasa Mahkemesi konuyu Direktif'in AB Temel Haklar Regülasyonu'nde yüceltilmiş olan gizlilik ve veri korunması haklarıyla uyumlu olup olmadığına karar verilmesi için Avrupa Adalet Divanı'na taşımıştır.

Avrupa Adalet Divanı (Yüce Divanı) dava üzerine karar vermiştir ve bu karar AB Veri Saklama Direktifi'nin iptaliyle sonuçlanmıştır. Avrupa Adalet Divanı, Direktif'in gizlilik ve veri korunması temel haklarına yönelik gerekli olanla sınırlı olmayan ciddi müdahaleler içerdiği kanaatine varmıştır. Direktif ulusal otoritelere ciddi suçları soruşturma açısından ilave olanaklar sunmasıyla meşru bir amaç taşımakta idi ve ceza soruşturmaları açısından değerli bir araçtı. Ancak Avrupa Adalet Divanı temel haklara yönelik sınırlandırmaların ancak sıkı sıkıya gerekli olduğu hallerde uygulanabileceğini ve kapsamlarını belirten açık ve net kuralların eşlik etmesi ve ilgili kişiler için korumalar içermesi gerektiğini ifade etmiştir.

Avrupa Adalet Divanı'na göre, Direktif gereklilik testini geçememiştir. İlk olarak, müdahalenin kapsamını belirleyen açık ve net kurallar koymamıştır. Saklanan veri ve söz konusu ciddi suç arasında bir illiyet olmasını şart koşmak yerine, Direktif bütün elektronik komünikasyon araçlarının bütün kullanıcılarına ait bütün üst veriye uygulanmaktaydı. Bu nedenle orantısız sayılabilecek şekilde neredeyse bütün AB nüfusunun gizlilik ve veri korunması haklarına bir müdahale teşkil etmekteydi. Kişisel verilere erişme yetkisine sahip kişileri sınırlandıracak koşulları içermemekteydi ve söz konusu erişim, erişim öncesinde bir idari otoritenin ya da mahkemenin onayını almak gibi bir usuli koşula bağlanmamıştı. Son olarak Direktif saklanan verinin korunması açısından açık korumalar belirlememekteydi. Dolayısıyla verilerin kötüye kullanma riskine ve hukuka aykırı erişim ve kullanıma karşı korunmasını temin etme açısından yetersiz kalmıştır.[630]

630 CJEU, Müşterek davalar C OÜ Viking Line Eesti [GC], 11 Aralık 2007, para. 85. Modernize Edilmiş Sözleşme 108, Md. 12.-293/12 ve C-594/12, Digital Rights Ireland Ltd v. Minister for Communications, Marine

Genel prensip olarak, Avrupa Adalet Divanı bu sorulara cevap vermeli ve ön karar vermeyi söz konusu yanıtın somut olayla alakalı olmadığını ya da vakitli olmadığını iddia ederek reddetmemelidir. Öte yandan, görev alanına girmediği gerekçesiyle soruyu reddedebilecektir.[631] Avrupa Adalet Divanı sadece ön karar için iletilen talebin kurucu unsurlarına dayalı olarak karar verirken, ulusal mahkeme somut dava üzerinde karar vermek üzere yetkisini korumaktadır.[632]

Avrupa Konseyi hukuku altında, Modernize Edilmiş Sözleşme 108'in hükümlerinin ihlaline karşı Sözleşmenin Tarafları uygun adli ve adli olmayan çözümleri ortaya koymalıdır.[633] Bütün mevcut yerel kanun yolları tüketildiğinde, Avrupa İnsan Hakları Sözleşmesi'nin 8. maddesine karşı gelen veri koruma hakkı ihlallerine yönelik iddialar, ayrıca Avrupa İnsan Hakları Mahkemesi'nin önüne getirilebilecektir. 8. maddenin ihlaline yönelik Avrupa İnsan Hakları Mahkemesi'ne yapılacak savunmalar da kabul edilebilirlik kriterlerini karşılamalıdır (AİHS Madde 34-35).[634]

AİHM'e yapılacak başvuruların sadece Sözleşmenin Taraflarına yönlendirilebilecek olmasına karşın, dolaylı olarak özel tarafların eylemleri ve ihmallerine de bakılabilecektir; şu kadar ki, Sözleşmenin Taraflarından biri AİHS altındaki pozitif yükümlülüğünü yerine getirmemiş ve ulusal hukukundaki veri koruma haklarına yönelik ihlallere karşı yeterli koruma sağlamamış olmalıdır.

Örnek: K.U. v. Finland davasında[635], başvuran kişi – reşit olmayan bir kişi- bir çevrimiçi randevu sitesinde kendisi hakkında seksüel içerikli bir reklamın yayımlandığı yönünde şikayette bulunmuştur. Servis sağlayıcı söz konusu şeyi yayımlayan kişinin kimliğini Finlandiya hukuku kapsamındaki gizlilik yükümlülükleri nedeniyle açığa çıkarmamıştır. Başvuru sahibi Finlandiya hukukunun bu tür gerçek kişilerin itham edici verileri internete koymasına karşı yeterli korumayı sağlamadığını iddia etmiştir. AİHM, devletlerin sadece ilgili kişilerin özel hayatlarına müdahalede bulunmaktan kaçınmaya değil, "ilgili kişilerin aralarındaki ilişkilerde özel hayatın gizliliğine saygının korunması için gerekli önemlerin alınması"na yönelik pozitif yükümlülüğe de tabi olabileceğine karar vermiştir. Başvuranın olayında, kendisinin pratik ve etkin olarak korunması için failin belirlenmesi ve yargılanması için etkili adımların atılmasını gerektirmekteydi. Ancak, devlet gerekli korumayı sağlamamış olup, Mahkeme AİHS'nin 8. Maddesinin ihlal edildiğine karar vermiştir.

Örnek: Köpke v. Germany vakasında,[636] başvuru sahibinin işyerinde hırsızlık yaptığından şüphelenilmekteydi ve kamera kayıtlarının gizli kalması yönünde itirazda bulundu. AİHM, "yerel otoritelerin takdir payı dahilinde başvuranın Madde 8 altındaki özel hayatın gizliliğine saygı duyulmasını isteme hakkı ile işverenin mülkiyet hakkının korunması hakkı ve kamu menfaati arasında adil bir denge kurmada başarısız olduğunu gösteren bir husus olmadığı" sonucuna varmıştır. Bu nedenle, başvurunun kabul edilmediği ilan edilmiştir.

---

ve Natural Resources ve Diğerleri ve Kärntner Landesregierung ve Diğerleri [GC], 8 Nisan 2014, para. 69.
631 CJEU, C-244/80, Pasquale Foglia v. Mariella Novello (No. 2), 16 Aralık 1981; CJEU, C-467/04, Gasparini ve Diğerlerine karşı Ceza Yargılamaları, 28 Eylül 2006.
632 CJEU, C-438/05, International Transport Workers' Federation, Finnish Seamen's Union v. Viking Line ABP,
633 OÜ Viking Line Eesti [GC], 11 Aralık 2007, para. 85. Modernize Edilmiş Sözleşme 108, Md. 12.
634 AİHS, Md. 34–37.
635 AİHM, K.U. v. Finlandiya, No. 2872/02, 2 Aralık 2008.
636 AİHM, Köpke v. Almanya (dec.), No. 420/07, 5 Ekim 2010.

AİHM, Sözleşmenin Taraflarından birinin AİHS altında korunan haklardan birini ihlal ettiği kanısına varırsa, ilgili taraf AİHM'in kararını uygulamakla yükümlüdür (AİHS Madde 46). Uygulama önlemleri öncelikle ihlalin sonlandırılmasını sağlamalı ve, mümkün olduğu oranda, başvuran tarafa yönelik negative etkilerini çözüme kavuşturmalıdır. Kararların uygulanması aynı zamanda Mahkemenin tespit ettiği ihlale benzer ihlallerin önlenmesi için mevzuatta değişiklik, içtihat ya da diğer yollarla alınacak genel önlemleri de gerektirebilecektir.

AİHM'in AİHS'ye yönelik ihlal tespit etmesi halinde, AİHS Madde 41 başvuru sahibine masrafları ilgili tarafa ait olmak üzere "adilane tazmin" sağlanabileceğini öngörmektedir.

Bir kar amacı gütmeyen kurum, kuruluş veya birlik dikte etme hakkı

GDPR, ilgili kişilerin kendilerini temsil etmek üzere bir kar amacı gütmeyen kurum, kuruluş veya birliğe dikte etmesini denetleyici otoriteye şikayet ileterek ya da mahkeme önüne taşıyarak talep etmelerini mümkün kılmaktadır.[637] Söz konusu kar amacı gütmeyen kuruluşlar, kamu menfaati çerçevesinde yasal amaçlara sahip olmalıdır ve veri koruma alanında aktif olmalıdır. Bu kuruluşlar şikayeti arz edebilir ya veri sahiplerinin namına adli çözüm hakkını kullanabilir. Regülasyon, Üye Devletlere – ulusal hukuka uygun olarak – bir kuruluşun veri sahipleri namına söz konusu veri sahipleri tarafından yönlendirilmeden şikayetleri arz edip edemeyeceği hususunda seçme hakkı tanımaktadır. İşbu temsil hakkı, ilgili kişilerin söz konusu kar amacı gütmeyen kurumların ekspertiz ve organizasyonel ve finansal kapasitesinden yararlanabilmesini sağlamakta ve dolayısıyla ilgili kişilerin haklarının kullanımını oldukça kolaylaştırmaktadır. GDPR, bu kuruluşlara birden çok veri sahibinin namına kolektif iddialarda bulunma hakkı tanımaktadır. Bu durum benzer iddiaların grup halinde yapılması ve beraber incelenmesi dolayısıyla yargı sisteminin fonksiyonu ve verimliliğine de katkı sağlamaktadır.

6.2.3. Yükümlülük ve tazminat hakkı

Etkin çözüm hakkı ilgili kişilere kişisel verilerinin uygulanabilir hukuku ihlal eden biçimde işlenmesinden dolayı maruz kaldığı zararlar için tazminat talep etme yetkisi tanımalıdır. Veri sorumluları ve işleyenlerin hukuka aykırı veri işlemeden doğan yükümlülükleri GDPR'da açıkça belirtilmektedir.[638] Regülasyon, ilgili kişilere hem maddi hem de maddi olmayan zararlar için tazminat elde etme hakkı vermektedir öte yandan gerekçe kısmında "zarar kavramı Avrupa Adalet Divanı içtihatları ışığında regülasyonun amaçlarını yansıtan bir biçimde geniş yorumlanmalıdır" ifadesi vardır.[639] Veri sorumluları regülasyon altındaki yükümlülüklerine uymadığı takdirde sorumludur ve tazminat taleplerine maruz kalabilecektir. Kişisel veri işleyenler, sadece regülasyonun spesifik olarak veri işleyenlere yönelik ortaya koymuş olduğu yükümlülüklere uymadıkları zamanlarda ya da veri sorumlusunun hukuka uygun talimatlarının dışında veya onlara aykırı olarak davranmasının sonucunda ortaya çıkan zararlardan sorumludur. Bir veri sorumlusu ya da veri işleyen tamamen tazminat ödediğinde, GDPR'a göre ilgili veri sorumlusu ya da veri işleyen – aynı veri işleme faaliyetine dahil olan diğer veri sorumluları ya da veri işleyenlerden – tazminatın zarardan sorumlu oldukları oranına karşılık gelen miktarını talep edebilecektir.[640] Aynı zamanda, sorumluluğun istisnaları çok katıdır ve veri sorumlusu ya da veri işleyenin zararın meydana gelmesine sebep olan olaydan herhangi bir şekilde sorumlu olmadığının kanıtlanmasına tabidir.

Tazminat, meydana gelen zarara ilişkin olarak "tam ve etkin" olmalıdır. Zarara birden fazla veri

[637] GDPR, Md. 80
[638] A.g.e., Md. 82.
[639] A.g.e., Başlangıç 146.
[640] A.g.e., Md. 82 (2) ve (5).

sorumlusu ve veri işleyen tarafından sebep olunduğu hallerde her bir veri sorumlusu veya veri işleyen zararın tamamından sorumlu tutulmalıdır. Bu kural veri sahipleri için etkili tazminatın temin edilmesini amaçlamakta ve veri işleme faaliyetinde yer alan veri sorumluları ve veri işleyenlerce koordine biçimde uyumun sağlanmasını hedeflemektedir.

Avrupa Konseyi hukuki çerçevesinde, Modernize Edilmiş Sözleşme 108'in 12. Maddesi Sözleşmenin Taraflarının sözleşmenin yükümlülüklerini uygulamaya sokan ulusal hukuk düzenlemelerinin ihlali için uygun hukuki çarelerin oluşturulmasını şart koşmaktadır. Modernize Edilmiş Sözleşme 108'in Açıklayıcı Raporu bir karar ya da uygulamaya adli olarak karşı çıkma imkanının hukuki çareler içerisinde yer alması gerektiğini ayrıca adli olmayan çarelerin de mümkün kılınmasının zorunlu olduğunu belirtmektedir.[641] Söz konusu çarelere erişime yönelik yöntem ve farklı kurallar, takip edilecek prosedürle birlikte, her bir Sözleşme Tarafının takdirine bırakılmıştır. Sözleşmenin tarafları ve ulusal mahkemeler, veri işlemeden kaynaklanan maddi ve maddi olmayan zararlara yönelik finansal tazminat hükümlerini ve onun yanında kolektif aksiyona olanak verilmesi ihtimalini göz önüne almalıdır.[642]

6.2.4. Yaptırımlar

Avrupa Konseyi hukuku altında, Modernize Edilmiş Sözleşme 108'in 12. Maddesi, Sözleşme 108'de belirlenmiş olan temel veri koruma prensiplerine etkinlik tanıyan yerel kanun hükümlerinin ihlaline karşı her bir Sözleşme Tarafı tarafından uygun yaptırım ve çarelerin oluşturulması zorunluluğunu düzenlemektedir. Sözleşme belirli bir dizi yaptırım oluşturmamakta ya da empoze etmemektedir. Aksine, her bir Sözleşme Tarafının adli ya da adli olmayan yaptırımların doğası hakkında karar vermek üzere takdir yetkisi olduğunu belirtmektedir. Bunlar cezai, idari ya da mülki olabilecektir. Modernize Edilmiş Sözleşme 108'in Açıklayıcı Raporu yaptırımların etkin, ölçülü ve caydırıcı olması gerektiğini belirtmektedir.[643] Sözleşmenin Tarafları yerel hukuk düzenlerinde mevcut olan yaptırımların doğası ve ağırlığını belirlerken bu prensibe saygı göstermek zorundadır.

AB hukuku altında, GDPR'ın 83. Maddesi üye ülkelerin denetleyici otoritelerine Regülasyonun ihlali halinde idari para cezaları uygulama yetkisi vermektedir. Cezaların seviyesi, ulusal otoritelerin ceza uygulayıp uygulamamaya yönelik karar alırken göz önünde bulunduracağı hususlar ve cezanın sınırları da 83. maddede belirtilmektedir. Böylece, yaptırım rejimi AB sathında uyumlu hale getirilmiş olmaktadır.

GDPR cezalara yönelik aşamalı bir yaklaşım takip etmektedir. Denetleyici otoritelerin Regülasyonun ihlali halinde € 20,000,000'a kadar ya da, bir teşebbüsün söz konusu olması halinde, dünya çapındaki cirosunun %4'üne kadar – hangisi yüksekse - idari para cezası uygulama yetkileri vardır. Bu gibi bir cezayı tetikleyebilecek ihlaller; veri işlemenin temel prensiplerine ve rızanın şartlarına yönelik ihlalleri, veri sahibinin haklarının ihlalini ve kişisel verilerin üçüncü ülkelere aktarımını düzenleyen hükümlerin ihlalini içermektedir. Diğer ihlaller açısından ise denetleyici otorite € 10,000,000'a kadar ya da, bir teşebbüsün söz konusu olması halinde, dünya çapındaki cirosunun %2'sine kadar – hangisi yüksekse - para cezası uygulayabilecektir.

Uygulanacak cezanın tipi ve seviyesi belirlenirken, denetleyici otoriteler bir dizi faktörü göz önüne almalıdır.[644] Örneğin, ihlalin tabiatını, ehemmiyetini ve süresini, ilgili kişisel veri

[641] Modernize Edilmiş Sözleşme 108'in Açıklayıcı Raporu, para. 100.
[642] A.g.e.
[643] A.g.e.
[644] GDPR, Md. 83 (2).

kategorilerini ve ihlalin bilinçli ya da ihmale dayalı bir karakteri olup olmadığını göz önüne almak zorundadırlar. Veri sorumlusu ya da işleyenin veri sahibinin maruz kaldığı zararı azaltmak için aksiyona geçmiş olduğu hallerde bu durum da dikkate alınmalıdır. Benzer şekilde, ihlalin akabinde denetleyici otoriteyle girilen işbirliğinin derecesi ve otoritenin ihlali hangi yolla öğrendiği (örneğin, veri işleme faaliyetinden sorumlu kuruluş tarafından mı yoksa hakları ihlal edilen veri sahibi tarafından mı bildirildiği) denetleyici otoritelere kararları açısından yol gösteren diğer önemli faktörlerdir.[645]

İdari para cezası uygulama kabiliyetinin yanı sıra, denetleyici otoritelerin geniş bir yelpazede kullanabileceği diğer düzeltici yetkileri de mevcuttur. Denetleyici otoritelerin söz konusu "düzeltici" yetkileri GDPR'ın 58. maddesinde belirlenmiştir. Bu yetkiler veri sorumluları ve veri işleyenlere talep, uyarı ve tekdir verilmesinden, veri işleme faaliyetlerine yönelik geçici hatta kalıcı yasaklamalara kadar uzanmaktadır.

AB hukukunun AB kurum ya da kuruluşları tarafından ihlallerine yönelik yaptırımlar açısından, AB Kuruluşları Veri Koruma Regülasyonunun özel hafifletici düzenlemesi dolayısıyla, söz konusu yaptırımlar disiplin işlemi olarak öngörülebilecektir. Regülasyonun 49. Maddesi uyarınca "İşbu Regülasyondaki yükümlülüklere uyulmaması halinde, bilinçli ya da ihmale dayalı olup olmadığı fark etmeksiniz, Avrupa Topluluğu'nun resmi ya da sair kuruluşuna disiplin işlemi uygulanabilir […]"

7. Yurt Dışına Veri Aktarımı ve Verilerin Dolaşımı

AB	Ele Alınan Konular	Avrupa Konseyi
Kişisel veri aktarımları		
GDPR, Madde 44	Konsept	Modernize Sözleşme 108, Madde 14 (1) ve (2)
Kişisel verilerin serbest dolaşım		
GDPR, Madde 1 (3) ve Başlangıç 170	AB Üye Ülkeleri Arasında	
	Sözleşme 108'e taraf olan taraflar arasında	Modernize Sözleşme 108, Madde 14 (1)
Üçüncü ülkelere ya da uluslararası organizasyonlara kişisel veri aktarımları		
GDPR, Madde 45 C-362/14, *Maximillian Schrems v. Data Protection Commissioner* [GC], 2015	Uygunluk kararı/yeterli düzeyde korumaya sahip üçüncü ülkeler ve uluslararası organizasyonlar	Modernize Sözleşme 108, Madde 14 (2)

[645] Madde 29 Çalışma Grubu (2017), 2016/679 sayılı Regülasyonun amaçlarına uygun şekilde idari para cezalarının belirlenmesi ve uygulaması, WP 253, 3 Ekim 2017.

GDPR, Madde 46 (1) ve 46 (2)	Standart sözleşme hükümleri, bağlayıcı şirket kuralları, davranış kuralları ve sertifikasyon mekanizmaları yoluyla sağlanan, veri sahipleri için uygulanabilen haklar ve hukuki çareler dahil olmak üzere uygun korumalar	Modernize Sözleşme 108, Madde 14 (2), (3), (5) ve (6)
GDPR, Madde 46 (3)	Yetkin denetleyici otorite tarafından yetkilendirmeye tabi olan: kamu otoriteleri arasındaki idari düzenlemelerin içerdiği sözleşmesel şartlar ve hükümler	
GDPR, Madde 46 (5)	Direktif 95/46 temelinde mevcut olan yetkilendirmeler	
GDPR, Madde 47	Bağlayıcı şirket kuralları	
GDPR, Madde 49	Özel durumlar için istisnalar	Modernize Sözleşme 108, Madde 14 (4)
Örnekler: AB–ABD PNR Anlaşması AB–ABD SWIFT Anlaşması	Uluslararası anlaşmalar	Modernize Sözleşme 108, Madde 14 (3) (a)

AB hukuku altında, GDPR verilerin Avrupa Birliği içerisinde serbest akışını düzenlemektedir. Ancak AB dışındaki üçüncü ülkelere ve uluslararası kuruluşlara veri aktarımlarına yönelik özel şartlar içermektedir. Regülasyon söz konusu aktarımların önemini tanımakta, özellikle uluslararası ticaret ve iş birliği açısından dikkate almakta, ancak aynı zamanda kişisel verilere yönelik artan riski de tanımaktadır. Dolayısıyla Regülasyon üçüncü ülkelere aktarılan kişisel verilerin AB içerisinde sahip olduğu koruma düzeyinin sunulmasını amaçlamaktadır.[646] Avrupa Konseyi Hukuku taraf olmayanlara aktarımlara yönelik özel şartlar ve sınır ötesi veri aktarımları için uygulanacak kuralların önemini de tanımaktadır.

7.1. Kişisel veri aktarımlarının doğası

Avrupa Konseyi hukuku altında, sınır ötesi veri akışları kişisel verilerin yabancı bir yargı yetkisine tabi alıcılara aktarılması olarak tanımlanmaktadır.[647] İlgili tarafın yargı yetkisine tabi olmayan alıcılara sınır ötesi veri akışına ancak yeteli düzeyde korumanın sağlanması halinde

[646] GDPR, Başlangıç 101 ve 116.
[647] Modernize Edilmiş Sözleşme 108'in Açıklayıcı Raporu, para. 102.

izin verilir.[648]

AB Hukuku, "işlenmekte olan ya da üçüncü bir ülkeye ya da uluslararası kuruluşa aktarımı sonrasında işlenmesi planlanan kişisel verilerin […]" aktarımını düzenlemektedir.[649] Söz konusu veri akışlarına ancak GDPR Bölüm 5'te belirlenen kurallara uyulması halinde izin verilecektir.

Avrupa Konseyi ya da Avrupa Birliği hukuku uyarınca Sözleşmeye Taraf ya da Üye Ülkenin yargı yetkisine tabi olan alıcılara yapılacak sınır ötesi aktarımlara izin verilmektedir. İki hukuk sistemi de belirli şartların yerine getirilmesi kaydıyla kişisel verilerin Sözleşmeye Taraf ya da Üye Ülke olmayan ülkelere aktarımına izin vermektedir.

7.2. Kişisel verilerin Üye Ülkeler ya da Sözleşmenin Tarafları arasında serbest hareketi/akışı

Avrupa Konseyi hukuku altında, Modernize Edilmiş Sözleşme 108'e taraf olan ülkeler arasında serbest kişisel veri akışı olmalıdır. Ancak aktarım; "başka bir tarafa yapılacak aktarımın Sözleşmenin hükümlerini bozacağına yönelik gerçek ve ciddi bir risk olması" halinde ya da "bölgesel uluslararası bir kuruluş üyesi ülkeler tarafından paylaşılan uyumlu kurallar" uyarınca yasaklanabilecektir.[650]

AB hukuku altında, AB Üye Devletleri arasında kişisel verilerin serbest dolaşımına yönelik kişilerin kişisel verilerin işlenmesi hususunda korunmasına yönelik sebeplerle kısıtlamalar ve yasaklar getirilemez.[651] İzlanda, Lihtenştayn ve Norveç'i iç pazara getiren Avrupa Ekonomik Alanı (EEA)'na[652] dair anlaşma ile verilerin serbest dolaşım alanı genişlemiştir.

Örnek: Aralarında Slovenya ve Fransa'nın da bulunduğu birtakım Üye Devletlerde yerleşik olan uluslararası bir şirketler grubunun, Slovenya'daki iştiraki Fransa'ya kişisel veri aktarırsa, söz konusu veri akışı Slovenya ulusal hukuku tarafından kişisel verilerin korunmasıyla bağlantılı nedenlerle kısıtlanamaz ya da yasaklanamaz.

Ancak, öte yandan, aynı Slovenya'da yer alan iştirak aynı kişisel verileri Malezya'daki ana şirkete aktarmak isterse, Slovenya'daki veri aktaran GDPR Bölüm 5'teki kuralları göz önüne almak zorundadır. Bu hükümler AB yargı yetkisine tabi veri sahiplerinin kişisel verilerini korumaya alma amacı taşımaktadır.

AB hukuku altında, EEA Üye Devletlerine ceza gerektiren suçların önlenmesi, soruşturulması, tespiti ya da yargılamasıyla ya da cezaların uygulanması ile bağlantılı amaçlarla kişisel veri akışları 2016/680 sayılı Direktif'e[653] tabidir. Bu Birlik içerisindeki yetkin otoriteler arasında kişisel veri aktarımının da veri koruma nedenleriyle kısıtlanmamasını ve yasaklanmamasını temin etmektedir. Avrupa konseyi hukuku altında, bütün kişisel verilerin işlenmesi (Sözleşme 108'in taraflarına sınır ötesi akışlar dahil), taraflarca muafiyetler tanınabilecek olsa da, amaçlara ya da alana yönelik hiçbir istisna olmaksızın Sözleşme 108'in kapsamına dahildir.

---

[648] Modernize Edilmiş Sözleşme 108, Md. 14 (2).
[649] GDPR, Md. 44.
[650] Modernize Edilmiş Sözleşme 108, Md. 14 (1).
[651] GDPR, Md. 1 (3).
[652] Konsey ve Komisyon'un Avrupa Topluluğu, Üye Ülkeleri ve Avusturya, Finlandiya, İzlanda, Lihtenştayn, Norveç, İsveç ve İsviçre arasında Avrupa Ekonomik Alanı Anlaşması'nın akdedilmesi üzerine 13 Aralık 1993 tarihli kararı, OJ 1994 L 1.
[653] 27 Nisan 2016 tarihli Direktif (EU) 2016/680

EEA'nın bütün üyeleri aynı zamanda Sözleşme 108'e taraftır.

7.3. Üçüncü ülkelere/taraf olmayanlara ya da uluslararası kuruluşlara kişisel veri aktarımları

Hem Avrupa Konseyi hem de AB'nin Üçüncü ülkelere veya uluslararası organizasyonlara veri akışına izin vermesine karşın farklı koşullar koymaktadırlar. Her iki koşullar dizini de ilgili kuruluşun farklı yapı ve amaçlarını göz önüne almaktadır.

AB hukuku altında, prensipte, kişisel verilerin üçüncü ülkelere ya da uluslararası kuruluşlara aktarımına izin vermenin iki yolu vardır. Kişisel verilerin aktarımı Avrupa Komisyonu tarafından verilecek yeterlilik kararına dayalı olabilir.[654] ya da söz konusu yeterlilik kararının bulunmadığı halde veri sorumlusu ya da veri işleyen veri sahibi hakları ve hukuki çareler dahil yeterli korumayı taahhüt ettiği takdirde gerçekleşebilecektir.[655] Hem yeterlilik kararının hem de yeterli korumanın mevcut olmadığı hallerde birtakım istisnalar vardır.

Avrupa Konseyi hukuku altında, Sözleşmeye taraf olmayanlara serbest veri aktarımına ancak aşağıdakiler temelinde izin verilmektedir:

- Söz konusu devletin ya da uluslararası kuruluşun kanunlarının, uygulanabilir uluslararası sözleşmeler dahil olmak üzere yeterli korumayı garanti etmesi
- Veri aktarımı ve ileri işleme faaliyetlerinde yer alan kişilerce benimsenen ve uygulanan hukuken bağlayıcı ve uygulanabilir araçlar tarafından sağlanan standardize edilmiş, onaylanmış korumaların mevcut olması[656]

AB hukukuna benzer olarak, yeterli veri korumanın mevcut olmadığı hallerde, istisnalar mevcuttur.

7.3.1. Yeterlilik kararına dayalı olarak aktarım

AB hukuku altında, yeterli veri koruma düzeyine sahip üçüncü ülkelere kişisel verilerin serbest aktarımı GDPR'ın 45. Maddesinde düzenlenmiştir. Avrupa Adalet Divanı "yeterli koruma düzeyi" kavramının üçüncü ülkenin temel hak ve özgürlükleri AB'deki hukukun temin ettiği garantilere "temelde eşit"[657] derecede korunmasının taahhüt edilmesi anlamına geldiğini açıklamıştır. Üçüncü bir ülkenin söz konusu koruma düzeyini sağlamada izlediği yol AB'de uygulananlardan farklı olabilecektir, yeterlilik standardı AB kurallarının birebir takip edilmesini gerektirmemektedir.[658]

Avrupa Komisyonu yabancı ülkelerdeki veri koruma düzeyini ulusal hukuklarına ve uygulanabilir uluslararası yükümlülüklere bakarak değerlendirir. İlgili ülkenin özellikle kişisel verilerin korunmasına yönelik çok taraflı ya da bölgesel sistemlere katılımı da göz önüne alınmaktadır. Şayet Avrupa Komisyonu üçüncü ülkenin ya da uluslararası kuruluşun yeterli koruma düzeyini taahhüt ettiğine karar verirse, bağlayıcı etkisi olan yeterlilik kararını yayımlayabilecektir.[659]Bununla birlikte Avrupa Adalet Divanı'nın, ulusal denetleyici

[654] GDPR, Md. 45.
[655] A.g.e., Md. 46.
[656] Modernize Edilmiş Sözleşme 108, Md. 14 (3) (a) ve (b).
[657] CJEU, C-362/14, Maximillian Schrems v. Data Protection Commissioner [GC], 6 Ekim 2015, para. 96.
[658] A.g.e., para. 74. Ayrıca bkz: Avrupa Komisyonu (2017), Komisyon'dan Avrupa Parlamentosu ve Konsey'e İleti "Küresel Dünyada Kişisel Verilerin Alışverişi ve Korunması" COM (2017)7 final 10 Ocak 2017, sy. 6.
[659]Sürekli olarak güncellenen yeterlilik tespiti yapılmış ülkeler listesi için bkz: Avrupa Komisyonu, Adalet Genel Müdürlüğü.

otoritelerin yine de bir kişinin Komisyon tarafından yeterli veri koruma düzeyine sahip olarak ilan edilen bir üçüncü ülkeye aktarılan verileri hakkında bulunacağı, söz konusu üçüncü ülkenin hukuku ve uygulamalarının yeterli koruma düzeyini temin etmediğine yönelik iddialarını inceleme yetkisi mevcuttur.[660]

Avrupa Komisyonu üçüncü bir ülke içerisindeki bir bölgenin yeterliliğini de değerlendirilebilir ya da kendisini örneğin Kanada'nın özel ticaret mevzuatında olduğu gibi belirli sektörlerle sınırlayabilir.[661] AB ve üçüncü ülkeler arasındaki anlaşmalara dayalı veri aktarımlarına yönelik yeterlilik tespitleri de mevcuttur. Bu kararlar havayolunun yolcu isim kayıtlarının (PNR) havayolu AB'den belirli deniz ötesi istikametlere uçtuğunda (bkz: Başlık 7.3.4) yabancı sınır kontrol otoritelerine aktarılması gibi münhasıran tek tip veri aktarımına yöneliktir.

Yeterlilik kararları devamlı olarak izlenmeye tabidir. Avrupa Komisyonu durumunu etkileyecek gelişmelerin takibi amacıyla periyodik olarak söz konusu kararları gözden geçirir. Dolayısıyla, Avrupa Komisyonu üçüncü ülke ya da uluslararası kuruluşun artık yeterlilik kararını meşru kılan koşulları sağlamadığı kanaatine varırsa, kararı değiştirebilir, askıya alabilir ya da geri çevirebilir. Komisyon ayrıca kararının arkasındaki problemin çözümü için üçüncü ülke veya uluslararası kuruluşlarla görüşmeler de yapabilir.

Avrupa Komisyonu tarafından 95/46/EC sayılı Direktif temelinde benimsenmiş olan yeterlilik kararları, GDPR Madde 45 kapsamında alınan bir Komisyon Kararı ile değiştirilene, yeri doldurulan ya da lağvedilene kadar yürürlükte kalır.

Bugüne kadar Avrupa Komisyonu Andorra, Arjantin, Kanada (PIPEDA Kanunu kapsamındaki ticari kuruluşlar için), Faroe Adaları, Guernsey, Man Adası, İsrail, Jersey, Yeni Zelanda, İsviçre ve Uruguay'ı yeterli korumayı sağlayan ülkeler olarak tanımıştır. ABD'ye yapılan aktarımlar açısında, Avrupa Komisyonu 2000 yılında AB'den aktarılan kişisel verilerin korunmasına yönelik kendini kanıtlayan ve "Safe Harbour Prensipleri"ne uyan şirketler için bir yeterlilik kararı benimsemiştir.[662] Avrupa Adalet Divanı, 2015 yılında bu geçerlilik kararını geçersiz kılmıştır ve Temmuz 2016'da şirketlerin 1 Ağustos 2016 itibariyle katılmasına izin verilen yeni bir yeterlilik kararı benimsenmiştir.

Örnek: Schrems davasında,[663] Maximilian Schrems, bir Avusturya vatandaşı, yıllardır bir Facebook kullanıcısı idi. Bay Schrems tarafından Facebook'a sağlanan tüm veriler Facebook'un İrlanda şubesinden ABD'de bulunan, işlendikleri serverlara aktarılmıştır. Bay Schrems İrlanda veri koruma otoritesine ABDli muhbir Edward Snowden'ın ortaya çıkardığı ABD istihbarat servislerinin yaptığı izlemeler ışığında ABD hukuku ve uygulamasının ülkeye aktarılan kişisel verilerin korunması bağlamında yeterli korumayı sağlamadığı yönünde şikayette bulunmuştur. İrlanda otoritesi şikayeti, Komisyon'un 26 temmuz 2000 tarihli kararında "Safe Harbour" tertibi kapsamında ABD'nin yeterli korumayı temin ettiğini göz önünde bulundurmuş olmasına dayanarak reddetmiştir. Dava İrlanda Yüksek Mahkemesi'nin önüne gelmiş ve mahkeme konuyu bir ön karar için Avrupa Adalet Divanı'na

[660] CJEU, C-362/14, Maximilian Schrems v. Data Protection Commissioner [GC], 6 Ekim 2015, paragraf 63 ve 65–66
[661] Avrupa Komisyonu (2002), Direktif 95/46/EC uyarınca Kanada'nın yasalarının sağladığı yeterli koruma üzerine 2002/2/EC sayılı 20 Aralık 2001 tarihli Karar, OJ 2002 L 2.
[662] 26 Temmuz 2000 tarihli Safe Harbour prensiplerinin sağladığı yeterli koruma ve ilişkili ABD Ticaret Bakanlığı tarafından yayınlanan sık sorulan sorular 2000/520/EC sayılı Komisyon Kararı , OJ L 215. Karar CJEU tarafından geçersiz ilan edilmiştir, C-632/14, Maximilian Schrems v. Data Protection Commissioner [GC].
[663] CJEU, C-362/14, Maximilian Schrems v. Data Protection Commissioner [GC], 6 Ekim 2015.

iletmiştir.

Avrupa Adalet Divanı, Komisyon'un Safe Harbour çerçevesine yönelik yeterlilik kararının geçersiz olduğuna karar vermiştir. Avrupa Adalet Divanı ilk olarak, kararın Safe Harbour veri koruma prensiplerinin uygulanmasına ulusal güvenlik, kamu menfaati veya kolluk gereklilikleri ya da ABD iç mevzuatı temeli ile sınırlı olarak izin verdiğini belirtmektedir. Dolayısıyla karar kişisel verileri ABD'ye aktarılan kişilerin temel haklarına müdahaleye imkan tanımış olmaktadır.[664] Dahası, kararın ABD'de söz konusu müdahaleyi sınırlamaya yönelik ya da benzer bir müdahaleye karşı etkin hukuki koruma sağlamaya yönelik kuralların varlığına dair bir tespit içermediği ifade edilmiştir.[665] Avrupa Adalet Divanı AB'de temel hak ve hürriyetlere yönelik sağlanan garantilerin Madde 7 ve 8 ile uyumlu olmayan mevzuatın bir önlemin kapsam ve uygulamasını tanımlayan açık ve net kurallar koymasını ve kişisel verilerin korunmasına yönelik minimum önlem, istisna ve sınırlamaları belirlemesini gerektirdiğinin altını çizmiştir.[666]

Komisyon kararının ABD'nin iç hukuku ya da uluslararası taahhütleri uyarınca söz konusu koruma düzeyini temin edeceğini belirtmemiş olması nedeniyle, CJEU Veri Koruma Direktifi'ndeki ilgili aktarım hükümlerinin şartlarını taşımadığı dolayısıyla geçersiz olduğuna karar vermiştir.[667]

Dolayısıyla ABD'nin koruma düzeyi AB tarafından garanti edilen temel hak ve hürriyetlere "temelde eşit" değildi.[668]680 CJEU AB Temel Haklar Regülasyonu'nun çeşitli maddelerinin ihlal edildiğini savunmuştur. İlk olarak ABD mevzuatının "elektronik iletişimin içeriğine yönelik kamu otoritelerine genel bir erişim sağlıyor olması" nedeniyle 7. maddenin özüyle çelişmiştir. İkinci olarak, Madde 47'nin özü de söz konusu mevzuatın ilgili kişilere kişisel verilere erişim ya da yok etme veya silmeye yönelik hukuki çözümler sunmaması nedeniyle ihlal edilmiştir. Son olarak Safe Harbour anlaşmasının yukarıdaki maddeleri ihlal etmesi nedeniyle kişisel veriler artık hukuka uygun olarak işlenmemekte ve durum 8. Maddenin ihlalini teşkil etmektedir.

CJEU Safe Harbour'ı geçersiz ilan ettikten sonra, Komisyon ve ABD yeni bir çerçevede anlaştılar: AB-ABD Privacy Shield. 12 Temmuz 2016'da Komisyon ABD'nin Birlik'ten ABD'deki kuruluşlara yönelik veri aktarımları için Privacy Shield altında yeterli düzeyde korumayı taahhüt ettiğini ilan eden bir kararı benimsemiştir.[669]

Safe Harbour'a benzer olarak, AB-ABD Privacy Shield çerçevesi AB'den ABD'ye ticari amaçlarla aktarılan kişisel verileri koruma amacını taşımaktadır.[670]

---

[664] A.g.e., para. 84.
[665] A.g.e., para. 88–89.
[666] A.g.e., para. 91–92.
[667] A.g.e., para. 96–97.
[668] A.g.e., para. 73–74 ve 96.
[669] 95/46/EC sayılı Direktif uyarınca 12 Temmuz 2016 tarihli, AB – ABD Privacy Shield tarafından sağlanan korumanın yeterliliği hakkında 2016/1250 sayılı Komisyon Uygulama Kararı (AB) OJ L 207. Madde 29 Çalışma Grubu Safe Harbour'a kıyasla Privacy Shield mekanizması tarafından getirilen geliştirmelerden memnun kalmış olup, Komisyon ve ABD otoritelerinin AB-ABD Privacy Shield yeterlilik kararının taslağına dair WP238 Görüşlerinde dile getirilen endişeleri dikkate almasından dolayı memnuniyetini ifade etmiştir. Yine de, hala gündemde olan bazı endişeleri dile getirmiştir. Daha fazla detay için, bkz: Madde 29 Veri Koruma Çalışma Grubu, 13 Nisan 2016 tarihli Görüş 01/2016, 16/EN WP 238.
[670] Daha fazla bilgi için bkz: AB-ABD Privacy Shield bilgi formu.

ABD şirketleri gönüllü olarak Privacy Shield listesine ilgili çerçevedeki veri koruma standartlarını sağlamak üzere katılabilecektir. Yetkin ABD otoriteleri onaylanmış olan şirketlerin söz konusu standartlarla uyumunu takip ve tasdik eder.

Privacy Shield özellikle aşağıda sayılanları getirmektedir:

- AB'den kendilerine kişisel veri aktarılan şirketlere yönelik veri koruma yükümlülükleri;
- İlgili kişiler için koruma ve tazmin, özellikle de ABD istihbarat servislerinden bağımsız ve kişisel verilerinin ulusal güvenlik alanında ABD otoriteleri tarafından hukuka aykırı biçimde kullanıldığına inanan kişilerin şikayetleriyle ilgilenen bir ombudsmanlık mekanizmasının kurulması;
- Çerçevenin uygulamasını takip etmek için yıllık bazda ortak bir gözden geçirme;[671] ilk inceleme Eylül 2017'de yapılmıştır.[672]

ABD hükümeti Privacy Shield kararına eşlik etmek üzere taahhüt ve teminatlar kaleme almıştır. Bunlar ABD hükümetinin kanuni yaptırım ve ulusal güvenlik amaçlarıyla kişisel verilere erişimine yönelik kısıtlamalar ve korumalar sağlamaktadır.

7.3.2. Yeterli korumaya tabi aktarımlar

Hem AB hem de Avrupa Konseyi hukuku veri aktaran veri sorumlusu ve üçüncü ülkede bulunan veri alıcısı ya da uluslararası kuruluş arasındaki yeterli korumayı alıcı için yeterli düzeyde alınan önlemleri veri korumasını temin etmek adına bir araç olarak tanımaktadır.

AB hukuku altında, bir üçüncü ülkeye ya da uluslararası kuruluşlara kişisel veri aktarımına ancak veri sorumlusu ya da veri işleyen uygun korumaları ve uygulanabilir veri sahibi haklarını sağlarsa ve ancak veri sahiplerinin etkin hukuk yollarına erişimi varsa izin verilmektedir.[673] AB veri koruma hukukunda kabul edilebilir 'uygun koruma' listesi münhasıran sağlanmaktadır.

Uygun koruma aşağıda sayılanlarla oluşturulabilir:

- Kamu otoriteleri ile arada bulunan hukuken bağlayıcı ve uygulanabilir dokümanlar;
- Bağlayıcı şirket kuralları;
- Avrupa Komisyonu ya da bir denetleyici otorite tarafından benimsenmiş standart veri koruma hükümleri;
- Davranış kuralları;
- Onaylama mekanizmaları.[674]

AB'de yer alan veri sorumlusu veya veri işleyen ile üçüncü ülkedeki veri alıcısı arasındaki özelleştirilmiş hükümler de uygun korumanın sağlanması için bir başka araçtır. Ancak bu

[671] Daha fazla bilgi için Avrupa Komisyonu web sayfasında bkz: AB-ABD Privacy Shield.
[672] Avrupa Komisyonu, Komisyon'dan Avrupa Parlamentosu ve Konseyi'ne AB – ABD Privacy Shield Anlaşmasının ilk yıllık gözden geçirmesine dair rapor COM(2017) 611 final, 18 Ekim 2017.
[673] GDPR, Md. 46.
[674] GDPR, Md. 46 (1) (c), (d), (2) (a), (b), (e), (f) ve 47.

sözleşmesel hükümlerin kişisel veri aktarımları için dayanılan bir araç olmaları yetkin bir denetleyici otorite tarafından onaylanmalarına bağlıdır. Benzer şekilde, kamu otoriteleri idari düzenlemelerinde yer alan veri koruma hükümlerini, denetleyici otoritenin onaylaması halinde kullanabilirler.[675]

Avrupa Konseyi hukuku altında, yeterli koruma düzeyi sağlandığı halde Modernize Edilmiş Sözleşme 108'e taraf olmayan bir devlet ya da uluslararası kuruluşa veri akışına izin verilmektedir. Bu şu şekilde sağlanabilecektir:

- Devletin ya da uluslararası kuruluşun hukukuyla; ya da
- Hukuken bağlayıcı bir belge içerisine gömülü geçici ya da standardize edilmiş korumalarla.[676]

Sözleşmesel hükümlere tabi aktarımlar

Hem Avrupa Konseyi hem de AB hukuku veri aktaran veri sorumlusu ve üçüncü ülkede yer alan alıcı arasındaki sözleşmesel hükümleri, alıcı açısından yeterli düzeyde veri korumanın sağlanmasına yönelik olası bir araç olarak tanımaktadır.[677]

AB düzeyinde, Avrupa Komisyonu Madde 29 Çalışma Grubu'nun desteğiyle daha önceden bir Komisyon kararıyla yeterli düzeyde veri korumanın kanıtı olarak onaylanan standart veri koruma hükümleri geliştirmiştir.[678] Komisyon kararlarının Üye Devletlerde tamamen bağlayıcı olması nedeniyle, veri aktarımlarını denetleyen ulusal otoriteler bu standart sözleşmesel hükümleri prosedürlerinde kabul etmelidir.[679] Dolayısıyla, veri aktaran veri sorumlusu ve üçüncü ülkedeki alıcı bu hükümleri kabul edip imzalarlarsa bu durum denetleyici otoriteye yeterli korumaların mevcut olduğunu gösterecektir. Yine de Schrems davasında, Avrupa Adalet Divanı, Avrupa Komisyonu'nun ulusal denetleyici otoritelerin kişisel verilerin bir Komisyon yeterlilik kararına tabi üçüncü ülkeye aktarımını denetleme yetkilerini kısıtlayacak yetkinliğe sahip olmadıklarına karar vermiştir.[680] Bu doğrultuda, ulusal denetleyici otoriteler, aktarım AB ya da ulusal veri koruma hukukunu ihlal ederek, örneğin veri paylaşanın standart sözleşmesel hükümlere uymadığı haller, gerçekleştiği takdirde kişisel verilerin aktarımını engellemek ya da yasaklamak dahil sahip oldukları yetkileri kullanmaktan alıkonulamaz.[681]

AB hukuki çerçevesinde standart veri koruma hükümlerinin varlığı veri sorumlularının başkaca özel bir amaca özgü, bireysel sözleşmesel hükümlerinin düzenlenmesini denetleyici otorite söz konusu hükümleri onayladığı müddetçe engellemez.[682] Öte yandan söz konusu hükümler standart veri koruma hükümleri tarafından sağlanan aynı koruma düzeyini temin etmelidir. Geçici hükümleri onaylarken, denetleyici otoriteler AB sathında tutarlı düzenleyici yaklaşımı

[675] A.g.e., Md. 46 (3).
[676] Modernize Edilmiş Sözleşme 108, Md. 14 (3) (b).
[677] Genel Veri Koruma Direktifi, Md. 46 (3); Modernize Edilmiş Sözleşme 108, Md. 14(3)(b
[678] A.g.e., Md. 46 (2) (b) ve Md. 46 (5).
[679] A.g.e., Md. 46 (3); Veri Koruma Geçici Komitesi (CAHDATA), Kişilerin kişisel verilerinin otomatik işlenmesine karşı korunması hakkında Modernize Edilmiş Sözleşmenin Açıklayıcı Raporu, para. 105.
[680] CJEU, C-362/14, Maximilian Schrems v. Data Protection Commissioner [GC], 6 Ekim 2015, paras. 96– 98 ve 102–105.
[681] CJEU'nun Schrems davasındaki pozisyonunu göz önüne alarak Komisyon standart sözleşmesel hükümlere dair Kararını değiştirmiştir. 16 Aralık 2016 tarihli ve 2001/497/EC ve 2010/87/EU sayılı standart sözleşmesel hükümler üzerine kararları değiştiren 2016/2297 sayılı Komisyon Uygulama Kararı (EU), OJ 2016 L344.
[682] GDPR, Md. 46 (3) (a).

temin etmek adına süreklilik mekanizmasını uygulama yükümlülüğüne sahiptir.[683] Bu, yetkin denetleyici otoritenin hükümler hakkındaki taslak kararını EDPB'ye iletmesi gerektiği anlamına gelmektedir. EDPB konu hakkında bir görüş yayınlar ve denetleyici otorite vereceği karara yönelik süreçte bu görüşü mümkün olduğunca dikkate almak zorundadır. Şayet EDPB görüşüne uyulmayacaksa, EDPB içerisindeki uyuşmazlık çözümü mekanizması tetiklenecek ve Kurul bağlayıcı bir karar alacaktır.[684]

Standart sözleşmesel hükümlerin en önemli özellikleri şunlardır:

- Sözleşmeye taraf olmasalar da veri sahiplerinin sözleşmesel haklarını kullanmalarını sağlayan üçüncü taraf lehtar hükmü;
- Veri alıcısının ya da aktaranın uyuşmazlık halinde veri aktaran veri sorumlusunun ulusal denetleyici otoritesine ve/veya mahkemelerine tabi olmayı kabul etmesi.

Veri aktaranların aralarından seçebileceği veri sorumluları arası aktarımlar için iki grup standart hüküm mevcuttur.[685] Veri sorumlusundan veri işleyene aktarımlarda, sadece tek bir grup standart sözleşmesel hükümler vardır.[686] Ancak, bu standart sözleşmesel hükümler an itibariyle hukuki süreçlerin konusudur.

Örnek: CJEU Safe Harbour Kararını geçersiz ilan ettikten sonra,[687] ABD'ye kişisel veri aktarımları artık bu yeterlilik kararına dayalı olamayacaktır. ABD otoriteleri ile görüşmeler devam ederken ve yeni bir yeterlilik kararını bekletirken (nihayetinde 12 Temmuz 2016 tarihinde benimsenmiştir) aktarımlar ancak standart sözleşmesel hükümler veya bağlayıcı şirket kuralları gibi diğer hukuki temellere dayalı olarak gerçekleşebilmiştir. Facebook İrlanda (Safe Harbour kararının geçersizliğine sebep olan davanın yöneltildiği taraf) dahil birçok şirket AB-ABD veri transferlerini devam ettirmek için standart sözleşmesel hükümlere geçiş yapmıştır.

Bay Schrems İrlanda denetleyici otoritesine ABD'ye standart sözleşmesel hükümlere dayanarak yapılan veri aktarımlarını askıya almasını talep ederek bir şikayette bulunmuştur. Esas itibariyle, kişisel verilerinin Facebook'un İrlanda şubesinden Facebook Inc'e ve ABD'de bulunan serverlara aktarıldığında korunacaklarına dair garantinin mevcut olmadığını iddia etmiştir. Facebook Inc. kişisel verileri ABD kolluk otoritelerine ifşa etmekle yükümlü tutabilecek Amerikan kanunları ile bağlıdır ve Avrupalı kişilerin bu uygulamaya itiraz etmesi için adli yollar mevcut değildir.[688] Bu nedenlerle, Avrupa Adalet Divanı, Safe Harbour

[683] A.g.e., Md. 63 ve Md. 64 (1) (e).
[684] A.g.e., Md. 64 ve Md. 65.
[685] Set I, Avrupa Komisyonu (2001), 15 Haziran 2001 tarihli 2001/497/EC sayılı kişisel verilerin 95/46/EC sayılı Direktif altında üçüncü ülkelere aktarımı için standart sözleşmesel hükümler hakkında Komisyon Kararı'nın Ek'inde yer almaktadır, OJ 2001 L 181; Set II Avrupa Komisyonu (2004), 27 Aralık 2004 tarihli 2004/915/EC sayılı 2001/497/EC sayılı kişisel verilerin üçüncü ülkelere aktarımı için alternatife bir takım standart sözleşemesel hükümler getirilmesi hakkında Kararı değiştiren Komisyon Kararı'nın Ek'inde yer almaktadır, OJ 2004 L 385.
[686] Avrupa Komisyonu (2010), 5 Şubat 2010 tarihli 2010/87 sayılı kişisel verilerin üçüncü ülkede kurulmuş olan işleyenlere aktarımı için standart sözleşmesel hükümler hakkında Komisyon Kararı, OJ 2010 L 39. İşbu el kitabı yazıldığı tarihte, kişisel verilerin ABD'ye aktarımında dayanak olarak standart sözleşmesel hükümlerin kullanılması, İrlanda Yüksek Mahkemesi önünde hukuki süreçlere tabi idi.
[687] CJEU, C-362/14, Maximillian Schrems v. Data Protection Commissioner [GC], 6 Ekim 2015.
[688] Daha fazla bilgi için, İrlanda Veri Koruma Komisyoneri'nin 1 Aralık 2015 tarihli Facebook İrlanda ve

kararının geçersiz olduğu kararını vermiştir ve mahkemenin kararı söz konusu kararın incelemesiyle sınırlı olsa da, başvuru sahibi aktarımın sözleşmesel hükümlere dayalı olduğu hallerde ileri sürülen konuların da aynı şekilde alakalı olduğu iddiasındadır. Bu satırların yazıldığı esnada, dava İrlanda Yüksek Mahkemesi önünde görülmekteydi. Başvuru sahibi, anlaşıldığı üzere, davayı Avrupa Komisyonu'nun standart sözleşmesel hükümler üzerine verdiği kararın geçerliliğini tartışmaya açmak amacıyla Avrupa Adalet Divanı'na taşımak istemektedir. Bölüm 5'te, belirtildiği üzere sadece Avrupa Adalet Divanı'nın bir AB enstrümanını geçersiz ilan etmeye yetkinliği vardır.

Bağlayıcı şirket kurallarına tabi aktarımlar

AB hukuku da aynı teşebbüs ya da ortak ekonomik faaliyetlerde bulunan kuruluş bünyesindeki şirketler grupları arasında gerçekleşen uluslararası aktarımlar için bağlayıcı şirket kurallarına dayalı kişisel veri aktarımlarına izin vermektedir.[689] Bağlayıcı şirket kurallarına kişisel verilerin aktarımı için bir araç olarak dayanılmasından önce, yetkin denetleyici otoritenin, bağlayıcı şirket kuralları doğrultusunda, süreklilik mekanizmasını kullanarak onları onaylaması gerekmektedir.

Onaylanmaları için, bağlayıcı şirket kurallarının hukuken bağlayıcı olmaları, temel veri koruma prensiplerini kapsamaları ve ilgili grubun tüm üyelerine uygulanabilir olmaları gerekmektedir. Veri sahiplerine yönelik uygulanabilir hakları açıkça sunmalı, tüm temel veri koruma prensiplerini içermeli ve teşebbüsün yapısını belirtmek, aktarımı açıklamak ve veri koruma prensiplerinin nasıl uygulanacağını belirtmek gibi belirli şekli yükümlülüklere uymalıdırlar. Bu söz konusu bilgilerin veri sahiplerine sunulmasını da içermektedir.

Bağlayıcı şirket kuralları, diğer şeylerin yanı sıra, veri sahiplerinin haklarını ve kuralların ihlaline dair hükümleri de belirtmelidir.[690] Bağlayıcı şirket kuralları onaylanırken, denetleyici otoriteler arasındaki işbirliği için süreklilik mekanizması (Bölüm 5'te belirtilen) tetiklenecektir.

Süreklilik mekanizmasının çerçevesinde, ilgili denetleyici otorite teklif edilen bağlayıcı şirket kurallarını gözden geçirir, bir taslak karar oluşturur ve EDPB'ye iletir. Kurul, konu hakkında bir görüş yayımlar ve ilgili denetleyici otorite bağlayıcı şirket kurallarını, Kurul'un görüşünü "mümkün olduğunca dikkate alarak" resmi olarak onaylayabilir. Bu görüş hukuken bağlayıcı değildir; ancak denetleyici otoritenin görüşü göz ardı ettiği takdirde uyuşmazlık çözümü mekanizması tetiklenecek ve Kurul'un üyelerinin 2/3 çoğunluğu ile hukuken bağlayıcı bir karar almaları gerekecektir.[691]

Avrupa Konseyi hukuku altında, hukuken bağlayıcı belgelerin içerisinde gömülü geçici ya da standardize korumalar bağlayıcı şirket kurallarını[692] da içermektedir.

7.3.3. Özel durumlar için istisnalar

AB hukuku altında, üçüncü bir ülkeye kişi veri aktarımları, yeterlilik kararı ya da standart sözleşmesel hükümler veya bağlayıcı şirketleri kuralları gibi korumaların yokluğunda dahi aşağıda yer alan durumlardan birinin söz konusu olması halinde meşru kılınabilir:

Maximillian Schrems' karşı revize edilmiş şikayete bakınız.
[689] GDPR, Md. 47.
[690] Daha detaylı açıklama için, bkz: GDPR, Md. 47.
[691] A.g.e., Md. 57 (1) (s), 58 (1) (j), 64 (1) (f), 65 (1) ve (2).
[692] Modernize Edilmiş Sözleşme 108, Md. 14 (3) (b).

- Veri sahibinin veri aktarımı için açık rızasını vermesi;
- Veri sahibinin yurtdışına veri aktarımının gerekli olduğu bir sözleşmesel ilişkiye girmesi ya da girmeye hazırlanması;
- Veri sorumlusu ve üçüncü taraf arasında veri sahibinin menfaatine bir sözleşme akdedilmesi;
- Önemli kamu menfaati;
- Hukuki hakların oluşturulması, kullanılması ya da savunulması;
- Veri sahibinin hayati çıkarlarının korunması;
- Verilerin kamuya açık sicilden aktarılması (bu kamuoyunun kamuya açık sicillerde yer alan bilgilere erişme hakkının örneğidir).[693]

Bu koşullarının hiçbirinin geçerli olmadığı hallerde ve aktarımların bir yeterlilik kararı ya da yeterli korumaya dayandırılamayacağı hallerde bir aktarım ancak tekrarlı olmaması, kısıtlı sayıda veri sahibini ilgilendirmesi ve veri sorumlusunun meşru menfaatinin sağlanması için gerekli olması halinde – veri sahibi haklarının baskın olmadığı hallerde – gerçekleşebilecektir.[694] Bu hallerde veri sorumlusu aktarımın şartlarını değerlendirmeli ve koruma sağlamalıdır. Ayrıca denetleyici otoriteyi ve etkilenen veri sahiplerini hem aktarım hakkında hem de haklı kılan meşru menfaat üzerine bilgilendirmelidir.

İstisnaların hukuka uygun aktarımlar için son merci olması[695] (sadece yeterlilik kararının ve başka korumaların mevcut olmadığı durumlarda kullanılmak üzere) müstesna doğasının altını çizmektedir ve GDPR'ın gerekçelerinde de detaylıca vurgulanmaktadır. Bu bağlamda istisnalar rıza temelinde ve "aktarımın bir sözleşme ya da hukuki taleple ilgili arada sırada ve gerekli" olduğu hallerde[696] "belirli koşullar altındaki aktarımlar" için bir imkan olarak kabul edilmektedir.

İlaveten, Madde 29 Çalışma Grubu tarafından yayımlanan rehberlere göre, özel durumlarda istisnalara dayanılması istisnai olmalıdır, bireysel olaylara dayanmalıdır ve geniş kapsamlı ya da tekrarlayan aktarımlar için kullanılamaz.[697] Avrupa Veri Koruma Denetçisi de 45/2001 sayılı Regülasyon altındaki aktarımlar için hukuki dayanak olarak kullanılan istisnaların olağandışı karakterinin altını çizmiş, bu çözümün sadece "kısıtlı durumlarda" ve "ara sıra" kullanılması gerektiğini belirtmiştir.[698]

Yeterlilik kararı mevcut olmadıkça, veri aktarımı için diğer koşulların sağlanmasına karşın, kamu menfaati için AB veya Üye Ülkeleri özel nitelikli kişisel verilerin üçüncü ülkelere aktarımlarına yönelik kısıtlamalar belirlemeye yetkilidir. Bu sınırlamalar istisnai olarak

[693] GDPR, Md. 49.
[694] A.g.e.
[695] A.g.e., Md. 49 (1).
[696] A.g.e.
[697] Madde 29 Çalışma Grubu (2005), 24 Ekim 1995 tarihli, 95/46/EC sayılı Direktif Madde 26 (1)'in yorumlanması üzerine çalışma dokümanı, WP 114, Brüksel, 25 Kasım 2005.
[698] Avrupa Veri Koruma Denetçisi, AB kurum ve kuruluşları tarafından kişisel verilerin üçüncü ülkelere ve uluslararası kuruluşlara aktarımI, Durum Kağıdı, Brüksel, 14 Temmuz 2014, sy. 15.

algılanmalıdır ve Üye Devletler ilgili hükümleri Komisyon'a bildirmelidir.[699]

Avrupa Konseyi hukuku yeterli veri korumaya sahip olmayan bölgelere veri akışına aşağıdaki hallerde izin vermektedir:

- Veri sahibinin rıza vermesi;
- Veri sahibinin menfaatinin gerektirmesi;
- Kanun tarafından sağlanan baskın meşru menfaatin, özellikle de önemli kamu menfaatinin, söz konusu olması;
- Demokratik bir toplumda gerekli ve ölçülü bir önlem olması[700]

7.3.4. Uluslararası anlaşmalara dayalı aktarımlar

AB üçüncü ülkelerle belirli amaçlarla kişisel veri aktarımını düzenleyen uluslararası anlaşmalar akdedebilir.

Bu anlaşmalar ilgili kişilerin kişisel verilerinin korunmasının temini için uygun korumaları içermelidir.[701]

Üye Devletler de üçüncü ülkelerle ya da uluslararası kuruluşlarla ilgili kişilerin temel hak ve özgürlüklerine uygun düzeyde koruma sağlayan uluslararası anlaşmalar – bu anlaşmalar GDPR uygulamalarını etkilemediği müddetçe - akdedebilir.

Modernize Edilmiş Sözleşme 108 Madde 12 (3) (a)'da da benzer bir kural yer almıştır.

Yolcu İsim Kayıtları (PNR) anlaşmaları kişisel verilerin aktarımına dair uluslararası anlaşmalara örnektir.

Yolcu İsim Kayıtları

PNR verileri hava taşıyıcıları tarafından uçuş rezervasyon sürecinde toplanır ve diğer bilgilerle birlikte hava yolcularının isimlerini, adreslerini, kredi kartı bilgilerini ve koltuk numaralarını içerir. Hava taşıyıcıları bu bilgileri kendi ticari amaçları için de toplamaktadır. AB belirli üçüncü ülkelerle (Avustralya, Kanada ve ABD) PNR verilerinin aktarımı hususunda terör saldırılarının veya ciddi uluslararası suçların önlenmesi, tespiti, soruşturulması ya da yargılanmasının sağlanması için anlaşmalar yapmıştır. İlaveten, Birlik 2016 yılında 2016/861 sayılı Direktifi – AB-PNR Direktifi[702] olarak bilinen – benimsemiştir. İşbu Direktif AB Üye Ülkelerine diğer üçüncü ülkelerdeki yetkili otoritelere terör saldırılarının veya ciddi uluslararası suçların önlenmesi, tespiti, soruşturulması ya da yargılanmasının sağlanması için PNR verilerini aktarmaları için yasal çerçeveyi düzenlemektedir. Üçüncü ülke otoritelerine PNR aktarımları somut duruma göre ve aktarımın Direktif'te belirtilen amaçlar için gerekli olup olmadığı ve temel hakların korunduğuna yönelik münferit değerlendirmeye tabidir.

AB ve üçüncü ülkeler arasındaki PNR anlaşmaları açısından, AB Temel Haklar Tüzüğünde yüceltilmiş olan gizlilik ve veri koruma temel hakları ile uyumlulukları tartışılmıştır. 2014

[699] Özellikle bkz: Madde 29 Çalışma Grubu (2005), Direktif 95/46/EC'nin Madde 26 (1) hükmünün ortak yorumlanması hakkında çalışma dokümanı, WP 114, Brüksel, 25 Kasım 2005.
[700] Modernize Edilmiş Sözleşme 108, Md. 14 (4).
[701] GDPR, Başlangıç 102.
[702] 27 Nisan 2016 tarihli yolcu isim kaydı (PNR) verilerinin terörist saldırılar ve ciddi suçların önlenmesi, tespiti, soruşturulması ve yargılaması hakkında Direktif (EU) 2016/681 OJ 2016 L 119.

yılında AB – Kanada ile müzakerelerin akabinde – PNR verilerinin aktarımı ve işlenmesi hakkında anlaşmayı imzaladığında, Avrupa Parlamentosu konuyu anlaşmanın AB hukuku ve özellikle Tüzüğün 7. ve 8. Maddeleri açısından hukukiliğinin değerlendirilmesi için Avrupa Adalet Divanı'na iletmeye karar verdi.

Örnek: AB-Kanada PNR anlaşmasının[703] hukukiliğine dair Görüşünde Avrupa Adalet Divanı, mevcut haliyle, öngörülen anlaşmanın Tüzük tarafından tanınan temel haklar ile uyumsuz olduğuna ve dolayısıyla akdedilemeyeceğine karar vermiştir. Kişisel verilerin işlenmesine dair olması nedeniyle, Tüzüğün 8. maddesinde korunan kişisel verilerin korunması hakkına bir müdahale teşkil etmekteydi. Aynı zamanda, bir bütün olarak ele alındığında PNR verilerinin birleştirilerek seyahat alışkanlıklarını, kişiler arasındaki ilişkileri, finansal durumlarına dair bilgileri, beslenme alışkanlıkları ve sağlık durumlarını ortaya çıkaracak şekilde analiz edilerek kişilerin özel hayatına tecavüz teşkil edebilmesi nedeniyle 7. maddede yüceltilmiş olan özel hayatın gizliliğine saygı hakkına da bir kısıtlama getirmektedir.

Öngörülen anlaşmanın getirdiği temel haklara müdahale kamu güvenliği ve terörizm ile ciddi uluslararası suçlara karşı mücadele yoluyla kamu yararı amacı gütmekteydi. Ancak Avrupa Adalet Divanı, kamu yararının makul olması için bir müdahalenin sadece ulaşılmak istenen amacın elde edilmesi için kesin surette gerekli olanlarla sınırlı olması gerektiğini hatırlatmıştır. Hükümlerini incelemesinin akabinde, Avrupa Adalet Divanı öngörülen anlaşmanın "kesin surette gerekli olma" kriterlerine uymadığına karar vermiştir. Avrupa Adalet Divanı'nın bu sonuca varırken göz önüne aldığı unsurlardan bazıları şu şekildedir:

- Öngörülen anlaşmanın hassas verilerin aktarılmasına neden olması. Öngörülen anlaşmaya göre toplanan PNR, ırk ya da etnik köken, dini inançlar ya da yolcunun sağlık durumu gibi hassas verileri içerebilecektir. Hassas verilerin Kanada otoriteleri tarafından aktarılması ve işlenmesi ayrımcılığa karşı prensiplere yönelik risk teşkil edebilecektir ve bu nedenle kamu güvenliği ve ciddi suçlarla mücadele haricinde kesin ve sağlam bir gerekçeye ihtiyaç duymaktadır. Öngörülen anlaşma bu şekilde bir gerekçeyi sunmayı başaramamıştır.[704]

- Yolcular Kanada'dan ayrılmış olsa dahi bütün yolcuların PNR verilerinin aralıksız olarak beş yıllık bir periyot boyunca tutulması da kesin surette gerekliliğin limitlerinin aşılması olarak değerlendirilmiştir. CJEU, Kanada otoritelerinin nesnel delillerin kamu güvenliğine tehdit oluşturabileceğini gösterdiği kişilerin verilerini Kanada'dan ayrılsalar dahi tutabilecekleri değerlendirmesini yapmıştır. Öte yandan, kendilerine dair kamu güvenliğine risk teşkil ettiklerine dair dolaylı delillerin bile olmadığı bütün yolcuların kişisel verilerinin saklanması meşru değildir.[705]

Sözleşme 108'in Danışma Komitesi PNR anlaşmasının Avrupa Konseyi hukuku altındaki veri koruma etkileri hakkında bir görüş sunmuştur.[706]

Mesajlaşma verisi

Avrupa bankalarından yapılan küresel para transferlerinin çoğu için veri işleyen olan Belçika merkezli Dünya Bankalararası Finansal İletişim Birliği (SWIFT) ABD'de bir "ayna" merkez

[703] CJEU, Mahkeme'nin (Yüce Divan) 1/15 sayılı Görüşü, 26 Temmuz 2017.
[704] A.g.e., para. 165
[705] A.g.e., paras. 204–207.
[706] Avrupa Konseyi, Yolcu İsim Kayıtlarının işlenmesinin veri korumaya etkileri hakkında Görüş, T-PD(2016)18rev, 19 Ağustos 2016.

ile faaliyet göstermekte olup Terörist Finansman Takip Programı[707] kapsamında terörizm soruşturmaları amacıyla ABD Hazine Bakanlığı'na belirli verileri ifşa etmesine yönelik bir taleple karşılaşmıştır.

AB perspektifine göre, - genellikle AB'deki vatandaşlar hakkında olan - bu verilerin sadece SWIFT'in veri hizmet işleme merkezlerinden birinin orada bulunmasına dayanılarak ABD'ye ifşası için yeterli hukuki dayanak bulunmamaktaydı.

2010 yılında AB ve ABD arasında, gerekli hukuki dayanağı sağlamak ve yeterli veri koruma standartlarını temin etmek amacıyla, SWIFT Anlaşması olarak bilinen özel bir anlaşma akdedilmiştir.[708]

Bu anlaşma kapsamında, SWIFT tarafından muhafaza edilen finansal verilerin terörizm ya da terörizm finansmanının engellenmesi, soruşturulması, tespiti ya da yargılaması amaçlarıyla ABD Hazine Bakanlığı'na sağlanmasına devam edilecektir. ABD Hazine Bakanlığı ilgili talep aşağıda yer alan unsurları taşıdığı takdirde SWIFT'ten finansal verileri talep edebilecektir:

- Finansal verileri olabildiğince açık şekilde ifade etmesi;
- Verinin gerekliliğini açıkça desteklemesi;
- Talep edilen verilerin mümkün olduğunca minimize edilmesi için tasarlanmış olması;
- Single Euro Payments Area (SEPA)'ya dahil verileri içermemesi.[709]

Europol, ABD Hazine Bakanlığı tarafından gerçekleştirilen her talebin bir kopyasını temin etmeli ve SWIFT anlaşmasının prensiplerine uyulup uyulmadığını onaylar.[710] Eğer uyuluyorsa, SWIFT bu finansal verileri doğrudan ABD Hazine Bakanlığı'na sağlamalıdır. Bakanlık, finansal verileri sadece terörizm ya da finansmanını soruşturan analistlerin erişebileceği güvenli fiziksel ortamlarda muhafaza etmelidir ve finansal veriler başka bir veri tabanı ile bağlantılı olmamalıdır. Genel olarak SWIFT'ten gelen veriler teslim alınmasından itibaren beş yıl içerisinde silinmelidir. Belirli soruşturma ya da yargılamalarla ilgili finansal veriler ancak ilgili soruşturma veya yargılamaların gerektirdiği sürece saklanmalıdır.

ABD Hazine Bakanlığı SWIFT'ten aktarılan bilgileri ABD'de ya da ABD dışında yer alan belirli kolluk, kamu güvenliği veya terörizme karşı otoritelere münhasıran terörizm ve finansmanının soruşturulması, tespiti, önlenmesi ya da yargılanması amaçlarıyla aktarabilecektir. Finansal verilerin ileriki aktarımı bir AB Üye Devletinin vatandaşı ya da ikamet eden kişiyi kapsıyorsa, verilerin üçüncü bir ülkenin otoriteleri ile paylaşımı ilgili Üye Devletin yetkili otoritelerinin önceden rıza göstermesine bağlıdır. Veri paylaşımının kamu

---

[707] Bu bağlamda, bkz: Madde 29 Çalışma Grubu (2011), kara para aklama ve terrorist finansmanının önlenmesine dair veri koruma hususları hakkında Görüş 14/2011, WP 186, Brüksel, 13 Haziran 2011; Madde 29 Çalışma Grubu (2006), OSWIFT tarafıdan kişisel verilerin işlenmesi hakkında Görüş 10/2006, WP 128, Brüksel, 22 Kasım 2006; Belçika Gizliliğin Korunması Komisyonu (Commission de la protection de la vie privée) (2008),
'SWIFT scrl uyarınca başlatılan control ve tavsiye prosedürü', Karar, 9 Aralık 2008.

[708] 13 Temmuz 2010 tarihli, 2010/412/EU sayılı Avrupa Birliği ile Amerika Birleşik Devletleri arasında finansal mesajlaşma verilerinin ABD'nin Terörist Finansmanı Takip Programı amaçlarıyla AB'den ABD'ye aktarımına dair anlaşmanın akdedilmesi hakkında Konsey Kararı, OJ 2010 L 195, pp. 3 ve 4. Anlaşmanın metni bu karara eklenmiştir, OJ 2010 L 195, pp. 5–14.

[709] A.g.e., Md. 4 (2).

[710] Europol'un Birleşik Denetim Organı, Europol'un faaliyet alanlarında denetimler gerçekleştirmiştir.

güvenliğine yönelik ani ve ciddi bir tehdidin önlenmesi için gerekli olması halinde istisnalar sağlanabilecektir.

Avrupa Komisyonu tarafından atanan bir kişi dahil, bağımsız denetçiler SWIFT Anlaşmasının prensipleriyle uyumu gözlemler. Eş zamanlı olarak ve geçmiş dönük olarak gözden geçirme, terörizm ile bağlantısını haklı kılan ilave bilgi talep etme ve anlaşma kapsamında düzenlenen korumaları ihlal ettiği anlaşılan herhangi bir aramayı engelleme olanakları vardır.

Veri sahiplerinin yetkin AB denetleyici otoritesinden kişiler veri koruma haklarına uyulduğuna dair onay temin etme hakları vardır. Veri sahiplerinin ayrıca, SWIFT Anlaşması altında ABD Hazine Bakanlığı tarafından toplanan ve saklanan kişisel verilerine yönelik yok etme, silme ve engelleme hakları da mevcuttur. Ancak, veri sahiplerinin erişim hakları belirli hukuki kısıtlamalara tabi olabilir. Erişimin kabul edilmediği hallerde, veri sahipleri redde ve ABD'de idari ve adli tazmin mekanizmalarına dair yazılı olarak bilgilendirilmelidir.

SWIFT Anlaşması beş yıl için geçerlidir, ilk geçerlilik periyodu Ağustos 2015'e kadar sürmüştür. Taraflardan biri diğerine en az altı ay önceden anlaşmayı uzatmama yönündeki niyetini bildirmediği sürece otomatik olarak bir yıllık periyotlarla uzar. Otomatik uzatma Ağustos 2015, 2016 ve 2017'de uygulanmış olup SWIFT Anlaşmasının geçerliliğini en az Ağustos 2018'e kadar temin etmiştir.[711]

8. Kolluk Faaliyetleri ve Ceza Yargılaması Bağlamında Kişisel Verilerin Korunması

AB	Ele Alınan Konular	Avrupa Konseyi
Polis ve Ceza Yargılaması Otoriteleri için Veri Koruma Direktifi	Genel	Modernize Edilmiş Sözleşme 108
	Polis	Polis Tavsiyesi Polis sektöründe kişisel verilerin kullanımı üzerine Uygulama Rehberi
	Gözetim	AİHM, *B.B. v. Fransa*, No. 5335/06, 2009
		AİHM, *S. ve Marper v. Birleşik Krallık* [GC], Nos. 30562/04 ve 30566/04, 2008
		AİHM, *Allan v. Birleşik Krallık* No. 48539/99, 2002
		AİHM, *Malone v. Birleşik Krallık* No. 8691/79, 1984
		AİHM, *Klass ve Diğerleri v. Almanya*, No. 5029/71, 1978
		AİHM, *Szabó ve Vissy v.*

[711] A.g.e.; Md. 23 (2).

		Macaristan, No. 37138/14, 2016 AİHM, *Vetter v. Fransa*, No. 59842/00, 2005
	Siber Suçlar	Siber Suçlar Anlaşması
Diğer spesifik hukuki araçlar		
Prüm Kararı	Özel veriler için: parmak izi, DNA, holiganizm, hava yolcu bilgileri, iletişim verileri vb.	Modernize Edilmiş Sözleşme 108, Madde 6 Polis Tavsiyesi, Polis sektöründe kişisel verilerin kullanımı üzerine Uygulama Rehberi
İsveç Girişimi (Konsey Çerçeve Kararı 2006/960/JHA)	Kolluk otoriteleri arasında bilgi ve istihbarat alışverişinin basitleştirilmesi	AİHM, *S. ve Marper v. Birleşik Krallık* [GC], No. 30562/04 ve 30566/04, 2008
Yolcu İsim Kaydı (PNR) verilerinin terörist saldırılar ve ciddi suçların önlenmesi, tespiti, soruşturulması ve yargılaması için kullanılması hakkında 2016/681 sayılı Direktif (AB) CJEU, birleşik davalar C-293/12 ve C-594/12, *Digital Rights Ireland ve Kärntner Landesregierung ve Diğerleri* [GC], 2014 CJEU, birleşik davalar C-203/15 ve C-698/15, *Tele2 Sverige ve Home Department v. Tom Watson ve Diğerleri* [GC], 2016	Kişisel verilerin muhafazası	AİHM, *B.B. v. Fransa*, No. 5335/06, 2009
Europol Düzenlemesi Eurojust Kararı	Özel kurumlardan	Polis Tavsiyesi
Schengen II Kararı VIS Regulation Eurodac Regulation CIS Kararı	Özel müşterek bilgi sistemlerinden	Polis Tavsiyesi AİHM, *Dalea v. France*, No. 964/07, 2010

İlgili kişinin veri korumasındaki menfaatleri ile toplumun suçla mücadele ve ulusal ve kamu güvenliğinin sağlanması amacıyla verilerin toplanmasındaki menfaati arasında bir denge kurmak için, Avrupa Konseyi ve AB özel hukuki araçları yasallaştırmıştır. Bu bölüm polis ve suç yargılaması konularında Avrupa Konseyi (Section 8.1) ve AB hukuklarına (Section 8.2) bir genel bakış sunmaktadır.

8.1. Avrupa Konseyi hukukunda veri koruma ve ulusal güvenlik, polis, suç yargılaması konuları

Avrupa Konseyi ve AB hukukları arasındaki önemli bir fark Avrupa Konseyi hukukunun AB hukuku aksine ulusal güvenlik alanına da uygulanmasıdır. Bu, Sözleşmenin Taraflarının ulusal güvenlikle ilgili faaliyetler dahil AİHS Madde 8 kapsamında kalmaları gerektiği anlamına gelmektedir AİHM'nin birçok kararı hassas alanlar olan ulusal güvenlik hukuku ve pratiği üzerinedir.[712]

Polis ve suç yargılaması hakkında, Avrupa düzeyinde, Modernize Edilmiş Sözleşme 109 kişisel verilerin işlenmesine dair bütün alanları kapsamaktadır ve hükümleri genel anlamda kişisel verilerin işlenmesini düzenleme amacındadır. Sonuç olarak, Modernize Edilmiş Sözleşme 108 polis ve suç yargılaması alanlarında veri korumaya da uygulanır. Genetik verilerin, suçlara dair verilerin, ceza yargılamalarının ve mahkumiyetler ve alakalı güvenlik tedbirlerinin, bir kişiyi eşsiz olarak belirleyen biyometrik verilerin ve bütün hassas verilerin işlenmesine ancak söz konusu verilerin işlenmesinin veri sahiplerinin menfaatleri, hakları ve temel özgürlüklerine yönelik doğurabileceği, ayrımcılık gibi, risklere karşı yeterli korumanın mevcut olduğu hallerde izin verilmektedir.[713]

Polis ve suç yargılaması otoritelerinin kanuni görevleri çok zaman kişisel verilerin işlenmesini gerektirir, bu durum da ilgili kişi için ciddi sonuçlar doğurabilir. Avrupa Konseyi tarafından 1987'de kabul edilen Polis Tavsiyesi Avrupa Konseyi üye ülkelerine Sözleşme 108'in maddelerini polis otoriteleri tarafından veri işleme faaliyetleri kapsamında nasıl uygulamaları gerektiği hususunda rehberlik etmektedir.[714]

Tavsiye, Sözleşme 108 Danışma Komitesi tarafından benimsenen polis sektöründe kişisel verilerin kullanımı üzerine uygulama rehberi ile tamamlanmıştır.[715]

Örnek: D.L. v. Bulgaristan davasında,[716] sosyal servisler başvuru sahibini mahkemenin emri üzerine güvenli bir eğitim kurumuna yerleştirmiştir. Bütün yazışma ve telefon görüşmeleri kurum tarafından toplu ve ayırt etmeksizin izlemeye tabi tutulmuştur. AİHM, somut olayda uygulanan önlemin demokratik bir toplumda gerekli olmaması nedeniyle, Madde 8'in ihlal edildiğine karar vermiştir. Mahkeme, bir kuruma yerleştirilen reşit olmayan kişilerin dış dünya ile yeterli irtibatı olması için her şeyin yapılması gerektiğini, bunun insanlık onuru için önemli olduğunu ve topluma geri kazandırılmada kesinlikle esas olduğunu belirtmiştir. Bu, ziyaretler için geçerli olduğu kadar yazışma ve telefon görüşmeleri için de geçerlidir. Dahası, gözetim aile ile ya da çocuk haklarını temsil eden sivil toplum kuruluşları ya da avukatlar açısından da bir ayrıma gitmemiştir. Ayrıca iletişimin takibi kararı her bir somut durum için ayrı bir analize dayalı olarak verilmemiştir.

Örnek: Dragojević v. Hırvatistan davasında,[717] başvuru sahibinin uyuşturucu ticaretine dahil olduğundan şüphelenilmekteydi. Sorgu hakiminin, başvuranın telefon konuşmalarının takibi için gizli takip önlemlerinin kullanılmasına izin vermesinden sonra suçlu bulundu. AİHM,

[712] Bkz: AİHM, Klass ve Diğerleri v. Almanya, No. 5029/71, 6 Eylül 1978; AİHM, Rotaru v. Romanya [GC], No. 28341/95, 4 May 2000 tarihli AİHM, Szabó ve Vissy v. Macaristan, No. 37138/14,
[713] 12 Ocak 2016. Modernize Edilmiş Sözleşme 108, Md. 6.
[714] Avrupa Konseyi, Bakanlar Komitesi (1987), Üye devletlerin polis sektöründe kişisel verilerin kullanımı düzenlemesine dair Tavsiye(87), 17 Eylül 1987.
[715] Avrupa Konseyi (2018), Sözleşme 108 Danışma Konseyi, kişisel verilerin polis sektöründe kullanımına dair Uygulama Rehberi , T-PD(2018)1.
[716] AİHM, D.L. v. Bulgaristan, No. 7472/14, 19 Mayıs 2016.
[717] AİHM, Dragojević v. Hırvatistan, No. 68955/11, 15 Ocak 2015.

hakkında şikayetin yöneltildiği söz konusu tedbirin özel hayatın ve iletişimin gizliliği hakkına bir müdahale teşkil ettiğine karar vermiştir. Sorgu hakimi tarafından verilen yetki yalnızca savcılığın "soruşturmanın başka araçlarla mümkün olamayacağına" yönelik ifadesine dayanmaktaydı. AİHM ayrıca ceza mahkemelerinin takip tedbirlerinin uygulanması açısından değerlendirmelerini kısıtladığını ve hükümetin de mevcut hukuki çözümleri ortaya sürmediğini eklemiştir. Dolayısıyla, Madde 8 ihlal edilmiştir.

8.1.1. Polis tavsiyesi

AİHM istikrarlı olarak kişisel verilerin polis veya ulusal güvenlik otoriteleri tarafından saklanması ve muhafazasının AİHS Madde 8 (1)'e müdahale teşkil ettiğine karar vermektedir. Pek çok AİHM kararı söz konusu müdahalenin gerekçelendirmesi ile ilgilidir.[718]

Örnek: B.B. v. Fransa davasında,[719] başvuran 15 yaşında reşit olmayan kişilerle güven ilişkisi içerisinde seks suçu işlemekten hüküm giymiştir. Hapis cezasını 2000 yılında tamamlamıştır. Bir yıl sonra, bu cezasının sabıka kaydından çıkarılmasını talep etmiştir; ancak bu talebi reddedilmiştir. 2004 yılında, bir Fransız kanunu ulusal adli bir seks suçluları veritabanı oluşturmuş ve başvuru sahibi oraya dahil edildiğine dair bilgilendirilmiştir. AİHM, hüküm giymiş bir seks suçlusunun ulusal adli bir veritabanına dahil edilmesinin AİHS'nin 8. Maddesi kapsamında olduğuna karar vermiştir. Ancak, veri sahibinin verilerin silinmesini talep etme hakkı, verilerin saklanmasının sınırlılığı ve bu gibi verilere kısıtlı erişim gibi yeterli veri koruma önlemlerinin alınması halinde olayda yarışan özel ve kamusal menfaatler arasında adil bir denge kurulmuştur. Mahkeme AİHS Madde 8'in ihlal edilmediğine kadar vermiştir.

Örnek: S. ve Marper v. Birleşik Krallık davasında,[720] başvuranların ikisi de ceza gerektiren suçlarla suçlanmakta ancak hüküm giymemişlerdir. Yine de, parmak izleri, hücresel örnekleri ve DNA profilleri polis tarafından tutularak saklanmıştır. kişi sonradan aklansa ya da tahliye edilse dahi, şüpheli kişinin yukarıda belirtilen biyometrik verilerinin sınırsız olarak muhafaza edilmesine mevzuat tarafından izin verilmektedir. AİHM, kişisel verilerin battaniye ve ayrım yapılmaksızın muhafazasının, zaman limiti olmadan ve aklanmış kişilerin silinme talebi için sadece kısıtlı imkanları olması nedeniyle, başvuranların özel hayatın gizliliği haklarına ölçüsüz bir müdahale teşkil ettiği kanaatine varmıştır. Mahkeme AİHS Madde 8'in ihlal edildiğine karar vermiştir.

Elektronik iletişim kapsamında önem arz eden bir husus, kamu otoriteleri tarafından gizlilik ve veri koruma haklarına yönelik müdahalelerdir. Dinleme cihazları gibi, iletişimin izlenmesi ya da takibine yönelik araçların kullanımına ancak kanunun izin vermesi ve demokratik bir toplum için gerekli bir tedbir olması, aşağıda sayılanların menfaati için gerekli olması durumunda izin verilebilir:

- Devlet güvenliğinin korunması;
- Kamu güvenliği;
- Devletin parasal çıkarları;

[718] Bkz: AİHM, Leander v. İsveç, No. 9248/81, 26 Mart 1987; AİHM, M.M. v. Birleşik Krallık, No. 24029/07, 13 Kasım 2012; AİHM, M.K. v. Fransa, No. 19522/09, 18 Nisan 2013, or AİHM, Aycaguer v. Fransa, No. 8806/12, 22 Haziran 2017.
[719] AİHM, B.B. v. Fransa, No. 5335/06, 17 Aralık 2009.
[720] AİHM, S. ve Marper v. Birleşik Krallık [GC], Nos. 30562/04 ve 30566/04, 4 Aralık 2008, para. 119 ve 125.

- Ceza gerektiren suçların engellenmesi; ya da
- Veri sahibinin ya da diğer kişilerin hak ve özgürlüklerinin korunması.

Pek çok diğer AİHM kararı gözetim yoluyla gizlilik hakkına müdahalenin gerekçeleri hakkındadır.

Örnek: Allan v. Birleşik Krallık davasında,[721] otoriteler gizlice bir mahkûm ile hapishanenin ziyaret alanındaki bir arkadaşı ve hapishane hücresinde ortak olarak suçlanan kişiyle arasındaki özel konuşmaları gizlice kaydetmiştir. AİHM, başvuranın hücresinde, hapishane ziyaret alanında ve başka bir mahkûmun üzerinde ses ve video kayıt cihazlarının kullanılmasının başvuranın özel hayatın gizliliğine müdahale teşkil ettiğine karar vermiştir. Mevzuatta ilgili zamanda polis tarafından gizli kayıt cihazlarının kullanımı düzenleyen bir sistem olmaması nedeniyle bu müdahale hukuka uygun değildir. Mahkeme, AİHS Madde 8'in ihlal edildiğine hükmetmiştir.

Örnek: Roman Zakharov v. Rusya davasında,[722] başvuru sahibi üç mobil şebeke operatörüne yönelik adli yargılamaya başvurmuştur. Başvuran, operatörlerin Federal Güvenlik Hizmeti'nin öncesinde adli yetkilendirme olmadan telefon görüşmelerini dinlemesine izin veren bir donanım kurması nedeniyle telefon iletişiminde gizlilik hakkının ihlal edildiğini iddia etmiştir. AİHM iletişimin dinlenmesini düzenleyen yerel kanuni hükümlerin keyfilik ve suistimal riskine yönelik yeterli ve etkin garantiler sağlamadığına kanaat getirmiştir.

Özellikle, ulusal hukuk saklamada hedeflenen amaç elde edildikten sonra dahi söz konusu saklanan verilerin silinmesini gerektirmemekteydi. Dahası, adli yetkilendirme gerekli olsa da adli tetkik sınırlıydı.

Örnek: Szabó ve Vissy v. Macaristan davasında,[723] başvuranlar Macaristan mevzuatının yeterince detaylı ve açık olmaması nedeniyle AİHS Madde 8'i ihlal ettiğini iddia etmişlerdir. Ayrıca, mevzuatın keyfilik ve suistimale karşı yeterli garantileri sağlamadığı savunulmuştur. AİHM, Macaristan hukukunun izlemenin mahkeme tarafından yetkilendirmeye tabi olmasını şart koşmadığını tespit etmiştir. Ayrıca, Mahkeme izleme Adalet Bakanı'nın onayına tabi tutulsa da, bu gözetimin politik olduğu ve "kesin surette gereklilik" değerlendirmesini temin etmekte yetersiz olduğunu belirtmiştir. Dahası, veri sahiplerine bildirim yapılmadığı için ulusal hukuk adli gözden geçirmeyi düzenlememektedir. Mahkeme AİHS Madde 8'in ihlal edildiğine karar vermiştir.

Polis otoriteleri tarafından veri işlenmesinin ilgili kişilere yönelik ciddi etkileri olabilmesi nedeniyle, bu alanda kişisel verilerin işlenmesine yönelikli detaylı veri koruma kuralları özellikle gerekmektedir. Avrupa Konseyi Polis Tavsiyesi, polis işleri için kişisel verilerin nasıl toplanması gerektiği, veri dosyalarının nasıl tutulması gerektiği, kişisel verilerin yabancı polis otoritelerine aktarım şartları dahil olmak üzere kimlerin bu dosyalara erişimi olması gerektiği, veri sahiplerinin veri koruma haklarını nasıl kullanabilmesi gerektiği ve bağımsız otoriteler tarafından kontrollerin nasıl uygulanması gerektiği hususlarında rehberlik ederek bu sorunu çözmeyi hedeflemiştir. Yeterli veri güvenliğinin sağlanması yükümlülüğü de göz önüne alınmıştır.

[721] AİHM, Allan v. Birleşik Krallık, No. 48539/99, 5 Kasım 2002.
[722] AİHM, Roman Zakharov v. Rusya, No. 47143/06, 4 Aralık 2015.
[723] AİHM, Szabó ve Vissy v. Macaristan, No. 37138/14, 12 Ocak 2016.

Tavsiye, kişisel verilerin polis otoriteleri tarafından ucu açık, ayrım yapmaksızın toplanmasına müsaade etmemektedir. Polis otoriteleri tarafından kişisel verilerin toplanmasını gerçek bir tehlikenin önlenmesi ya da belirli bir suçun yargılaması için gerekli olanlarla sınırlı tutmaktadır. Herhangi ilave veri toplama faaliyetinin spesifik bir ulusal mevzuata dayalı olması gerekmektedir. Belirli bir tahkikat kapsamında hassas verilerin işlenmesi kesinlikle gerekli olanlarla sınırlı tutulmalıdır.

Kişisel verilerin veri sorumlusunun bilgisi dışında toplandığı hallerde, veri sahibi kendisine yapılacak bildirimin yürütülen bir soruşturmayı etkileme ihtimalinin ortadan kalktığı an bilgilendirilmelidir. Verilerin teknik takip veya diğer otomatik araçlarla toplanması halinde spesifik bir hukuki dayanağı olması zorunludur.

Örnek: Versini-Campinchi ve Crasnianski v. Fransa davasında,[724] bir avukat olan başvuran, telefon hattı bir sorgu hakiminin talebi doğrultusunda dinlenen bir müvekkili ile telefon görüşmesi gerçekleştirmiştir. Konuşmanın transkripti, kendisinin hukuki profesyonel gizlilik kapsamında olan bazı bilgileri ifşa ettiğini göstermiştir. Savcı, bu bilgileri Baro Konseyi'ne göndermiş ve Baro başvurana ceza uygulamıştır. AİHM, sadece telefonu dinlenen kişi açısından değil, iletişimi takip edilen ve transkripte dökülen başvuran açısından da özel hayatın ve iletişimin gizliliği haklarına müdahale olduğunu belirtmiştir. Müdahale, kanunla uyum içerisinde gerçekleştirilmiş ve bozukluğun düzeltilmesine yönelik meşru bir amaç taşımaktaydı. Başvuran, kendisine karşı yürütülen disiplin süreci bağlamında telefon dinleme kayıtlarının transkriptinin sunulmasının hukukiliğine dair bir görüş elde etmiştir. Her ne kadar telefon görüşmesinin transkriptini iptal ettirmek üzere başvuruda bulunamamış olsa da, AİHM şikayet edilen müdahalenin demokratik bir toplumda gerekli olan düzeye sınırlanması için etkin tahkikatın yapıldığına kanaat getirmiştir. AİHM, transkripte dayalı olarak bir avukata yönelik adli işlem yapılması ihtimalinin avukat ile müvekkili arasındaki iletişim özgürlüğüne, dolayısıyla savunma hakkına etkisi olabileceği argümanını, avukat tarafından yapılan ifşanın hukuka aykırılık teşkil etmesi nedeniyle inandırıcı bulmamıştır. Dolayısıyla, Madde 8'in ihlal edilmediğine hükmedilmiştir.

Avrupa Komisyonu Polis Tavsiyesi, kişisel verilerin muhafazası sırasında şu hususlarda net ayrım yapılması gerektiğini düzenlemektedir: idari veri ve polis verisi; farklı veri sahiplerine ait kişisel veriler, şüpheli, hükümlü, mağdur ve tanık gibi; ve inkar edilemez gerçek olan veriler ile şüphe ya da spekülasyona dayalı veriler.

Polis verilerinin kullanılması için amaçlar sıkı şekilde sınırlanmış olmalıdır. Bu durumun polis verilerinin üçüncü kişilere ifşası için sonuçlar doğurmaktadır: polis sektörü içerisinde bu gibi verilerin aktarımı ya da ifşası bu bilgilerin paylaşılmasında meşru menfaatin mevcut olup olmadığına göre yönetilmelidir. Bu verilerin polis sektörü dışında aktarımı ya da ifşasına açık bir hukuki yükümlülük ya da yetkilendirme olduğunda izin verilmelidir.

Örnek: Karabeyoğlu v. Türkiye davasında,[725] bir hakim olan başvuranın, üye olmasından ya da yardım ve destek sağladığından şüphelenilen yasadışı bir örgüte yönelik ceza soruşturması kapsamında telefon hatları dinlenmiştir. Suçlamama kararının ardından soruşturmanın yetkili

[724] AİHM, Versini-Campinchi ve Crasnianski v. Fransa, No. 49176/11, 16 Haziran 2016.
[725] AİHM, Karabeyoğlu v. Türkiye, No. 30083/10, 7 Haziran 2016.

savcısı söz konusu kayıtları yok etmiştir. Ancak, bir kopyası adli soruşturmacıların elinde kalmış olup bu materyaller başvuru sahibine karşı bir disiplin soruşturması kapsamında kullanılmıştır. AİHM, bilgiler toplama amacından farklı amaçlarla kullanıldığı ve mevzuatta yer alan süre sınırları içerisinde yok edilmediği için ilgili mevzuatın ihlal edildiğini belirtmiştir. Kişi hakkındaki disiplin soruşturması uyarınca başvuranın özel hayatın gizliliği hakkına yönelik müdahale kanuna uygun gerçekleşmemiştir.

Ciddi ve gerçekleşmesi yakın bir tehlikenin önlenmesi için gerekli olması halleri haricinde, uluslararası aktarım ve ifşalar yabancı polis otoriteleriyle sınırlı olmalı ve özel kanuni hükümlere, muhtemelen uluslararası anlaşmalara, dayalı olmalıdır.

Yerel veri koruma hukukuyla uyumu temin etmek için polis tarafından verilerin işlenmesi bağımsız denetime tabi olmalıdır. Veri sahipleri Modernize Edilmiş Sözleşme 108 içerisinde yer alan tüm erişim haklarına sahip olmalıdır. Etkin polis soruşturmaları ve cezaların uygulanmasının menfaatine olarak, veri sahibinin erişim hakları Sözleşme 108'in 9. maddesine göre kısıtlandığı hallerde, veri sahibi yerel hukuk kapsamında ulusal veri koruma otoritesine ya da başka bir bağımsız kuruma başvurma hakkına sahip olmalıdır.

8.1.2. Siber Suçlar Hakkında Budapeşte Anlaşması

Suç faaliyetleri elektronik veri işleme sistemlerini daha fazla kullanıp etkiledikçe, bu zorluğun karşılanması için yeni cezai kanun hükümleri gerekmektedir. Dolayısıyla Avrupa Konseyi, bir uluslararası hukuki belgeyi – Budapeşte Anlaşması olarak bilinen Siber suçlar Anlaşması – elektronik ağlara karşı ve onlar yoluyla işlenen suçlara ilişkin problemlere çözüm üretmek adına hayata geçirmiştir.[726] Bu anlaşma Avrupa Konseyi üyesi olmayanların da erişimine açıktır. 2018 başı itibariyle, Avrupa Konseyi dışında 14 devlet anlaşmaya taraf olmuştur[727] ve üye olmayan diğer yedi devlete kabul etmeleri yönünde davet gönderilmiştir.

Siber suçlar anlaşması internet ya da diğer bilgi ağları üzerinden gerçekleşen ihlallerle ilişkili en etkili uluslararası anlaşma olmaya devam etmektedir. Tarafların ceza kanunlarını hackleme ve telif hakkı ihlalleri, bilgisayar yoluyla dolandırıcılık, çocuk pornosu ve diğer gayri meşru siber aktiviteler dahil diğer güvenlik ihlallerine karşı uyumlu hale getirmelerini şart koşmaktadır. Anlaşma ayrıca bilgisayar ağlarının aranması ve siber suçlarla mücadele bağlamında iletişimin gözetlenmesini de içeren usuli yetkileri de düzenlemektedir. Son olarak, etkin uluslararası iş birliğine olanak tanımaktadır. Anlaşmanın bir ek protokolü bilgisayar ağlarında ırkçı ve yabancı düşmanı propagandanın suç haline getirilmesi ile ilgilidir.

Anlaşma veri korumayı desteklemek üzerine bir belge olmasa da, veri sahibinin verileri üzerindeki haklarını ihlal etmesi muhtemel faaliyetleri suç haline getirmektedir. Dahası, Sözleşmenin Taraflarına ulusal otoritelerine verilerin dolaşımı ve içeriğini gözetlemelerine izin vermelerini şart koşmaktadır.[728] Ayrıca Sözleşmenin Taraflarına sözleşmeyi uygularken veri koruma hakkı gibi AİHS altında korunan haklar dahil insan hak ve özgürlüklerine yönelik yeterli korumayı öngörme yükümlülüğü getirmektedir.[729] Tarafların Siber Suçlar Hakkında Budapeşte Anlaşması'na taraf olmak için Sözleşme 108'e de taraf olması gerekmemektedir.

---

[726] Avrupa Konseyi, Bakanlar Komitesi (2001), Siber Suçlar Sözleşmesi, CETS No. 185, Budapeşte, 23 Kasım 2001, 1 Temmuz 2004'te yürürlüğe girmiştir.
[727] Avustralya, Kanada, Şili, Dominik Cumhuriyeti, Israil, Japonya, Mauritius, Panama, Senegal, Sri Lanka, Tonga ve Birleşik Devletler. Bkz: Temmuz 2017 itibariyle Sözleşme 185'in imza ve onay tablosu
[728] Avrupa Konseyi, Bakanlar Komitesi (2001), Siber Suçlar Sözleşmesi, CETS No. 185, Budapeşte, 23 Kasım 2001, Md. 20 ve 21.
[729] A.g.e., Md. 15 (1).

8.2. AB hukukunda polis ve ceza yargılaması hususlarında veri koruma

Kilit Noktalar

- AB içerisinde, polis ve ceza yargılaması sektöründe verilerin korunması Üye Devlet ve AB aktörlerinin polis ve ceza yargılaması otoriteleri tarafından gerçekleştirilen ulusal ve sınır ötesi veri işleme faaliyetleri bağlamında düzenlenmiştir.
- Üye Devlet düzeyinde, Polis ve Ceza Yargılaması Otoriteleri için Veri Koruma Direktifi ulusal hukukun içine yerleştirilmelidir.
- Polis ve kolluk sınır ötesi iş birliğinde, özellikle terörizm ve sınır ötesi suçlarla mücadeleyi, özel hukuki belgeler yönetmektedir.
- Sınır ötesi kanuni yaptırıma yardım eden ve destekleyen AB kuruluşları olan Avrupa Polis Dairesi (Europol), AB Adli İşbirliği Birimi (Eurojust) ve yeni kurulan Avrupa Savcılık Makamı için özel veri koruma kuralları mevcuttur.
- Yetkin polis ve adli otoriteler arasında sınır ötesi bilgi alışverişi için AB düzeyinde oluşturulan müşterek bilgi sistemleri için de özel veri koruma kuralları söz konusudur. Önemli örnekler Schengen Bilgi Sistemi II (SIS II), Vize Bilgi Sistemi (VIS) ve AB Üye Devletlerinden birine sığınma başvurusunda bulunan üçüncü ülke vatandaşlarının ya da vatansız kişilerin parmak izi verilerini içeren merkezi bir sistem olan Eurodac'tır.
- AB, Polis ve Ceza Yargılaması Otoriteleri İçin Veri Koruma Direktifi ile aynı doğrultuda olmaları için yukarıda belirtilen veri koruma hükümlerini güncelleme aşamasındadır.

8.2.1. Polis ve Ceza Yargılaması Otoriteleri İçin Veri Koruma Direktifi

Direktif gerçek kişilerin verilerinin yetkin otoriteler tarafından suçların önlenmesi, tespiti, soruşturulması ve yargılaması veya cezaların infazı amacıyla işlenmesine karşı gerçek kişilerin korunması ve söz konusu verilerin serbest dolaşımı hakkında 2016/680/EU sayılı Direktif (Polis ve Ceza Yargılaması Otoriteleri için Veri Koruma Direktifi)[730] aşağıda yer alan ceza yargılaması amaçlarıyla toplanan ve işlenen kişisel verileri korumayı hedeflemektedir:

- suçların önlenmesi, tespiti, soruşturulması ve yargılaması veya cezaların infazı, kamu güvenliğine yönelik tehditlerin önlenmesine karşı korumalar da dahil olmak üzere;
- bir cezanın infazı; ve
- Polis veya diğer kolluk otoritelerinin kanunu uygulama ve kamu güvenliğine ve toplumun temel haklarına yönelik tehditlere karşı koruma oluşturma ve önleme amaçlı hareket ettiği haller.

Polis ve Ceza Yargılaması Otoriteleri İçin Veri Koruma Direktifi ceza yargılamalarında tanık, muhbir, şüpheli ve suç ortağı olarak yer almış farklı kişi kategorilerindeki kişilerin kişisel verilerini korumaktadır. Polis ve ceza yargılaması otoriteleri ne zaman kanuni yaptırım amaçlarıyla direktifin kişisel ve maddi kapsamı içerisinde kişisel veri işliyorlarsa, direktifin

[730] Avrupa Parlamentosu ve Konseyi 27 Nisan 2016 tarihli Direktif 2016/680/EU , OJ 2016 L 119, p. 89 (Polis ve Ceza Yargılaması Otoriteleri İçin Veri Koruma Direktifi).

hükümlerine uymakla yükümlüdür.[731]

Ancak, verilerin farklı bir amaçla kullanılmasına da belirli şartlar altında izin verilmektedir. Kişisel verilerin toplandıklarından farklı bir kolluk faaliyeti amacıyla işlenmesine ancak Ulusal ya da AB hukukuna göre hukuka uygun, gerekli ve ölçülü olduğu hallerde izin verilir.[732] Diğer amaçlar için, GDPR kuralları uygulanır. Şikayetlerden doğan sorumlulukların açıklanmasına yardımcı olunması için veri paylaşımının loglanması ve dokümante edilmesi yetkin otoritelerin özel görevlerinden biridir.

Polis ve ceza yargılaması alanında çalışan yetkin otoriteler kamu otoriteleri ya da ulusal hukuk ve kamusal otoriteler tarafından kamu otoritesinin fonksiyonlarını yerine getirmek üzere yetkilendirilmiş otoritelerdir,[733] örneğin özel işletmeye sahip hapishaneler.[734] Direktif'in uygulanabilirliği hem yerel düzeyde veri işlemeye hem de Üye Ülkelerin polis ve adli otoriteleri arasında sınır ötesi işlemelere hem de yetkin otoriteler tarafından üçüncü ülkelere ve uluslararası kuruluşlara yapılan aktarımlara uzanmaktadır.[735] Ulusal güvenlik veya kişisel verilerin AB kurum, kuruluş, büro ve daireleri tarafından işlenmesini kapsamamaktadır.[736]

Direktif, geniş oranda, polis ve ceza yargılaması alanlarının özel yapısı göz önüne alınarak, GDPR'da yer alan prensip ve tanımlara dayanmaktadır. Denetim, GDPR altında da söz konusu işlevi gören Üye Ülke otoriteleri tarafından gerçekleştirilebilecektir. Veri Koruma Görevlilerinin atanması ve Veri Koruma Etki Analizi'nin gerçekleştirilmesi direktife polis ve ceza yargılaması otoritelerine yönelik yeni yükümlülükler olarak eklenmiştir.[737] Her ne kadar bu konseptler GDPR'dan ilham alınmış olsa da, Direktif polis ve ceza yargılaması otoritelerinin özel tabiatını ele almaktadır. Tüzük ile düzenlenen ticari amaçlarla verilerin işlenmesine kıyasla güvenlik ile bağlantılı işleme faaliyetleri belirli bir düzeyde esneklik gerektirebilecektir. Örneğin, veri sahiplerine bilgi edinme hakkı, erişim hakkı, silme hakkı gibi hallerde GDPR'da düzenlenenle aynı düzeyde koruma sağlanması hukuki yaptırım bağlamında gerçekleştirilecek gözetleme faaliyetlerinin etkisiz olmasına sebep olabilecektir. Dolayısıyla bu Direktif şeffaflık prensibini içermemektedir. Benzer şekilde, veri minimizasyonu ve kişisel verilerin sadece toplandıkları amaçlar için gerekli olduğu ölçüde işlenmesini gerektiren amacın sınırlandırılması prensipleri aynı şekilde güvenlikle bağlantılı veri işlemelerde esnek biçimde uygulanmalıdır. Belirli bir dava kapsamında yetkin otoriteler tarafından toplanan ve muhafaza edilen bilgiler gelecekte başka davaların çözülmesi hususunda çok faydalı olabilecektir.

İşlemeyle alakalı prensipler

Polis ve Ceza Yargılaması Otoriteleri İçin Veri Koruma Direktifi kişisel verilerin kullanılması hususunda bazı önemli korumalar belirlemektedir. Ayrıca bu verilerin işlenmesine yönelik prensipler de belirlemektedir. Üye Devletler kişisel veriler açısından aşağıdakileri temin etmelidir:

---

[731] Polis ve Ceza Yargılaması Otoriteleri İçin Veri Koruma Direktifi, Md. 2 (1).
[732] A.g.e., Md. 4 (2).
[733] A.g.e., Md. 3 (7).
[734] Avrupa Komisyonu (2016), Komisyon'dan Avrupa Parlamentosu'na TFEU Madde 294 (6) uyarınca Konsey'in ilgili kişilerin kişisel verilerinin cezai suçların önlenmesi, soruşturulması, tespiti veya yargılaması amacıyla ya da cezaların uygulanması amacıyla yetkin otoriteler tarafından işlenmesi karşısında korunması ve söz konusu verilerin serbest dolaşımı hakkındaki ve 2008/977/JHA sayılı Konsey Çerçeve Kararı'nı ilga eden Avrupa Parlamentosu ve Konseyi Direktifi'nin kabulü hakkında ileti, COM(2016) 213 final, Brüksel, 11 Nisan 2016.
[735] Polis ve Ceza Yargılaması Otoriteleri İçin Veri Koruma Direktifi, Bölüm V.
[736] A.g.e., Md. 2 (3).
[737] A.g.e., sırasıyla Md. 32 ve Md. 27.

- Hukuka uygun ve adil olarak işlenmeleri;
- Belirli, açık ve meşru amaçlar için toplanmaları ve bu amaçlarla uyumlu olmayan bir biçimde işlenmemeleri;
- İşlenme amaçları açısında yeterli, ilişkili ve aşırı olmaması;
- Doğru, ve gerekliği olduğunda, güncel tutulmaları; işlenme amaçları göz önüne alındığında doğru olmayan kişisel verilerin gecikme olmaksızın silinmesi veya yok edilmesi için gerekli tüm adımlarının atıldığının temin edilmesi;
- İşlenme amaçlarının gerektirdiğinden daha uzun süre veri sahiplerinin kimliklerinin belirlenmesine olanak tanımayan bir şekilde saklanmaları;
- Kişisel verilerin yetkisiz ya da hukuka aykırı işleme ve kazaen kayıplara, yok olma ya da hasara karşı, uygun teknik ve idari önlemlerle yeterli güvenliğinin temin edilmesini sağlayacak şekilde işlenmesi;[738]

Direktif altında, veri işleme ancak ilgili görevin ifa edilmesi kapsamında gerekli olduğu müddetçe hukuka uygundur. Ayrıca, Direktifte belirtilen amaçların sağlanması amacıyla yetkin bir otorite tarafından ve AB hukuku ya da ulusal hukuka dayalı olarak yapılmalıdır.[739] Veriler gerekli olandan daha uzun süre tutulmamalıdır ve periyodik olarak silinmeli ya da gözden geçirilmelidir. Sadece yetkin otorite tarafından ve kişisel verilerin toplandığı, aktarıldığı ya da erişime açıldığı amaçlarla kullanılmalıdır.

Veri sahibinin hakları

Bu Direktif veri sahiplerinin haklarını da belirlemektedir. Bunlar aşağıdakileri kapsamaktadır:

- Bilgi edinme hakkı. Üye Devletler veri sorumlusuna veri sahibine 1) veri sorumlusunun kimliği ve iletişim bilgileri 2) veri koruma görevlisinin iletişim bilgileri 3) planlanan işleme faaliyetinin amaçları 4) denetleyici otoriteye şikayette bulunma hakkı ve iletişim bilgileri 5) kişisel verilere erişim hakkı, silme ve yok etme hakkı ve verilerin işlenmesini sınırlama haklarını sağlama yükümlülüğü yüklemelidir.[740] Bu genel bilgi gerekliliklerine ek olarak, direktif, özel durumlarda haklarının kullanılmasını sağlamak için veri sorumlularının veri sahiplerine işlemenin hukuki dayanağı ve verilerin ne kadar saklanacağı hususunda bilgi vermelerini düzenlemektedir. Eğer kişisel veriler üçüncü ülkelerdekiler ve uluslararası kuruluşlar dahil olmak üzere başka alıcılara aktarılacaksa veri sahibi alıcı kategorileriyle ilgili bilgilendirilmelidir. Son olarak, veri sorumluları kişisel verilerin işlendiği özel durumları – örneğin kişisel veriler gizli izleme neticesinde toplanıyorsa - göz önüne alarak her türlü ek bilgiyi sağlamalıdır. Bu veri sahibi adına adil işleme faaliyetini korumaktadır.[741]
- Kişisel verilere erişim hakkı. Üye Devletler veri sahiplerinin kişisel verilerinin işlenip işlenmediğini öğrenme hakkını temin etmelidir. Eğer işleniyorsa, veri sahibi işlenen kişisel veri kategorileri gibi belirli bilgilere erişebilmelidir.[742] HAncak bu hak sınırlanabilir – örneğin, soruşturmanın engellenmesini veya bir suçun yargılamasına gölge düşürülmesini önlemek ya da kamu güvenliğini ve diğerlerinin hak ve özgürlüklerini korumak -[743]

[738] A.g.e., Md. 4 (1).
[739] A.g.e., Md. 8.
[740] A.g.e., Md. 13 (1).
[741] A.g.e., Md. 13 (2).
[742] A.g.e., Md. 14.
[743] A.g.e., Md. 15.

- Kişisel verilerin yok edilmesini isteme hakkı. Üye Devlet veri sahibinin, doğru olmayan kişisel verilerin gecikmeksizin yok edilmesini sağlama hakkının temin edilmesiyle yükümlüdür. Dahası, veri sahibi eksik kişisel verilerin tamamlanması hakkına da sahiptir.[744]
- Kişisel verilerin silinmesi ve işlenmenin kısıtlanması hakkı. Belirli hallerde, veri sorumlusunun kişisel verileri silmesi geekmektedir. Ayrıca, veri sahibi kişisel verilerinin silinmesini sağlayabilir ancak sadece hukuka aykırı işlendiklerinde.[745] 758 Belirli durumlarda, kişisel verilerin silinmesi yerine işlenmesinin kısıtlanması söz konusu olabilir. Bu durum 1) kişisel verilerin doğruluğu tartışılmakta olup bu durum doğrulanamıyorsa 2) kişisel verilere delil amacıyla ihtiyaç duyuluyorsa ortaya çıkabilir.[746]

Veri sorumlusu kişisel verileri yok etmeyi ya da silmeyi veya kişisel verilerin işlenmesini kısıtlamayı reddediyorsa veri sahibi yazılı olarak bilgilendirilmelidir. Üye Devletler bu bilgi edinme hakkını kamu güvenliğini ya da başkalarının hak ve özgürlüklerini korumak için, erişim hakkındaki aynı sebeplerle kısıtlayabilir.[747]

Veri sahibi normal şartlar altında kişisel verilerinin işlenmesine dair bilgi edinme hakkına ve doğrudan veri sorumlusuna başvurarak kullanabileceği erişim, yok etme, silme, kısıtlama haklarını haizdir. Bir son çare olarak, Polis ve Ceza Yargılaması Veri Koruma Direktfi kapsamında veri sahibi haklarının veri koruma denetleyici otoritesi yoluyla dolaylı olarak kullanılması da mümkündür ve veri sorumlusu veri sahibinin hakkını kısıtladığı takdirde devreye girer.[748] Direktif'in 17. Maddesi Üye Devletlerin veri sahiplerinin haklarının kendi denetleyici otoriteleri vasıtasıyla da kullanabilmesini temin eden önlemleri almasını şart koşmaktadır. Bu nedenle, veri sorumluları veri sahibini dolaylı erişim olanağı hakkında bilgilendirmelidir.

Veri sorumlusu ve veri işleyenin yükümlülükleri

Polis ve Ceza Yargılaması Otoriteleri İçin Veri Koruma Direktifi bağlamında, veri sorumluları yetkili kamu otoriteleri ya da kişisel verilerin işlenmesine dair amaçları ve araçları belirleyen ilgili kamusal yetkilere sahip diğer kuruluşlardır. Direktif veri sorumlularına kanuni yaptırım amaçlarıyla işlenen kişisel verilere yüksek düzeyde koruma sağlamak amacıyla birçok yükümlülük getirmektedir.

Yetkili makamlar otomatik işleme sistemlerinde gerçekleştirdikleri işleme faaliyetleri için logları tutmak zorundadır. Loglar en azından toplama, değiştirme, danışma, aktarım dahil ifşalar, birleştirme ve kişisel verilerin silinmesi için tutulmalıdır.[749] Direktife göre, danışma ve ifşanın logları; faaliyetin tarih ve saatini, gerekçesini ve mümkün olduğu oranda sisteme erişen ya da aktarımı yapan kişinin kimliğini ve ilgili verilerin alıcısını belirlemeyi olanaklı kılmalıdır. Loglar sadece işlemenin hukukiliğini doğrulamak, öz-izleme, kişisel verilerin doğruluğunu ve güvenliğini temin etme ve ceza yargılamaları amaçlarıyla kullanılmalıdır.[750] Denetleyici otoritenin talebi üzerine, veri sorumlusu ve veri işleyen logları erişimine sunmalıdır.

[744] A.g.e., Md. 16 (1).
[745] A.g.e., Md. 16 (2).
[746] A.g.e., Md. 16 (3).
[747] A.g.e., Md. 16 (4).
[748] A.g.e., Md. 17.
[749] A.g.e., Md. 25 (1).
[750] A.g.e., Md. 25 (2).

Bilhassa, veri sorumluları için veri işlemenin bu direktife uygun biçimde gerçekleşmesinin temini ve söz konusu işlemenin hukuka uygunluğunu kanıtlayabilmek için uygun teknik ve idari tedbirleri alma yönünde genel bir yükümlülük vardır.[751] Bu önlemleri tasarlarken, veri işlemenin tabiatını, kapsamını ve bağlamını ve ilgili kişilerin hak ve özgürlüklerine yönelik herhangi bir olası riski göz önüne almaları gerekmektedir. Veri sorumluları veri koruma prensipleriyle, özellikle tasarımla gelen ve varsayılan veri koruma prensipleriyle, uyumu kolaylaştırmak için dahili politikalar edinmeli ve önlemleri uygulamalıdır.[752] Veri işlemenin ilgili kişilerin haklarına yönelik yüksek risk doğurmasının muhtemek olduğu hallerde – örneğin yeni teknolojilerin kullanımı sebebiyle - veri sorumluları işlemeye başlamadan önce veri koruma etki analizi gerçekleştirmek zorundadır.[753] Direktif ayrıca veri işlemenin güvenliğinin temini için uygulanması zorunlu olan önlemleri saymaktadır. Bunlar, kişisel verilere yetkisiz erişimi önlemek, yetkili kişilerin sadece yetkilerinin kapsadığı kadarıyla erişebildiklerinin temin edilmesi, işleme sisteminin fonksiyonlarının düzgün çalışmasının temini ve muhafaza edilen kişisel verilerin sistemdeki bir aksaklık nedeniyle zarar göremeyeceğinin teminine yönelik önlemleri içermektedir.[754] Şayet bir kişisel veri ihlali meydana gelirse; veri sorumluları denetleyici otoriteyi üç gün içerisinde ihlalin niteliğini, muhtemel sonuçlarını, ilgili kişisel veri kategorilerini ve tahmini etkilenen veri sahibi sayısını içerecek şekilde bilgilendirmelidir. Kişisel veri ihlal olayının, ilgili kişinin hak ve özgürlüklerine yönelik yüksek risk doğurmasının muhtemel olduğu hallerde veri sahibine de "fazla gecikmeksizin" bildirilmelidir.[755]

Direktif hesap verilebilirlik prensibini içermekte olup veri sorumlularına bu prensiple uyum için önlemleri uygulama yükümlülüğü getirmektedir. Veri sorumluları sorumlulukları altındaki tüm veri işleme faaliyeti kategorilerini kayıt altına almalıdır: söz konusu kayıtların detaylı içeriği direktifin 24. Maddesinde belirtilmektedir. Kayıtlar talep halinde denetleyici otoritenin erişimine hazır olmalıdır, böylece veri sorumlusunun işleme faaliyetleri denetlenebilecektir. AHesap verilebilirliği sağlamak için bir başka önemli önlem bir Veri Koruma Görevlisi (DPO)'nin atanmasıdır. Direktif Üye Devletlere söz konusu yükümlülükten mahkemeleri ve diğer bağımsız adli makamları muaf tutma hakkı verse de, veri sorumluları bir DPO atamalıdır.[756]

DPO'nun görevleri GDPR altındakilere benzemektedir. DPO direktife uyumu denetler, bilgi sağlar ve veri işleme faaliyetlerinde bulunan çalışanlara veri koruma mevzuatı altındaki yükümlülükleri üzerine tavsiyeler verir. DPO ayrıca veri koruma etki analizi gerçekleştirilmesine yönelik ihtiyaç hususunda tavsiyeler verir ve denetleyici otorite ile irtibat kişisi olarak hareket eder

Üçüncü ülkelere veya uluslararası kuruluşlara aktarımlar

GDPR'a benzer şekilde, direktif kişisel verilerin üçüncü ülkelere veya uluslararası kuruluşlara aktarımı için şartlar ortaya koymaktadır. Eğer veriler AB yargı alanının dışına serbest şekilde aktarılırsa, AB hukuku altında tanınan önlemler ve kuvvetli korumalar baltalanabilecektir. Ancak, şartlar GDPR'da yer alanlardan oldukça farklıdır. Üçüncü ülkelere ya da uluslararası kuruluşlara aktarıma ancak aşağıdaki hallerde izin verilmektedir:[757]

[751] A.g.e., Md. 19.
[752] A.g.e., Md. 20.
[753] A.g.e., Md. 27.
[754] A.g.e., Md. 29.
[755] A.g.e., Md. 30 ve 31.
[756] A.g.e., Md. 32.
[757] A.g.e., Md. 35.

- Aktarım direktifin amaçları için gerekliyse.
- Kişisel verilerin, direktif anlamında, üçüncü ülkenin ya da uluslararası kuruluşun yetkin otoritesine aktarılması – her ne kadar münferit ve belirli durumlarda bu kuralın istisnaları olsa da.[758]
- Sınır-ötesi iş birliği esnasında alınan kişisel verilerin üçüncü ülkelere ya da uluslararası kuruluşlara aktarımının, verinin kaynağının bulunduğu Üye Devletin yetkilendirmesini gerektirmesi halinde, her ne kadar acil hallerde muafiyetler mevcut olsa da.
- Avrupa Komisyonu tarafından bir yeterlilik kararı alınmış olması, yeterli korumaların oluşturulması, ya da özel durumlardaki aktarım istisnalarının uygulanabilir olması.
- Kişisel verilerin farklı bir üçüncü ülke ya da uluslararası kuruluşa ileri aktarımları, baştaki yetkili otoritenin yetkilendirmesini gerektirmektedir, bu otorite, diğer şeylerin yanında, suçun mahiyetini ve ikinci uluslararası aktarımdaki hedef ülkedeki veri koruma düzeyini göz önüne alacaktır.[759]

Direktif kapsamında, kişisel verilerin aktarımı üç koşuldan birinin sağlandığı takdirde mümkündür. Birincisi, Avrupa Komisyonu'nun direktif kapsamında bir yeterlilik kararı yayımlamasıdır. Bu karar üçüncü bir ülkenin tamamına uygulanabileceği gibi, üçüncü ülkenin belirli kısımlarına ya da bir uluslararası kuruluşa da uygulanabilir. Fakat, bu durum ancak yeterli korumanın temin edildiği ve direktifte yer alan koşulların yerine getirildiği hallerde mümkün olabilecektir.[760] Bu gibi durumlarda, kişisel verilerin aktarımı Üye Devletin onayına tabi değildir.[761] Avrupa Komisyonu yeterlilik kararının işlevini etkileyebilecek gelişmeleri takip etmelidir. İlaveten, kararın periyodik gözden geçirme mekanizmasını içermesi gerekmektedir. Komisyon, mevcut bilgiler üçüncü ülke ya da uluslararası kuruluştaki şartların artık yeterli koruma düzeyini sağlamadığını gösteriyorsa, kararı geri alabilir, değiştirebilir ya da askıya alabilir. Bu halde, Komisyon'un duruma bir çözüm bulunması için üçüncü ülke ya da uluslararası kuruluşla istişarelere girmesi gerekmektedir.

Yeterlilik kararının mevcut olmadığı hallerde, aktarımlar yeterli korumanın sağlanmasına dayanabilir. Bu korumalar hukuken bağlayıcı belgelerle ortaya konulabilir ya da veri sorumlusu aktarım çerçevesindeki koşulları kendi içinde değerlendirerek yeterli korumaların mevcut olduğuna kanaat getirebilir. Bu öz değerlendirme Europol ve Eurojust ile üçüncü ülke ya da uluslararası kuruluş arasında akdedilmiş olabilecek iş birliği anlaşmalarını, gizlilik yükümlülüklerini ve verilerin ölüm cezası dahil herhangi bir zalimce ya da insanlığa sığmayan muamele amacıyla kullanılmayacağına yönelik verilen garantileri ve amacın sınırlandırılmasını da göz önüne almalıdır.[762] Bu son halde, veri sorumlusu yetkin denetleyici otoriteyi aktarımın kategorileri hususunda bilgilendirmelidir.[763]

Herhangi bir yeterlilik kararı alınmadığı ve uygun korumaların sağlanmadığı hallerde, aktarımlara yine de direktifte çerçevesi çizilen özel durumlarda izin verilebilir. Bunlar, diğerlerinin yanında, veri sahibi ya da başka bir kişinin hayati çıkarlarının korunmasını ve Üye Devlet ya da bir üçüncü ülkenin kamu güvenliğine karşı ani ve ciddi bir tehdidin önlenmesini içermektedir.

---

[758] A.g.e, Md. 39.
[759] A.g.e., Md. 35 (1).
[760] A.g.e., Md. 36.
[761] A.g.e., Md. 36 (1).
[762] A.g.e., Başlangıç 71.
[763] A.g.e., Md. 37 (1).

Münferit ve özel durumlarda, yetkin otoritelerden üçüncü ülkede kurulmuş olup yetkin otorite olmayan alıcılara aktarımın gerçekleşmesi için, yukarıda belirtilen üç şarttan birinin yerine getirilmesinin yanı sıra Madde 39'da yer alan ilave şartların da yerine gelmesi gerekmektedir. Özellikle, aktarım ilgili kişilerin temel hak ve özgürlüklerinin aktarımı meşru kılan kamu menfaatine baskın gelip gelmediğini de değerlendirmesi gereken aktarımı yapan yetkili otoritenin görevinin ifası için kesin surette gerekli olmalıdır. Bu gibi aktarımlar dokümante edilmeli ve aktarımı yapan yetkili otorite, yetkin denetleyici otoriteyi bilgilendirmelidir.

Son olarak ve üçüncü ülkeler ve uluslararası kuruluşlara ilişkin olarak, Direktif uluslararası iş birliği mekanizmalarının, mevzuatın etkin uygulanmasını sağlamak için, kurulmasını şart koşmaktadır ve böylece veri koruma denetleyici otoritelerin yurtdışındaki muadilleriyle iş birliği yapmalarına yardımcı olmaktadır.

Veri sahipleri için bağımsız denetim ve çareler

Her bir Üye Devlet, bir veya birden çok bağımsız yerel denetim otoritesinin direktif uyarınca kabul edilen düzenlemelerin uygulanmasına ilişkin görüş bildirme ve denetim yapmakla yükümlü kılınması gerekir[764]. Direktif uyarınca kurulan denetim otoritesi ile Genel Veri Koruma Regülasyonu kapsamında kurulan denetim otoritesi ile aynı olabilir ancak Üye Devletler, bağımsızlık şartını sağladığı sürece başka bir otorite belirlemekte serbesttirler. Denetim otoriteleri aynı zamanda yetkili otoritelerce kişisel verilerin işlenmesine ilişkin hak ve özgürlüklerinin korunmasına ilişkin herhangi bir kişinin yapacağı talepleri değerlendirecektir.

Veri sahibinin haklarını kullanması inandırıcı temeller dahilinde reddedilmiş olursa veri sahibinin yetkili yerel denetim otoritesine ve/veya mahkeme nezdinde temyiz hakkı olmalıdır. Direktifi uygulayan iç hukukun ihlali nedeniyle kişi zarar görürse bu kişinin veri sorumlusu veya Üye Devlet hukukunda yetkili herhangi bir otorite tarafından tazminata hakkı olmalıdır[765]. Genel olarak veri sahipleri, direktifi uygulayan iç hukuk tarafından garanti edilen haklarının herhangi bir ihlali halinde hukuki çarelere erişimi olmalıdır[766].

8.3. Emniyete ilişkin alanlarda veri korumasına dair diğer spesifik hukuki araçlar

Polis ve Ceza Yargılaması Otoriteleri için Veri Koruma Direktifi'ne ek olarak Üye Devletler tarafından bulundurulan bilgilerin belirli alanlarda paylaşılması, Üye Devletler arasında sabıka kayıtlarından elde edilen bilgilerin paylaşımının organizasyonu ve içeriğine ilişkin 2009/315/JHA sayılı Konsey Çerçeve Kararı, bilgi değişimine ilişkin Üye Devletlerin finansal istihbarat birimleri arasında iş birliği için düzenlemelere dair 2000/642/JHA sayılı Konsey Kararı ve Avrupa Birliği'nin Üye Devletlerinin kolluk otoriteleri arasında bilgi ve istihbarat değişiminin basitleştirilmesine ilişkin 2006/960/JHA sayılı ve 18 Aralık 2006 tarihli Konsey Çerçeve Kararı gibi birçok hukuki enstrümanla düzenlenmiştir[767].

Önemli arz eden bir diğer husus, yetkili otoriteler arasında sınır ötesi iş birliklerinin artan bir şekilde göçmen verisi içermesidir. Bu hukuk alanı polis ve ceza yargılaması konularına

[764] *A.g.e.,* Madde 38(1).
[765] *A.g.e.,* Madde 56.
[766] *A.g.e.,* Madde 54.
[767] Avrupa Birliği Konseyi (2009), sabıka kayıtlarından elde edilen bilgilerin paylaşımının organizasyonu ve içeriğine ilişkin 2009/315/JHA sayılı ve 26 Şubat 2009 tarihli Konsey Çerçeve Kararı, OJ 2009 L 93; Avrupa Birliği Konseyi (2000), bilgi değişimine ilişkin Üye Devletlerin finansal istihbarat birimleri arasında iş birliği için düzenlemelere dair 17 Ekim 2009 tarihli 2000/642/JHA sayılı Konsey Kararı, OJ 2000 L 271; Avrupa Birliği'nin Üye Devletlerinin kolluk otoriteleri arasında bilgi ve istihbarat değişiminin basitleştirilmesine ilişkin 2006/960/JHA sayılı ve 18 Aralık 2006 tarihli Konsey Çerçeve Kararı, OJ L 386.

girmemektedir ancak polis ve yargılama otoritelerinin işleri ile birçok açıdan ilgilidir. Aynı durum AB içerisinden ihraç edilen veya AB'ye ithal edilen ürünler için de geçerlidir. Schengen alanı kapsamında iç sınır kontrollerinin kaldırılması dolandırıcılık riskini yükseltmekte, Üye Devletler arasında özellikle sınır ötesi bilgi değişiminin daha etkin bir şekilde yerel ve AB gümrük mevzuat ihlallerini tespit edecek ve kovuşturacak şekilde iyileştirilmesi olmak üzere yoğunlaştırılmış iş birliğini gerekli kılmıştır. Bunlara ek olarak son senelerde dünyada, uluslararası seyahatleri de içeren ciddi ve organize suç ve terörizmin arttığı ve sınır ötesi polis ve kolluk iş birliğinin de birçok alanda artırılması gerektiği görülmektedir[768].

Prüm Kararı

Ülkece tutulan verilerin değiştirilmesi ile kurumlaşmış sınır ötesi iş birliğinin önemli örneklerinden bir tanesi, uygulama hükümlerini dahil olmak üzere sınır ötesi iş birliğinin artırılmasına ve özellikle terörizm ve sınır ötesi suçlarla mücadele edilmesine ilişkin olan ve 2008 yılında Prüm Anlaşmasını AB hukukuna dahil eden 2008/615/JHA sayılı Konsey Kararıdır (Prüm Kararı)[769]. Prüm Anlaşması, 2005 yılında Avusturya, Belçika, Fransa, Almanya, Lüksemburg, Hollanda ve İspanya arasında imzalanan bir uluslararası polis iş birliği anlaşmasıdır[770].

Prüm Kararı, imzacı Üye Devletlerin üç alandaki suçları önlemesi ve bunlarla mücadele etmesi amacıyla bilgi paylaşımının artırılmasına yardım etme amacı taşır. Bu üç alan; terörizm, sınır ötesi suçlar ve hukuka aykırı göçtür. Bu amaçla karar, aşağıdaki hususlara ilişkin düzenlemeler içermektedir:

- DNA profillerine, parmak izi verilerine ve birtakım ulusal araç kayıtları verilerine otomatik erişim;
- Sınır ötesi boyutu olan önemli olaylara ilişkin verinin sağlanması;
- Terör suçlarının önlenmesi için bilgi sağlanması;
- Sınır ötesi polis iş birliğinin iyileştirilmesi için diğer önlemler.

Prüm Kararı uyarınca erişime açık veri tabanları, tamamen ulusal hukuk ile yönetilmekte ancak verilerin değişiminde ek olarak karar uygulanmakta, bu kararın Polis ve Ceza Yargılaması Otoriteleri için Veri Koruma Direktifi ile uyumluluğunun incelenmesi gerekmektedir. Bu tür veri aktarımlarının denetlenmesi için yetkili birimler, ulusal veri koruma denetim otoriteleridir.

2006/960/JHA Çerçeve Kararı – İsveç Girişimi

2006/960/JHA sayılı Çerçeve Karar (İsveç Girişimi)[771], kolluk otoritelerince tutulan verilerin değişimine ilişkin sınır ötesi iş birliğine bir başka örnek teşkil etmektedir. İsveç Girişimi özellikle istihbarat ve bilgi değişimine odaklanmakta ve Madde 8'deki spesifik veri koruma kurallarını öngörmektedir.

---

[768] Bkz. Avrupa Komisyonu (2011), Yolcu İsim Kaydı verilerinin terör suçlarını ve ağır suçları önlemek, tespit etmek, soruşturmak ve kovuşturmak için kullanılmasına ilişkin Avrupa Parlamentosu ve Konseyi'nin Direktif Teklifi, COM(2011) 32 final, Brüksel, 2 Şubat 2011, sf.1.

[769] Avrupa Birliği Konseyi (2008), sınır ötesi iş birliğinin özellikle terörizm ve sınır ötesi suçlarla mücadelede artırılması hakkında 2008/615/JHA sayılı ve 23 Haziran 2008 tarihli Konsey Kararı, OJ 2008 L 210.

[770] Belçika Krallığı, Almanya Federal Cumhuriyeti, İspanya Krallığı, Fransız Cumhuriyeti, Lüksemburg Büyük Dükalığı, Hollanda Krallığı ve Avusturya Cumhuriyeti arasında özellikle terörizm, sınır ötesi suçlar ve hukuka aykırı göçle mücadeleye ilişkin sınır ötesi iş birliğinin artırılmasına dair anlaşma

[771] Avrupa Birliği Konseyi (2006), Avrupa Birliği'nin Üye Devletlerinin kolluk otoriteleri arasında bilgi ve istihbarat değişiminin basitleştirilmesine ilişkin 2006/960/JHA sayılı ve 18 Aralık 2006 tarihli Konsey Çerçeve Kararı.

Bu belge uyarınca değişime konu bilgi ve istihbaratın kullanılması, bilgiyi alan Üye Devletin ulusal veri koruma düzenlemelerine, adeta veriler bu Üye Devlette toplanmış gibi tabi olmalıdır. Madde 8 bunun da ötesine geçerek; bilgi ve istihbaratın sağlanması sırasında otorite, bunların kullanımına ilişkin olarak kendi ulusal hukuku uyarınca ve muhatap ülkenin kolluk mercilerinin tabi olacağı şartlar getirebilir. Bu şartlar, bilgi ve istihbarat değişimini gerektiren ceza soruşturmaları veya cezai istihbarat operasyonlarının sonuçlarının raporlanmasına da uygulanabilecektir. Ancak ulusal hukuk kullanıma ilişkin kısıtlamalara istisna getirdiğinde bilgi ve istihbarat ancak gönderen Üye Devlet ile önceden yapılacak bir danışma sonucunda kullanılabilecektir.

Sunulan bilgi ve istihbarat aşağıdaki hallerde kullanılabilir:

- Verilerin gönderilmesi ile hedeflenen amaç için; veya
- Kamu güvenliğine karşı mevcut ve ciddi bir tehdidin önlenmesi için.

Başka amaçlar ile kullanıma, ancak gönderen Üye Devlet'in ön onayı üzerine izin verilebilir.

Bunun yanında İsveç Girişimi, işlenen kişisel verilerin aşağıdaki uluslararası araçlar ile uyumlu olarak korunması gerektiğini belirtmektedir:

- Kişisel Verilerin Otomatik İşlenmesine ilişkin Kişilerin Korunması için Avrupa Konseyi Anlaşması[772];
- Bu Anlaşma'nın Denetim Otoriteleri ve Sınırlararası Veri Akışına ilişkin 8 Kasım 2001 tarihli Ek Protokolü[773];
- Polis Sektöründe Kişisel Verilerin Kullanılmasını Düzenleyen R(87) 15 sayılı Avrupa Konseyi Tavsiye Kararı[774]

AB PNR Direktifi

Yolcu İsim Kaydı (PNR) verileri, taşıyıcıların rezervasyon ve kalkış kontrol sistemleri tarafından kendi ticari amaçları doğrultusunda elde edilen ve saklanan uçuş yolcuları bilgilerine ilişkindir. Bu veriler, yolculuk tarihleri, seyahat programı, bilet bilgisi, iletişim bilgileri, uçuşun rezerve edildiği seyahat acentesi, kullanılan ödeme yöntemi, koltuk numarası ve bagaj bilgisi gibi pek çok farklı bilgi türünü içermektedir[775]. PNR verilerinin işlenmesi, kolluk otoritelerine bilinen veya potansiyel şüphelileri belirlemelerinde ve genellikle suç faaliyetleri ile ilişkilendirilen yolculuk şemaları ve diğer göstergelere ilişkin değerlendirilmeleri yürütmelerinde yardımcı olabilecektir. PNR verilerinin analiz edilmesi aynı zamanda geriye dönük olarak yolculuk rotalarının ve suç faaliyetlerine dahil olduklarından şüphelenilen kişilerin kontaklarının takip edilmesine, dolayısıyla kolluk otoritelerinin suç ağlarını tespit

[772] Avrupa Konseyi (1891), Kişisel Verilerin Otomatik İşlenmesine ilişkin Kişilerin Korunması için Anlaşma, ETS n.108.
[773] Avrupa Konseyi (2001), Kişisel Verilerin Otomatik İşlenmesine ilişkin Kişilerin Korunması için Anlaşma'ya denetim otoriteleri ve sınırlararası veri akışına ilişkin Ek Protokol, ETS n.108.
[774] Avrupa Konseyi (1987), polis sektöründe kişisel veirleirn kullanılmasını düzenleyen üye devletlere yönelik R(87) 15 sayılı Bakanlar Komitesi Tavsiyesi (Bakanlar Komitesi tarafından 17 Eylül 1987 tarihli Bakanların Vekilleri toplantısında kabul edilmiştir).
[775] Avrupa Komisyonu (2011), Yolcu İsim Kayıt verilerinin terör suçlarının ve ağır suçların önlenmesi, tespit edilmesi, araştırılması ve kovuşturulmasına ilişkin Avrupa Parlamentosu ve Konseyi Direktif Teklifi, COM(2011) 32 final, Brüksel, 2 Şubat 2011, sf.1.

etmesine imkan tanır. Başlık 7'de açıklandığı üzere AB, PNR verilerinin değişimi için üçüncü ülkeler ile birtakım anlaşmalar akdetmiştir. Buna ek olarak, PNR verilerinin terör suçlarının ve ağır suçların önlenmesi, tespit edilmesi, araştırılması ve kovuşturulmasına ilişkin 2016/681/EU sayılı Direktif (AB PNR Direktifi)[776] ile AB içerisinde PNR verilerinin işlenmesini düzenlemiştir. Bu direktif, hava yolu şirketlerine PNR verilerini yetkili otoritelere iletmelerine ilişkin yükümlülük getirmekte ve bu verilerin işlenmesi ve toplanması için katı veri koruma tedbirleri belirlemektedir. AB PNR Direktifi, AB'den veya AB'ye olan uluslararası uçuşlara uygulandığı gibi Üye Devletin bu yöndeki kararına bağlı olarak AB içi uçuşlara da uygulanmaktadır[777].

Toplanan PNR verileri sadece AB PNR Direktifi'nin izin verdiği bilgileri içermelidir. Bu veriler, her Üye Devlette güvenli bir yerde tek bir bilgi biriminde tutulmalıdır. PNR verisi, havayolu şirketi tarafından iletilmelerinden altı ay sonra anonim hale getirilmelidir ve en fazla 5 yıllık periyodlarla tutulmalıdır[778]. PNR verileri, Üye Devletler arasında, bir Üye Devlet ile Europol arasında ve ancak durum bazında olarak üçüncü ülkeler ile paylaşılmaktadır.

PNR verilerinin iletilmesi ve işlenmesi ile ilgili kişiler için korunan haklar Polis ve Ceza Yargılaması Otoriteleri için Veri Koruma Direktifi ile uyumlu olmalı ve Bildirge, Modernize Edilmiş Sözleşme 108 ve AİHS'nin gerektirdiği yüksek seviyede gizlilik ile kişisel veri koruması sağlamalıdır.

AB PNR Direktifi uyarınca Üye Devletlerin yürürlüğe koyduğu düzenlemelerin uygulamalarına ilişkin görüş bildirilmesi ve bunların gözetiminden, Polis ve Ceza Yargılaması Otoriteleri için Veri Koruma Direktifi uyarınca yetkili bağımsız denetim otoriteleri de sorumludur.

Telekomünikasyon verilerinin saklanması

8 Nisan 2014 tarihinde *Digital Right Ireland* ile geçersiz ilan edilen Veri Saklama Direktifi[779], iletişim hizmeti sağlayıcılarını, spesifik olarak ağır suçlar ile savaşılması amacıyla 24 ayı geçmemek üzere en az altı ay boyunca meta veriyi, bu verilere faturalandırma veya hizmeti teknik olarak sunması için ihtiyacı olup olmasına bakmaksızın, hazır bulundurmak ile yükümlü tutmuştur.

Telekomünikasyon verilerinin saklanması açıkça verilerin korunması hakkına müdahale eder niteliktedir[780]. Bu müdahalenin meşruluğu AB Üye Devletlerinde birçok yargılamada tartışılmıştır[781].

---

[776] Yolcu isim kayıt (PNR) verilerinin terör suçlarının ve ağır suçların önlenmesi, tespit edilmesi, araştırılması ve kovuşturulması için kullanımına dair Avrupa Parlamentosu ve Konseyi 27 Nisan 2016 tarihli ve 2016/681 sayılı Direktif, OJ 2016 L 119, sf.132.

[777] PNR Direktifi, L 119, sf. 132, Madde 1(1) ve Madde 2(1).

[778] *A.g.e.*, Madde 12(1) ve Madde 12(2).

[779] Kamuya açık elektronik iletişimlerin hizmetlerine veya kamusal iletişim ağları düzenlemelerine ilişkin olarak üretilen veya işlenen verilerin saklanmasına dair ve 2002/58/EC sayılı Direktifi değiştiren Avrupa Parlamentosu ve Konseyi'nin 15 Mart 2006 tarihli 2006/24/EC sayılı Direktifi, OJ 2006 L 105.

[780] EDPS (2011), Veri Saklama Direktifi'ne (2006/24/EC sayılı Direktif) ilişkin Komisyon'dan Konsey ve Avrupa Parlamentosu'na Değerlendirme raporuna dair 31 Mayıs 2011 tarihli Görüş, 31 Mayıs 2011.

[781] Almanya, Federal Anayasa Mahkemesi (Bundesverfassungsgericht), 1 BvR 256/08, 2 Mart 2010; Romanya, Federal Anayasa Mahkemesi (Curtea Constituþionalã a Românieі), No. 1258, 8 Ekim 2009; Çek Cumhuriyeti, Anayasa Mahkemesi (Ústavní soud České republiky), 94/2011 Coll., 22 Mart 2011.

Örnek: *Digital Rights Ireland* ve *Kärntner Landesregierung and Others*[782] davalarında, Digital Rights grubu ve Bay Seitlinger, İrlanda'da ve Avusturya'da sırasıyla Yüksek Mahkeme'de ve Anayasa Mahkemesi'nde dava açarak elektronik telekomünikasyon verilerinin saklanmasına izin veren ulusal düzenlemelerin hukuka uygunluğunu gündeme getirilmiştir. Digital Rights, İrlanda mahkemesinden 2006/24 sayılı Direktif'i ve ulusal ceza kanunun terör suçlarına ilişkin kısmını geçersiz ilan etmesini talep etmiştir. Benzer şekilde Bay Seitlinger ve 11,000'den fazla başka başvuru sahipleri, Avusturya telekomünikasyon mevzuatının 2006/24 sayılı Direktif ile getirilmiş bir düzenlemesinin iptal edilmesini talep etmişlerdir.

Bu taleplere değindiği ön kararında CJEU, Veri Saklama Direktifi'nin geçersiz olduğunu ilan etmiştir. CJEU'ye göre direktif kapsamında saklanabilecek veriler tümüyle ele alındıklarında bireylere ilişkin kesin bilgiler sağlamaktadır. Bununla beraber, CJEU, özel hayata saygı ve kişisel verinin korunması temel haklarına yapılan müdahalenin ciddiyetine ilişkin değerlendirme yapmıştır. Buna göre saklama kamu yararı – özellikle ağır suçlarla mücadele ve dolayısıyla kamu güvenliği- amacını karşılamaktadır. Buna rağmen CJEU, AB yasa koyucusunun bu direktifi yürürlüğe sokarak orantılılık prensibini ihlal ettiğini belirtmiştir. Gerekli amacın karşılanmasında direktifin uygun olabilmekle beraber "Direktif'in gizliliğe saygı ve kişisel verilerin korunmasına temel haklarına geniş kapsamlı ve bilhassa ciddi müdahalesinin sınırları, müdahalenin gerçekten kesin surette gerekli olanla sınırlanmış olmasını sağlayacak şekilde çizilmemiştir".

2002/58/EC sayılı Direktif (Gizlilik ve Elektronik İletişimlere ilişkin Direktif)[783] kapsamında telekomünikasyonların gizliliğinin istisnası olarak veri saklama, önleyici tedbir olarak ancak sadece ağır suçlarla savaşma amacı ile, veri saklamaya ilişkin spesifik bir yasal düzenleme olmadıkça mümkündür. Böyle bir saklama; saklanan veri kategorilerine, etkilenen iletişimin yöntemi, ilgili kişiler ve saklama için belirlenen süre açılarından kesinlikle gerekli olan ile sınırlı olmalıdır. Ulusal otoriteler, saklanan verilere bağımsız mercilerin ön incelemeleri dahil olmak üzere ancak katı şartlar altında ulaşabilmelidir. Veriler AB içerisinde saklanmalıdır.

Örnek: Digital Rights Ireland ve Kärntner Landesregierung and Others kararlarını[784] takiben CJEU'nun önüne, İsveç ve Birleşik Krallık'ta, geçersiz kılınan Veri Saklama Direktifi tarafından gerektirildiği üzere elektronik iletişim hizmetleri sağlayıcılarına zorunlu tutulan telekomünikasyon verilerinin saklanmasına ilişkin genel yükümlülük hakkında iki tane daha dava getirilmiştir. Tele2 Sverige and Home Department/Tom Watson and Others davasında[785] CJEU, saklanması gereken veri ile kamu güvenliğine ilişkin tehdit arasında herhangi bir ilişki gerektirmeden ve hiçbir şart belirtmeden (saklama için süre aralığı, coğrafi

[782] CJEU, Birleştirilmiş dosyalar C-293/12 ve C-594/12, Digital Rights Ireland Ltd/Minister for Communications, Marine and Natural Resources and Others and Kärntner Landesregierung and Others [GC], 8 Nisan 2014, para. 65.
[783] Elektronik iletişim sektöründe kişisel verilerin işlenmesi ve gizliliğin korunmasına ilişkin Avrupa Parlamentosu ve Konseyi'nin 12 Temmuz 2002 tarihli ve 2002/58/EC sayılı Direktifi (Gizlilik ve elektronik iletişim Direktifi), OJ 2002 L 201.
[784] CJEU, Birleştirilmiş dosyalar C-293/12 ve C-594/12, Digital Rights Ireland Ltd/Minister for Communications, Marine and Natural Resources and Others and Kärntner Landesregierung and Others [GC], 8 Nisan 2014.
[785] CJEU, Birleştirilmiş dosyalar C-203/15 ve C-698/15, Tele2 Sverige AB/Post- och telestyrelsen and Secretary of State for the Home Department/Tom Watson and Others [GC], 21 Aralık 2016.

alan, ağır suçlara ilişkili olması muhtemel kişi grupları gibi) genel ve ayrım yapmaksızın verilerin saklanmasını düzenleyen ulusal yasa koyucuların, kesinlikle gereklilik teşkil etmenin limitlerini aştığını ve bu durumun demokratik bir toplumda meşru sayılamayacağını AB Temel Haklar Bildirgesi ışığında değerlendirilen 2002/58/EC sayılı Direktif uyarınca karara bağlamıştır.

Genel Bakış

Ocak 2017 tarihinde Avrupa Komisyonu, 2002/58/EC sayılı Direktif'i yürürlükten kaldıran ve elektronik iletişimde özel hayata saygı ve kişisel verilerin korunmasına ilişkin bir Tüzük teklifi yayınlamıştır[786]. Teklif veri saklanmasına ilişkin özel bir düzenleme getirmemektedir. Ancak, tüzük kapsamında Üye Devletlerin, sınırlamanın ulusal güvenlik, savunma, kamu güvenliği gibi spesifik bir kamu yararının korunması ve suç fiillerinin önlenmesi, soruşturulması, tespit edilmesi veya kovuşturulması veya cezai yaptırımların uygulanması için gerekli ve orantılı tedbir teşkil etmesi halinde kanunla birtakım yükümlülük ve hakları sınırlayabileceklerini düzenlemektedir[787]. Bu nedenle Üye Devletler, saklama tedbirlerine ilişkin ulusal veri saklama çerçevelerini, Birlik hukukuna uygun olduğu sürece ve CJEU'nun e-Gizlilik Direktifi ve AB Temel Haklar Bildirgesi'nin yorumlanmasına dair içtihatlarını dikkate alarak koruyabilecek veya düzenleyebileceklerdir[788]. El kitabının hazırlandığı dönemde tüzüğün kabulüne ilişkin tartışmalar devam etmektedir.

Kolluk amaçları dahilinde paylaşılan kişisel verilerin korunmasına ilişkin AB-ABD Kişisel Veri Güvenliği Şemsiye Anlaşması

1 Şubat 2017 tarihinde ABD ile suç fiillerinin önlenmesi, soruşturulması, tespit edilmesi ve kovuşturulması için kişisel verilerin işlenmesi için AB-ABD Şemsiye anlaşması yürürlüğe girmiştir[789]. AB-ABD Şemsiye anlaşması, AB ve ABD kolluk otoritelerinin iş birliğini artırırken AB vatandaşları için yüksek seviye veri koruması sağlamayı amaçlamaktadır. Kolluk otoriteleri arasında mevcut AB-ABD ve Üye Devlet-ABD sözleşmelerini tamamlamakta ve aynı zamanda bu alanda ileride yapılacak sözleşmeler için net ve uyumlu veri koruma kurallarının oluşturulmasına yardım etmektedir. Bu yönüyle sözleşme, bilgi değişiminin kolaylaştırılması için kalıcı bir hukuki çerçeve belirlenmesini hedeflemektedir.

Sözleşme kendi başına kişisel veri paylaşımı için uygun bir hukuki zemin sağlamamakla beraber bunun yerine ilgili kişilere uygun veri koruma güvenceleri sunmaktadır. Sözleşme, terörizm dahil olmak üzere suç fiillerinin önlenmesi, soruşturulması, tespit edilmesi ve kovuşturulması için gerekli tüm kişisel veri işleme faaliyetlerini kapsamaktadır[790].

---

[786] Avrupa Komisyonu (2017), elektronik iletişimlerde özel hayata saygı ve kişisel verileri korunmasına ilişkin ve 2002/58/EC sayılı Direktif'i yürürlükten kaldıran Avrupa Parlamentosu ve Konseyi'nin Tüzük Teklifi (Gizlilik ve Elektronik İletişim Regülasyonu), COM(2017) 10 final, Brüksel, 10 Ocak 2017.

[787] *A.g.e.*, Gerekçe 26.

[788] Gizlilik ve Elektronik İletişim Regülasyonu Teklifi açıklayıcı bilgi notu COM (2017) 10 final, madde 1.3'e bakınız.

[789] AB Konseyi (2016), "*Kolluk iş birliğinde AB vatandaşları için artırılmış veri koruma hakları: AB ve ABD "Şemsiye Sözleşme"yi imzaladı*", Basın Açıklaması 305/16, 2 Haziran 2016.

[790] Amerika Birleşik Devletleri ile Avrupa Birliği arasında 18 Mayıs 2016 tarihli suç fiillerinin önlenmesi, soruşturulması, tespit edilmesi ve kovuşturulmasına ilişkin kişisel bilgilerin korunması hakkında Sözleşme, (OR.en) 8557/16, Madde 3(1). Ayrıca bkz. 26 Mayıs 2010 tarihli AB-ABD veri koruma sözleşmesi müzakereleri hakkında Komisyon bildirimi, MEMO/10/216 ve26 Mayıs 2010 tarihli AB-ABD veri koruma sözleşmesinde yüksek gizlilik standartları hakkında AB Komisyonu Basın Açıklaması (2010), P/10/609.

Sözleşme, kişisel verilerin ancak sözleşmede belirtilen amaçlarla kullanılmasını sağlamak üzere birçok güvence belirlemiştir. Özellikle AB vatandaşlarına aşağıdaki korumaları öngörmüştür:

- Verinin kullanımının sınırlandırılması: suç fiillerinin önlenmesi, soruşturulması, tespit edilmesi ve kovuşturulması için kişisel veriler işlenebilir;
- Keyfi ve gerekçesiz ayrımcılıklara karşı koruma;
- İleri aktarımlar: ABD veya AB ülkesi olmayanlara veya uluslararası organizasyonlara yapılan herhangi bir ileri aktarım, veriyi aslen aktaran ülkenin yetkili otoritesinin ön onayına tabi olmalıdır;
- Verinin niteliği: kişisel veri saklanırken doğruluğu, ilgililiği, güncelliği ve tamlığı dikkate alınmalıdır;
- Kişisel veri ihlalinin bildirilmesi dahil olmak üzere işlenmenin güvenliği;
- Hassas verilerin işlenmesi ancak kanunlar uyarınca uygun tedbirler ile mümkündür;
- Saklama dönemleri: Kişisel veriler gerekli veya uygun sürelerin ötesinde saklanamayacaktır;
- Erişim ve düzeltme hakları: her birey, birtakım koşullar dahilinde kişisel verilerine erişmeye yetkilidir ve doğru olmaması halinde verinin düzeltilmesini talep edebilir;
- Otomatik karar verme, insan müdahalesinin söz konusu olabilmesi dahil, uygun güvenlik tedbirlerini gerektirir;
- AB ve ABD gözerim otoriteleri arasında iş birliği dahil olmak üzere etkili gözetim; ve
- Hukuki çareler ve yaptırım: ABD otoritelerinin erişim veya düzeltme taleplerini reddettiği veya kişisel verileri hukuka aykırı olarak ifşa ettiği hallerde AB vatandaşlarının ABD mahkemeleri nezdinde hukuki çare arama hakları[791] vardır.

"Şemsiye anlaşma" nezdinde aynı zamanda, gerekli olduğu hallerde, herhangi bir veri koruma ihlali hakkında bundan etkilenen kişinin bulunduğu Üye Devletteki yetkili otoritelere bildirim yapılmasına ilişkin bir sistem getirilmiştir. Anlaşma ile getirilen hukuki korumalar, gizlilik ihlali söz konusu olduğunda AB vatandaşlarının AB'de eşit muamele görmelerini güvence altına almaktadır[792].

8.3.1. AB Adli ve Kolluk Birimlerinde Veri Koruması

Europol

[791] AB Hukuki Çare Kanunu, 24 Şubat 2016 tarihinde Başkan Obama tarafından imzalanarak kanunlaşmıştır.

[792] Avrupa Veri Koruma Denetçisi, AB-ABD Anlaşması hakkında bir Görüş yayınlayarak, diğer görüşlerinin yanında şu eklemelerin yapılmasını tavsiye etmiştir: 1)" aktarılmalarının spesifik amacı için" ifadesinin verinin saklanmasında gereklilik ve uygunluk maddesine eklenmesini, 2) mümkün olabilecek hassas verilerin yığın halinde aktarımının kapsam dışında bırakılması. Bkz. Avrupa Veri Koruma Denetçisi, Görüş 1/2016, *Suç fiillerinin önlenmesi, soruşturulması, tespit edilmesi ve kovuşturulmasına ilişkin kişisel bilgilerin korunmasına ilişkin Amerika Birleşik Devletleri ile Avrupa Birliği arasında sözleşmeye dair ön görüş*, §35.

AB'nin adli kolluk birimi olan Europol (Avrupa Polis Teşkilatı), her bir Üye Devlette Europol Ulusal Birimleri (ENU) bulunmakla beraber merkezi Lahey'dedir. Europol, 1998'de kurulmuştur ve AB kurumu olarak hukuki statüsü, Adli Kolluk İş Birliği için Avrupa Birliği Kurumuna ilişkin Regülasyon'a (Europol Regülasyonu) dayanmaktadır[793]. Europol'ün amacı, Europol Regülasyonu'nun Ek-1'inde listelenen ve iki veya daha fazla Üye Devleti etkileyen organize suçların, terörün ve diğer ağır suçların önlenmesine ve soruşturulmasına destek olmaktır. Bu destek, bilgi paylaşımı yapılması ve AB'nin bilgi merkezi olarak hareket etmesi, istihbarat analizlerinin ve tehdit değerlendirmelerinin sağlanması ile gerçekleşmektedir.

Amaçlarına ulaşmak için Europol, ENU'lar aracılığı ile suça ilişkin istihbarat ve bilgi değişimi için Üye Devletlere veri tabanı sağlayan bir Europol Bilgi Sistemi kurmuştur. Europol Bilgi Sistemi, şüpheli olan kişiler, Europol'un yetki alanındaki bir suçtan dolayı hüküm giymiş kişiler veya bu tür suçları işleyeceklerine dair somu göstergeler olan kişilere ilişkin verilerin erişilebilir tutulması için kullanılabilmektedir. Europol ve ENU'lar doğrudan Europol Bilgi Sistemi'ne veri girebilir ve buradan veri çekebilir. Sisteme veriyi giren kişi ancak bu verileri değiştirilebilir, düzeltebilir veya silebilir. AB birimleri, üçüncü ülkeler ve uluslararası organizasyonlar da Europol'e bilgi sağlayabilmektedir.

Kişisel veri dahil, bilgiler, internet gibi kamuya açık kaynaklar ile Europol'den elde edilebilmektedir. Kişisel verilerin AB birimlerine aktarılmalarına ancak Europol'ün veya muhatap AB biriminin görevini yerine getirmesi için gerekli ise izin verilir. Kişisel verilerin üçüncü ülkelere veya uluslararası organizasyonlara aktarılması ise ancak Avrupa Komisyonun ilgili üçüncü ülkenin veya uluslararası organizasyonun yeterli düzeyde veri koruması sağladığına ilişkin kararı ile ("yeterlilik kararı") ve uluslararası veya iş birliği anlaşmasının olması halinde mümkündür. Ulusal hukukuna uygun olarak bu kişisel verilerin bir ENU tarafından, iş birliği anlaşması ile mevcut bir iş birliği olan üçüncü ülkedeki bir irtibat noktası veya uluslararası organizasyon tarafından veya yeterlilik kararına konu veya AB ile uluslararası anlaşmanın tarafı olan bir üçüncü ülkenin veya uluslararası organizasyon otoritesi tarafından iletilmesi halinde Europol, özel hukuk taraflarından ve kişilerinden katı şartlar altında kişisel veri alabilir ve işleyebilir. Tüm bilgi değişimleri Güvenli Bilgi Paylaşımı Ağı Uygulaması (SIENA) üzerinden gerçekleştirilir.

Yeni gelişmeler üzerine Europol içerisinde uzmanlaşmış merkezler kurulmuştur. Avrupa Siber Suçlar Merkezi 2013 yılında Europol içerisinde kurulmuştur[794]. Merkez, online suçların gerçekleşmesi hallerinde daha hızlı harekete geçilmesine katkıda bulunur, adli bilişim kapasitesini geliştirir ve etkin bir şekilde kullanır, siber suçlar soruşturmalarına ilişkin üstün uygulama sergiler ve siber suçlar üzerine AB bilgi merkezi olarak hizmet verir. Merkez aşağıdaki siber suçlara odaklanır:

- Online dolandırıcılık gibi yüksek suç geliri elde etmeye yönelik ve organize gruplarca işlenenler;
- Çocuğun internet aracılığı ile cinsel istismarı gibi mağdura ciddi zarar verenler;
- AB içerisinde kritik altyapı veya bilgi sistemlerini etkileyenler.

[793] Adli Kolluk İşbirliği için Avrupa Birliği Kurumuna ilişkin ve 2009/371/JHA, 2009/934/JHA, 2009/935/JHA, 2009/936/JHA and 2009/968/JHA sayılı Konsey Kararlarının yerine geçen ve kaldıran Avrupa Parlamentosu ve Konseyinin 11 Mayıs 2016 tarihli (EU) 2016/794 sayılı Regülasyonu, OJ 2916 L 135, sf.53.

[794] Ayrıca bkz. EDPS (2012), *Avrupa Siber Suçlar Merkezi'nin kurulmasına ilişkin Avrupa Komisyonu'ndan Konsey ve Avrupa Parlamentosu'na Bildirime ilişkin Veri Koruma Denetçisi'nin Görüşü*, Brüksel, 29 Haziran 2012.

Avrupa Terörle Mücadele Merkezi (ECTC), Ocak 2016 tarihinde Üye Devletlere terör suçlarına ilişkin soruşturmalarda operasyonel destek vermek üzere oluşturulmuştur. Merkez, canlı operasyonel veri ile Europol'un sahip olduğu verileri karşılaştırır, finansal ipuçlarını hızlıca ortaya çıkarır ve soruşturmaya ilişkin mevcut tüm detayları terör ağının yapılandırılmış resminin oluşturulmasına destek olunması için analiz eder[795].

Avrupa Göçmen Kaçakçılığı Merkezi (EMSC), 2015 Kasım tarihli bir Konsey toplantısını takiben, Üye Devletlere göçmen kaçakçılığına dahil olan suç ağlarının belirlenmesi ve dağıtılmasına destek olmak için Şubat 2016'da kurulmuştur. Merkez, Katanya (İtalya) ve Pire (Yunanistan)'da bulunan AB Bölgesel Çalışma Birimi bürolarını destekleyen ve yerel otoritelere istihbarat paylaşımı, suç soruşturmaları ve insan kaçakçılığı yapan ağların yargılanması gibi birçok alanda destek sağlayan bir bilgi merkezi olarak hareket etmektedir[796].

Europol'ün tabi olduğu veri koruma rejimi, geliştirilmiş bir rejimdir ve AB Kuruluşları Veri Koruma Regülasyonu[797] prensiplerinden yararlanmaktadır ve ayrıca haklar Polis ve Ceza Yargılaması Otoriteleri için Veri Koruma Direktifi, Modernize Edilmiş Sözleşme 108 ve Polis Önerisi ile tutarlıdır.

Suç fiillerinin mağdurlarına, tanıklarına veya suç fiiline ilişkin bilgi verebilecek diğer kişilere veya 18 yaşından küçüklere ilişkin kişisel verilerin işlenmesine, Europol'ün amaçları kapsamındaki suçların engellenmesi veya bunlarla mücadele edilmesi için kesinlikle gerekli ve orantılı olduğu sürece izin verilmektedir[798]. Hassas verilerin işlenmesi, Europol'ün amaçları kapsamındaki suçların engellenmesi veya bunlarla mücadele edilmesi için kesinlikle gerekli ve orantılı olması ve bu verilerin Europol tarafından işlenen diğer kişisel verileri destekliyor olması halleri dışında yasaktır[799]. Her iki halde de sadece Europol ilgili verilere erişebilir[800].

Verilerin saklanmasına ancak gerekli ve orantılı bir süre zarfı için izin verilir ve saklamanın devam etmesi, her üç yılda bir yapılacak değerlendirmeye tabidir, aksi takdirde veriler otomatik olarak silinecektir[801].

Birtakım şartlar altında Europol verileri bir AB organına veya üçüncü ülke otoritesine veya bir uluslararası organizasyona doğrudan aktarmaya yetkilidir[802]. Veri ihlalleri, veri sahiplerinin hak ve özgürlüklerini ciddi ve olumsuz bir şekilde etkileyecek ise, gecikmeksizin ilgili kişilere bildirilmelidir[803]. Üye Devletler nezdinde ise Europol'ün kişisel veri işlemesini takip edecek bir ulusal gözetim otoritesi görevlendirilecektir[804].

EDPS, Europol tarafından kişisel verilerin işlenmesine ilişkin olarak gerçek kişilerin temel hak ve özgürlüklerinin korunmasını gözetme ve sağlamakla, ve kişisel verilerin işlenmesine ilişkin tüm konularda Europol'e ve veri sahiplerine görüş vermekle sorumludur. Bu maksatla EDPS, bir soruşturma ve şikayet organı olarak hareket etmekte ve ulusal gözetim otoriteleri ile iş birliği

---

[795] Bkz. Europol'ün ECTC'ye ilişkin internet sitesi.
[796] Bkz. Europol'ün EMSC'ye ilişkin internet sitesi.
[797] Topluluğun kuruluşları ve organları tarafından kişisel verilerin işlenmesine ilişkin bireylerin korunması ve bu verilerin serbest dolaşımına ilişkin Avrupa Parlamentosu ve Konseyi'nin 18 Aralık 2000 tarihli ve (EC) 45/2001 sayılı Regülasyonu, OJ 2001 L 8.
[798] Europol Regülasyonu, Madde 30(1).
[799] *A.g.e.*, Madde 30(2).
[800] *A.g.e.*, Madde 30(3).
[801] *A.g.e.*, Madde 31.
[802] *A.g.e.*, sırasıyla Madde 24 ve Madde 25.
[803] *A.g.e.*, Madde 35.
[804] Europol Regülasyonu, Madde 42.

içinde faaliyet göstermektedir[805]. EDPS ve ulusal gözetim otoriteleri her yıl en az iki kere, tavsiye niteliğinde bir fonksiyonu olan İş Birliği Kurulu'nda toplanmaktadır[806]. Üye Devletler, kişisel verilerin Europol'e aktarılmasının, geri alınmasının ve kişisel verinin Europol ile olan tüm iletişiminin uygunluğunu gözetlemeye yetkili bir gözetim otoritesini kanun ile kurmakla yükümlüdür[807]. Üye Devletler ayrıca ulusal gözetim otoritesinin Europol Regülasyonu altında görevlerini yerine getirirken tamamen bağımsız hareket etmesini güvence altına almakla yükümlüdürler[808]. Veri işlemenin hukuka uygunluğunu teyit etmek, faaliyetlerini kendi kendine gözetim altında tutmak ve veri bütünlüğü ile güvenliğini sağlamak için Europol, veri işleme faaliyetlerinin log kayıtlarını veya belgelendirmelerini tutmaktadır. Bu loglar, toplama, değiştirme, danışma, ifşa, birleştirme ve silmeye ilişkin otomatik işleme sistemlerinde gerçekleşen işleme operasyonlarına dair bilgiler içermektedirler[809].

EDPS'nin bir kararına karşı itirazlar CJEU'nun önüne getirilebilir[810]. Hukuka aykırı veri işleme operasyonu sonucu zarara uğrayan herhangi bir kişi, CJEU veya yetkili ulusal mahkeme nezdinde dava açarak bu zararların, Europol veya sorumlu Üye Devlet tarafından karşılanması hakkına sahiptir[811]. Buna ek olarak, yerel parlamentoların uzmanlaşmış Ortak Parlamenter İnceleme Grubu (JPSG) ve Avrupa Parlamentosu, Europol'ün faaliyetlerini detaylı olarak inceleyebilir[812]. Her birey, kendisi hakkında Europol'ün elinde bulundurduğu kişisel verilerin kontrol edilmesi, düzeltilmesi veya silinmesini talep etme haklarına ek olarak bunlara erişim hakkına sahiptir. Bu durum istisnalara ve kısıtlamalara tabi olabilir.

Eurojust

2002'de kurulan Eurojust, merkezi Lahey'de bulunan bir AB organıdır. En az iki Üye Devleti ilgilendiren ağır suçlara ilişkin soruşturma ve kovuşturma alanlarında adli iş birliği sağlamaktadır[813]. Eurojust'ın yetkileri şu şekildedir;

- Birden çok Üye Devletlerin yetkili otoriteleri arasında soruşturma ve kovuşturma alanlarındaki iş birliğinin teşvik edilmesi ve geliştirilmesi;

- Adli iş birliğine ilişkin talep ve kararların icrasını kolaylaştırmak.

Eurojust'ın fonksiyonları ulusal üyelerce gerçekleştirilmektedir. Her bir Üye Devlet, Eurojust'a, statüsü yerel hukuka tabi olan ve adli iş birliğinin teşvik edilmesi ve geliştirilmesi için gerekli görevler için gerekli yetkilerle donatılmış bir hakim veya savcı atamaktadır. Ek olarak, ulusal üyeler özel Eurojust faaliyetlerini yerine getirmek için ortaklaşa ve elbirliği ile çalışmaktadır.

---

[805] *A.g.e.*, Madde 43 ve Madde 44.
[806] *A.g.e.*, Madde 45.
[807] *A.g.e.*, Madde 42 (1).
[808] *A.g.e.*, Madde 42 (1).
[809] *A.g.e.*, Madde 40.
[810] *A.g.e.*, Madde 48.
[811] *A.g.e.*, Madde 50.
[812] *A.g.e.*, Madde 51.
[813] Avrupa Birliği Konseyi (2002), Ağır suçlara ilişkin mücadelenin güçlendirilmesi amacıyla Eurojust'ı kuran 28 Şubat 2002 tarihli ve 2002/187/JHA sayılı Konsey Kararı, OJ 2002 L 63; Avrupa Birliği Konseyi (2003), Ağır suçlara ilişkin mücadelenin güçlendirilmesi amacıyla Eurojust'ı kuran 2002/187/JHA sayılı Konsey Kararı değiştiren 2003/659/JHA sayılı Konsey Kararı, OJ 2003 L 44; Avrupa Birliği Konseyi (2009), Eurojust'ın güçlendirilmesi ve Ağır suçlara ilişkin mücadelenin güçlendirilmesi amacıyla Eurojust'ı kuran 28 Şubat 2002 tarihli ve 2002/187/JHA sayılı Konsey Kararının değiştirilmesine ilişkin 16 Aralık 2008 tarihli ve 2009/426/JHA sayılı Konsey Kararı, OJ 2009 L 138 (Eurojust Kararları).

Eurojust, amaçlarına ulaşmak için gerekli olduğu ölçüde kişisel veri işleyebilir. Ancak bu işleme, Eurojust'ın yetki alanındaki bir suç fiilini işlediği veya işlenmesinde yer aldığına ilişkin şüpheli olan veya bunlardan hüküm giyen kişilere dair spesifik bilgiler ile sınırlıdır. Eurojust aynı zamanda Eurojust'ın yetkisine giren suç fiillerinin tanıkları veya mağdurlarına ilişkin birtakım bilgileri işleyebilir[814]. İstisnai hallerde Eurojust, kısıtlı bir zaman zarfı için, devam eden soruşturma için doğrudan ilgili olması şartıyla bir suçun detaylarına ilişkin daha geniş kapsamlı kişisel veri işleyebilir. Yetki alanı içerisinde Eurojust diğer AB kuruluşları, oranları ve kurumları ile iş birliği yapabilir ve bunlarla kişisel veri değişiminde bulunabilir. Eurojust ayrıca üçüncü ülkelerle ve organizasyonlarla kişisel veri değişimi yapabilir, bunlarla iş birliğinde bulunabilir.

Veri korumasına ilişkin olarak; Eurojust en az Modernize Edilmiş Sözleşme 108 ve bunu takip eden değişikliklerdeki prensiplere denk gelen bir koruma seviyesi garanti etmelidir. Veri değişimi hallerinde ise, Eurojust Konsey Kararları ve Eurojust Veri Koruma Kuralları[815]'na uygun olarak iş birliği sözleşmesine veya çalışma düzenlemelerinde düzenlenmiş spesifik kurallar ve kısıtlamalar dikkate alınmalıdır.

Eurojust bünyesinde, Eurojust'ın gerçekleştirdiği kişisel veri işleme faaliyetlerini gözlemleme ile görevli bağımsız bir Ortak Gözetim Organı (JSB) kurulmuştur. Kişiler, Eurojust'ın kişisel verilere erişim, bunları düzeltme, bloklama veya silme taleplerine ilişkin verdiği kararlar ile tatmin olmamaları halinde JSB'ye itirazda bulunabilecektir. Eurojust'ın kişisel verileri hukuka aykırı olarak işlemesi halinde Eurojust, merkezinin bulunduğu Üye Devletin, Hollanda'nın, iç hukuku uyarınca veri sahibinin uğrayacağı tüm zararlardan sorumlu olacaktır.

Genel Bakış

Avrupa Komisyonu Temmuz 2013 tarihinde Eurojust'ı yeniden düzenlenmesine ilişkin bir regülasyon teklifi sunmuştur. Bu teklife, Avrupa Savcılığı Ofisi'nin (aşağıya bakınız) kurulmasına ilişkin teklif eşlik etmiştir. Bu regülasyon ile fonksiyonların ve yapının Lizbon Anlaşması ile uyumlu olacak şekilde düzenlenmesi amaçlanmaktadır. Bunun ötesinde reformun amacı, Eurojust'ın Eurojust Heyeti tarafından yerine getirilen operasyonel görevleri ile idari görevleri arasında net bir ayrım yapmaktır. Bu, aynı zamanda Üye Devletlerin operasyonel görevler üzerinde odaklanmalarını sağlayacaktır. İdari görevlerin yerine getirilmesinde heyete destek olacak yeni bir Yönetim Kurulu kurulacaktır[816].

Avrupa Savcılığı Ofisi

Üye Devletler, AB bütçesinin uygunsuz kullanımı ve dolandırıcılık suçlarını, potansiyel sınır ötesi etkisi de olarak, kovuşturma yetkisine münhasıran sahiptirler. Bu tür suçların faillerinin soruşturulması, yargılanması ve adalete teslim edilmesinin önemi, özellikle devam eden ekonomik kriz düşünüldüğünde, gittikçe artmıştır[817]. Avrupa Komisyonu, AB'nin finansal çıkarlarına zarar veren suç fiilleri ile mücadele amacıyla bağımsız bir Avrupa Savcılık Bürosu'nun (EPPO) kurulmasını teklif etmiştir[818]. EPPO, en az dokuz Üye Devletinin, diğer

[814] 2003/659/JHA sayılı Konsey Kararı ve 2009/426/JHA sayılı Konsey Kararı ile değiştirilmiş 2002/187/JHA sayılı Konsey Kararının konsolide versiyonu, Madde 15(2).
[815] Eurojust'ta Kişisel Verilerin İşlenmesi ve Korunmasına ilişkin Usul Kuralları, OJ 2005 C 68/01, 19 Mart 2005, sf. 1.
[816] Bkz. Avrupa Komisyonu'nun Eurojust internet sitesi.
[817] Bkz. Avrupoa Komisyonu (2013), Avrupa Savcılık Bürosu'nun kurulması için Konsey Regülasyonu için Teklif, COM(2013) 534 final, Brüksel, 17 Temmuz 2013, sf. 1 ve Komisyon'un EPPO internet sitesi.
[818] Avrupa Komisyonu (2013), Avrupa Savcılık Bürosu'nun kurulması için Konsey Regülasyonu için Teklif,

AB ülkeleri dahil olmaksızın AB yapıları içerisinde ileri seviye iş birliği sağlamasına izin verecek artırılmış iş birliği prosedürü ile oluşturulacaktır[819]. Belçika, Bulgaristan, Hırvatistan, Kıbrıs, Çek Cumhuriyeti, Estonya, Finlandiya, Fransa, Almanya, Yunanistan, Letonya, Litvanya, Lüksemburg, Portekiz, Romanya, Slovenya, Slovakya ve İspanya, iş birliğini artırmaya yönelik birleşmişler, Avusturya ve İtalya ise katılımlarına ilişkin niyetlerini ifade etmişlerdir[820].

EPPO, farklı iç hukuk düzenlemeleri arasında soruşturmaların ve kovuşturmaların etkili bir şekilde koordine edilmesi, kaynakların kullanımının ve Avrupa seviyesinde bilgi değişiminin iyileştirilmesi amaçları ile AB'nin finansal çıkarlarını etkileyen AB dolandırıcılık ve diğer suçların soruşturulması ve kovuşturulmasında yetkili olacaktır[821].

EPPO, her bir Üye Devlette bulunan en az bir tane o Üye Devletteki soruşturma ve kovuşturmaları yürütmekle görevli delege edilmiş Avrupa Savcısı ile Avrupa Savcılığı'nın altında olacaktır.

Teklif, EPPO'nun soruşturmalarına dahil olan kişilerin haklarını iç hukuk, AB hukuku ve AB Temel Haklar Bildirgesi'nde belirtildiği üzere güvence altına almak üzere güçlü güvenlikler ortaya koymaktadır. Çoğunlukla temel haklara dokunan soruşturma tedbirleri yerel mahkemenin ön iznine ihtiyaç duyacaktır[822]. EPPO'nun soruşturmaları yerel mahkemelerin yargısal denetimine tabi olacaktır[823].

AB Kuruluşları Veri Koruma Regülasyonu[824], EPPO tarafından gerçekleştirilen idari kişisel verilerin işlenmesine uygulanacaktır. EPPO'nun fonksiyonları dahilinde Üye Devletler seviyesinde kolluk ve yargı otoriteleri ile kişisel veri işleme faaliyetlerini içereceği düşünülürse, operasyonel konulara ilişkin kişisel verilerin işlenmesi için, Europol'de olduğu gibi, Europol ve Eurojust'ın faaliyetlerini düzenleyenlere benzer şekilde EPPO'nun kendisine ait ayrı bir veri koruma rejimi olacaktır. EPPO veri koruma kuralları bu nedenle Polis ve Ceza Yargılaması Otoriteleri için Veri Koruma Direktifi kuralları ile neredeyse aynıdır. EPPO'nun kurulmasına ilişkin Teklif uyarınca, kişisel verilerin işlenmesi; hukuka uygunluk ve dürüstlük, amaçla sınırlılık, veri minimizasyonu, doğruluk, bütünlük ve gizlilik kurallarına uygun olması gerekmektedir. EPPO, suç fiillerinden hüküm giymiş veya sadece şüpheli, tanık veya mağdur olan kişiler gibi farklı kişisel veri sahiplerinin kişisel verileri arasında mümkün olduğu kadar net bir ayrım yapmalıdır. Ayrıca kişisel verinin niteliğini doğrulamayı ve mümkün olduğunca vakaya dayalı kişisel veri ile kişisel değerlendirmeye dayalı kişisel veriler arasında ayrım yapmayı hedeflemelidir.

Teklif, özellikle bilgi alma hakkı, kişisel veriye erişme hakkı, düzeltme, silme ve işlemenin kısıtlanmasını talep hakları olmak üzere veri sahiplerinin haklarına ilişkin düzenlemeler içermektedir ve bu hakların dolaylı olarak EDPS üzerinden kullanılabileceği düzenlenmiştir.

COM(2013) 534 final, Brüksel, 17 Temmuz 2013.

[819] AB'nin İşleyişi Hakkında Anlaşma, Madde 86 (1) ve Madde 329 (1).

[820] Bkz. Avrupa Birliği Konseyi (2017), "*20 üye ülke Avrupa Savcılık Bürosu'nun (EPPO) kurulmasına ilişkin detaylar üzerinde anlaştı*", basın açıklaması, 8 Haziran 2017.

[821] Avrupa Komisyonu (2013), Avrupa Savcılık Bürosu'nun kurulması için Konsey Regülasyonu için Teklif, COM(2013) 534 final, Brüksel, 17 Temmuz 2013, sf. 1 ve 51-51. Ayrıca bkz. Komisyon'un EPPO internet sitesi.

[822] Avrupa Komisyonu (2013), Avrupa Savcılık Bürosu'nun kurulması için Konsey Regülasyonu için Teklif, COM(2013) 534 final, Brüksel, 17 Temmuz 2013, Madde 26(4).

[823] *A.g.e.*, Madde 36.

[824] Topluluğun kuruluşları ve organları tarafından kişisel verilerin işlenmesine ilişkin bireylerin korunması ve bu verilerin serbest dolaşımına ilişkin Avrupa Parlamentosu ve Konseyi'nin 18 Aralık 2000 tarihli ve (EC) 45/2001 sayılı Regülasyonu, OJ 2001 L 8.

Ayrıca, EPPO'nun işlemenin teşkil ettiği riske uygun bir güvenlik seviyesi sağlamak için uygun teknik ve idari tedbirler almasını, tüm işleme faaliyetlerinin kayıtlarını tutmasını ve işleme türünün muhtemelen bireylerin haklarına karşı yüksek risk teşkil edeceği hallerde (örneğin yeni teknolojilerin kullanıldığı işleme faaliyetleri) işlemeden önce veri koruma etki değerlendirmesi yapmasını gerektiren işlenmenin güvenliği ve hesap verilebilirlik prensiplerini bünyesinde barındırmaktadır. Son olarak teklif, kişisel verilerin korunmasına ilişkin tüm konulara gereğince dahil olacak ve EPPO'nun uygulanacak veri koruma mevzuatına uygunluğunu temin edecek bir Veri Koruma Görevlisinin heyet tarafından belirlenmesini düzenlemektedir.

8.3.2. AB -seviyesinde ortak bilgi sistemlerinde veri koruması

Üye Devletler arasında veri değişimine ve sınırlar arası suçlarla savaşmak için Europol, Eurojust ve EPPO gibi uzmanlaşmış AB otoritelerinin oluşturulmasına ek olarak, yetkili ulusal ve AB otoriteleri arasında sınır güvenliği, göç, sığınma ve gümrük alanlarındaki spesifik amaçlar için iş birliği ve veri değişiminin sağlanması ve kolaylaştırılması için AB seviyesinde ortak bilgi sistemleri oluşturulmuştur. Schengen alanının ilk oluşturulması AB hukukundan bağımsız olarak uygulanan uluslararası bir anlaşma ile gerçekleştiği gibi Schengen Bilgi Sistemi (SIS) çok taraflı bir sözleşme sonucunda oluşturulmuştur ve bunu takiben AB hukuku kapsamına sokulmuştur. Visa Bilgi Sistemi (VIS), Eurodac, Eurosur ve Gümrük Bilgi Sistemi (CIS), AB hukukuna tabi araçlar olarak oluşturulmuştur.

Bu sistemlerin gözetimi ulusal gözetim otoriteleri ile EDPS arasında paylaşılmaktadır. İleri seviye bir koruma sağlanması için bu otoriteler, Eurodac, Visa Bilgi Sistemi, Schengen Bilgi Sistemi, Gümrük Bilgi Sistemi ve İç Pazar Bilgi Sistemi olmak üzere büyük ölçekli BT sistemlerine karşılık gelen Gözetim Koordinasyon Grupları (SCG'ler) ile beraber çalışmaktadırlar[825]. SCG'ler, seçilmiş bir Başkan'ın otoritesi altında genelde yılda iki kere toplanır ve Rehberler çıkarırlar, sınır ötesi olayları tartışırlar veya soruşturmalar için ortak çerçeveler belirlerler.

2012'de kurulan Büyük Ölçekli Bilgi Teknolojileri Sistemleri için Avrupa Bürosu (eu-LISA)[826], ikinci jenerasyon Schengen Bilgi Sistemi (SIS II), Visa Bilgi Sistemi (VIS) ve Eurodac'ın operasyon yönetiminden sorumludur. Eu-LISA'nın ana görevi, bilgi teknolojileri sistemlerinin etkin, güvenli ve sürekli operasyonunu güvence altına almaktır. Ayrıca sistemlerin ve verilerin güvenliğini sağlamak için gerekli önlemlerin alınması için sorumludur**.**

Schengen Bilgi Sistemi

Eski Avrupa Topluluğu'nun birkaç Üye Devleti, 1985 yılında, kişilerin Schengen bölgesi içerisinde sınır kontrolü engeline takılmadan serbest dolaşımını sağlamayı amaçlayan Benelüks Ekonomik Birliği, Almanya ve Fransa arasında ortak sınırlarındaki kontrollerin kademeli olarak kaldırılmasına ilişkin bir sözleşme (Schengen Anlaşması) imzalamışlardır[827]. Açık sınırların doğurabileceği kamu güvenliği tehditlerinin dengelenmesi adına, yerel polis ve adli otoritelerin arasındaki yakın iş birliğinin yanında Schengen bölgesinin dış sınırlarındaki sınır kontrolleri güçlendirilmiştir.

Schengen Anlaşması'na ek ülkelerin katılmasının bir sonucu olarak Schengen sistemi nihayet

[825] Bkz. Avrupa Veri Koruma Denetçisi'nin Gözetim Koordinasyonu internet sitesi.
[826] Özgürlük, güvenlik ve adalet alanlarında büyük ölçekli bilgi teknolojileri sistemleri için bir Avrupa Bürosu kuran Avrupa Parlamentosu ve Konseyi'nin 25 Ekim 2011 tarihli ve (EU)1077/2011 sayılı Regülasyonu
[827] Benelüks Ekonomik Birliği, Almanya Federal Cumhuriyeti ve Fransız Cumhuriyeti Devletleri arasında ortak sınırlarındaki kontrollerin kademeli olarak kaldırılmasına ilişkin Anlaşma, OJ 2000 L 239.

Amsterdam Anlaşması[828] ile AB hukuku çerçevesine dahil edilmiştir. Bu kararın yürürlüğe girmesi 1999 yılında gerçekleşmiştir. SIS II olarak anılan Schengen Bilgi Sistemi'nin en yeni versiyonu, 9 Nisan 2013 tarihinde uygulamaya girmiştir. Şu anda çok AB Üye Devletine[829] ek olarak İzlanda, Lihtenştayn, Norveç ve İsviçre'ye hizmet vermektedir[830]. Europol ve Eurojust'ın da SIS II'ye erişimi vardır.

SIS II, merkezi sistem (C-SIS), her bir Üye Devletteki ulusal sistem (N-SIS) ve merkezi sistem ile ulusal sistemler arasında bir iletişim altyapısından oluşmaktadır. C-SIS, kişiler ve eşyalara ilişkin Üye Devletler tarafından girilen birtakım verilerden oluşmaktadır. SIS, Schengen Bölgesinde bulunan yerel sınır kontrolü, polis, gümrük, vize ve adli otoriteler tarafından kullanılmaktadır. Her bir Üye Devlet, düzenli olarak güncellenen ve dolayısıyla C-SIS'i güncelleyen ve Ulusal Schengen Bilgi Sistemi (N-SIS) olarak bilinen C-SIS'in yerel bir kopyasını işletmektedir. SIS'de farklı tür uyarılar mevcuttur:

- Kişinin Schengen bölgesine girmeye veya kalmaya hakkı yoktur; veya
- Kişi veya mal, adli veya kolluk otoritelerince aranmaktadır (örn. Avrupa Yakalama Emirleri, gizli kontrol talepleri); veya
- Kişi kayıp olarak bildirilmiştir; veya
- Banknot, araba, kamyonet, ateşli silah ve kimlik belgesi gibi eşyalar çalıntı veya kayıp olarak bildirilmiştir.

Bir uyarı olduğu zaman bunu takip eden işlemler SIRENE bürosu aracılığı ile başlatılmaktadır. SIS II'nin, parmak izi ve fotoğraf gibi biyometrik veri; çalıntı deniz ve hava aracı, konteynır veya ödeme aracı gibi yeni uyarı kategorileri; kişiler ve eşyalara ilişkin daha detaylı uyarılar ve tutuklama, teslim etme veya sınır dışı etme için aranan kişilere ilişkin Avrupa Yakalama Emirlerin (EAW'ler) kopyalarını girme imkanı gibi yeni fonksiyonları vardır.

SIS II, birbirlerini tamamlayan iki hukuki işleme dayanmaktadır: SIS II Kararı[831] ve SIS II Regülasyonu[832]. AB kanun koyucusu, kararın ve regülasyonun kabul edilmesi için farklı hukuki temeller kullanmıştır. SIS II'nin suça ilişkin konularda polis ve adli iş birliği (AB'nin eski üçüncü ayağı) kapsamındaki amaçları için kullanımı karara tabidir. Regülasyon ise vize, sığınma, göç ve kişilerin serbest dolaşımına (eski birinci ayak) ilişkin diğer politikalar kapsamına giren uyarı prosedürlerine uygulanmaktadır. Bu iki hukuki işlemin Lizbon Anlaşmasından ve ayaklar yapısının kaldırılmasın önce kabul edildiği düşünülürse her bir ayak için mevcut uyarı prosedürünün bağımsız işlemler ile düzenlenmesi gerekmekteydi.

---

[828] Avrupa Toplulukları (1997), Avrupa Birliği Anlaşması, Avrupa Toplulukları'nı kuran Sözleşmeler ve birtakım ilgili düzenlemeleri değiştiren Amsterdam Anlaşması, OJ 1997 C 340.

[829] Hırvatistan, Kıbrıs ve İrlanda SIS II'ye entegre olmak için hazırlık faaliyetlerini yürütmekle birlikte henüz bunun bir parçası değildir. Bkz. Avrupa Komisyonu Göç ve İçişleri Genel Müdürlüğü'nün internet sitesinde mevcut olan Schengen Bilgi Sistemi'ne ilişkin olan bilgiler.

[830] İkinci jenerasyon Schengen Bilgi Sistemi'nin kurulması, işletilmesi ve kullanımına ilişkin Avrupa Parlamentosu ve Konseyi'nin 20 Aralık 2006 tarihli ve (EC) 1987/2006 sayılı Regülasyonu, OJ 2006 L 381 (SIS II) ve Avrupa Birliği Konseyi (2007), İkinci jenerasyon Schengen Bilgi Sistemi'nin (SIS II) kurulması, işletilmesi ve kullanımına ilişkin 12 Haziran 2007 tarihli ve 2007/533/JHA sayılı Konsey Kararı, OJ 2007 L 205.

[831] İkinci jenerasyon Schengen Bilgi Sistemi'nin kurulması, işletilmesi ve kullanımına ilişkin 12 Haziran 2007 tarihli ve 2007/533/JHA sayılı Konsey Kararı, (SIS II), OJ 2007 L 205, 7 Ağustos 2007.

[832] İkinci jenerasyon Schengen Bilgi Sistemi'nin (SIS II) kurulması, işletilmesi ve kullanımına ilişkin Avrupa Parlamentosu ve Konseyi'nin 20 Aralık 2006 tarihli ve (EC) 1987/2006 sayılı Regülasyonu, OJ 2006 L 381, 28 Aralık 2006.

Hukuki işlemlerin ikisi de veri korumasına ilişkin kurallar içermektedir. SIS II Kararı, hassas verinin işlenmesini yasaklamaktadır[833]. Kişisel verilerin işlenmesi, Modernize Edilmiş Sözleşme 108 kapsamında düzenlenmektedir[834]. Bunun yanında kişiler SIS II'ye girilmiş ve kendileri hakkındaki kişisel verilere erişim hakkı vardır[835].

SIS II Regülasyonu, AB vatandaşı olmayan kişilerin girişinin veya kalmasının reddedilmesine ilişkin uyarıların girilmesi ve işlenmesi için şartları ve usulleri düzenlemektedir. Ayrıca Üye Devlete girilmesi veya burada kalınması için tamamlayıcı ve ek bilgilerin değiştirilmesine ilişkin kurallar getirmektedir[836]. Bu regülasyon aynı zamanda veri korumaya ilişkin kurallar içermektedir. Genel Veri Koruma Regülasyonu'nun Madde 9(1)'de tanımlanan hassas veri kategorilerinin işlenmesine izin verilmemektedir[837]. SIS II Regülasyonu veri sahipleri için de birtakım haklar içermektedir:

- Veri sahibine ilişkin kişisel veriye erişim hakkı[838];
- Doğruyu yansıtmayan verilerin düzeltilmesi hakkı[839];
- Hukuka aykırı olarak saklanan verinin silinmesi hakkı[840]; ve
- Veri sahibi aleyhine bir uyarının söz konusu olması halinde bilgilendirilme hakkı. Bilgilendirme yazılı olacaktır ve uyarıyı çıkaran yerel kararın kopyası veya buna yapılan bir atfı içerecektir[841].

Şu hallerde bilgilendirilme hakkının kullanılması mümkün değildir; 1) kişisel verinin veri sahibinden elde edilmediği ve bilgi verilmesinin imkansız veya orantısız bir çaba gerektireceği haller, 2) veri sahibinin zaten bilgiye sahip olduğu haller veya 3) yerel hukukun, diğer hususların yanında, ulusal güvenliğin korunması veya suç fiillerinin önlenmesi temelinde sınırlamaya imkan verdiği haller[842].

Hem SIS II Kararı hem SIS II Regülasyonu nezdinde bireylerin SIS II'ye ilişkin erişim hakları herhangi bir Üye Devlette kullanılabilir ve o Üye Devletin iç hukukuna uygun olarak sürdürülür[843].

Örnek: Dalea/Fransa Kararında[844], başvuru sahibi, Fransız otoritelerinin Schengen Bilgi Sistemi'ne bu kişinin girişinin reddedilmesine ilişkin bildirimde bulunması sebebiyle Fransa'yı ziyaret etmek için gerekli vizeyi alamamıştır. Başvuru sahibi, Fransız Veri Koruma Komisyonu ve nihayet Danıştay nezdinde bu verilere erişim, düzeltme veya silme talebinde bulunmuştur ancak başarısızlıkla sonuçlanmıştır. AİHM, başvuru sahibinin Schengen Bilgi Sistemi'ne raporlanmasını hukuka uygun bulmuş ve ulusal güvenliğin korunması meşru amacını kabul etmiştir. Başvuru sahibinin Schengen alanına girmesinin reddedilmesinin

[833] SIS II Kararı, Madde 56; SIS II Regülasyonu Madde 40.
[834] SIS II Kararı, Madde 57.
[835] SIS II Kararı, Madde 58; SIS II Regülasyonu Madde 41.
[836] SIS II Regülasyonu, Madde 2.
[837] *A.g.e.*, Madde 40.
[838] *A.g.e.*, Madde 41(1).
[839] *A.g.e.*, Madde 41(5).
[840] *A.g.e.*, Madde 41(5).
[841] *A.g.e.*, Madde 42(1).
[842] *A.g.e.*, Madde 42(2).
[843] SIS II Regülasyonu, Madde 41(1) ve SIS II Kararı Madde 58.
[844] AİHM, Dalea/Fransa, No.964/97, 2 Şubat 2010.

sonucunda nasıl zarara uğradığını göstermemesi ve keyfi kararlara karşı kendisini koruyacak yeterli mekanizmaların varlığı dikkate alınırsa özel hayata saygı hakkına yapılan müdahale orantılıdır. Bu nedenle başvuru sahibinin Madde 8 kapsamında yaptığı şikayet kabul edilemez addedilmiştir.

Her bir Üye Devletteki yetkili yerel gözetim otoriteleri yerel N-SIS'i gözetim altında tutmaktadır. Yerel gözetim otoritesi, yerel N-SIS kapsamındaki veri işleme operasyonlarının denetiminin en az dört yılda bir yapılmasını sağlamalıdır[845]. EDPS C-SIS'in denetiminden sorumlu iken yerel gözetim otoriteleri ile EDPS iş birliğinde bulunmakta ve N-SIS'in koordine bir şekilde denetlenmesini sağlamaktadırlar. Şeffaflığın sağlanması adına her iki yılda bir faaliyetlerin ortak raporu Avrupa Parlamentosu'na, Konsey'e ve eu-LISA'ya gönderilecektir. SIS II'nin Gözetim Koordinasyon Grubu (SCG), SIS'in gözetim koordinasyonu sağlamak üzere kurulmuştur ve yılda iki kere toplanmaktadır. Bu grup; EDPS, Schengen üyeleri oldukları düşünüldüğünde SIS kullanımı nedeniyle İzlanda, Lihtenştayn, Norveç ve İsviçre yanında SIS II'yi kullanan Üye Devletlerin gözetim otoritelerinin temsilcilerinden oluşmaktadır[846]. Kıbrıs, Hırvatistan ve İrlanda henüz SIS II'nin bir parçası olmadıkları için SCG'ye sadece gözlemci olarak katılmaktadırlar. SCG kapsamında EDPS ve yerel gözetim otoriteleri, bilgi değişiminde bulunarak, denetim ve teftişlerin yürütülmesinde birbirlerine destek sağlayarak, potansiyel problemlere ortak çözümler için uyumlu teklifler tasarlayarak ve veri koruma haklarına ilişki farkındalığı artırarak aktif olarak iş birliği içerisinde bulunmaktadır[847]. SIS II SCG aynı zamanda veri sahiplerine yardımcı rehberler hazırlamaktadır. Bunlardan birine örnek, veri sahiplerine erişim haklarını kullanmalarına ilişkin rehberdir[848].

Genel Bakış

2016'da Avrupa Komisyonu, veri sahiplerinin kişisel verilerine SIS'de ulaşmaları, düzeltmeleri, silmeleri veya yanlış veriye ilişkin tazminat elde etmelerini sağlayan ulusal mekanizmaların kurulduğunu gösteren SIS'e ilişkin değerlendirme[849] yapmıştır. SIS II'nin verimliliğini ve etkililiğini artırmak için Avrupa Komisyonu regülasyon için üç teklifte bulunmuştur;

- Sınır kontrolleri alanında SIS'in kurulması, işletilmesi ve kullanımına ilişkin SIS II Regülasyonu'nu kaldıran bir düzenleme;

- Cezai konularda emniyet iş birliği ve adli iş birlik alanlarında SIS'in kurulması, işletilmesi ve kullanılmasına ilişkin ve diğerlerinin yanında SIS II Kararı'nı kaldıran bir düzenleme;

- Yasa dışı bir şekilde orada bulunan üçüncü ülke vatandaşlarının iadesi için SIS'in kullanımına ilişkin düzenleme.

---

[845] SIS II Regülasyonu, Madde 60(2).
[846] Bkz. Avrupa Veri Koruma Denetçisi'nin Schengen Bilgi Sistemi'ne ilişkin internet sitesi.
[847] SIS II Regülasyonu, Madde 46 ve SIS II Kararı Madde 62.
[848] Bkz. SIS II SCG, Schengen Bilgi Sistemi. Erişim Hakkının Kullanılmasına İlişkin Rehber, EDPS'nin internet sitesinden ulaşılabilir.
[849] Avrupa Komisyonu (2016), (EX) 1987/2006 sayılı Regülasyon'un 24(5), 43(3) ve 50(5) maddeleri ile 2007/533/JHA sayılı Karar'ın 59(3) ve 66(5) maddelerine göre ikinci Schengen Bilgi Sistemi (SIS II) değerlendirmesine ilişkin Komisyon'dan Avrupa Parlamentosu ve Konseyi'ne rapor, COM(2016) 880 final, Brüksel, 21 Aralık 2016.

Önemli bir nokta, teklifin, mevcut SIS II rejiminin parçası olan parmak izi ve fotoğrafa ek olarak diğer biyometrik veri kategorilerinin işlenmesine izin vermesidir. Yüz izleri, avuç içi izleri ve DNA profilleri de SIS veri tabanında tutulacaktır. Buna ek olarak, SIS II Regülasyonu ve SIS II kararı bir kişinin tespitinde parmak izi ile arama yapmayı düzenlemekteyken, teklif, başka bir şekilde kişinin kimliğinin tespit edilmesi mümkün değilse bu aramayı zorunlu tutmaktadır. Yüz resimleri, fotoğrafları ve avuç içi izleri, teknik olarak mümkün olduğunda sistemin aratılması ve kişinin tespitinde kullanılacaktır. Biyometrik özelliklere ilişkin yeni kurallar kişilerin haklarına karşı özel bir risk teşkil etmektedir. Komisyon tekliflerindeki görüşünde[850] EDPS, biyometrik verilerin oldukça hassas olduğu ve bunların bu denli büyük ölçekli veri tabanına dahil edilmelerine yönelik ihtiyacın somut delillere dayalı olmasının gerekli olduğunu belirtmiştir. Başka bir deyişle, yeni özelliklerin işlenmesindeki gereklilik gösterilmelidir. EDPS ayrıca DNA profiline hangi tür bilgilerin dahil edilebileceğinin daha çok detaylandırılması gerektiğini belirtmiştir. DNA profili hassas bilgiler içerebileceğinden (en önemli örneği sağlık problemleri ifşa eden bilgiler olacaktır), SIS'de bulundurulacak DNA profilleri "sadece kayıp kişilerin tespit edilmesi için kesinlikle gerekli olan minimum bilgiyi içermeli ve sağlık bilgisi, ırka ilişkin köken ve diğer tüm hassas bilgileri içermemelidir"[851]. Ancak teklif kesinlikle gerekli ve operasyonel anlamda gerekli olan verilerin toplanmasını ve öte işlenmelerini kısıtlayacak ek güvenceler getirmektedir ve erişim, kişisel veriyi işlemekte operasyonel gerekliliği olan kişilerle sınır olacaktır[852]. Teklif aynı zamanda, verinin niteliğini güvence alan uyarıların düzenli olarak gözden geçirilmesi için eu-LISA'yı Üye Devletler için düzenli aralıklarla veri niteliği raporları çıkarmakla yetkilendirmektedir[853].

Vize Bilgi Sistemi

Eu-LISA tarafından işletilen Vize Bilgi Sistemi (VIS), ortak AB vize politikasının oluşturulmasını desteklemek amacıyla kurulmuştur[854]. VIS, Schengen ülkelerinin, AB ülkeleri içerisinde olmayan Schengen ülkelerinin konsolosluk ve elçilikleri ile tüm Schengen ülkelerinin dış sınır değişimi noktalarını bağlayan tamamen merkezileşmiş bir sistem üzerinden vize başvurularını ilgilendiren verileri değişmelerine izin verir. VIS, Schengen bölgesinin ziyaretine veya bölgeden transit geçişe ilişkin kısa dönem vize başvurularına ilişkin verileri işler. VIS, sınır otoritelerinin, özellikle parmak izi olmak üzere biyometrik özelliklerin yardımı ile vizesini sunan kişinin bu vizenin haklı sahibi olup olmadığını tespit etmelerini ve belgesi olmayan veya sahte belgesi olan kişilerin kimliklerini tespit etmelerini sağlar.

Vize Bilgi Sistemi (VIS) ve kısa dönemli vizelerde Üye Devletler arasında veri paylaşımına ilişkin Avrupa Parlamentosu ve Konseyi'nin (EC)767/2008 numaralı Regülasyonu (VIS Regülasyonu), kısa dönemli vize başvurularına ilişkin kişisel verilerin aktarılması için şartları

[850] EDPS (2017), Schengen Bilgi Sistemi'nin yeni hukuki zeminine ilişkin EDPS Görüşü, Görüş 7/2017, 2 Mayıs 2017.
[851] *A.g.e.*, para.22.
[852] Avrupa Komisyonu (2016), Cezai konularda emniyet iş birliği ve adli iş birlik alanlarında SIS'in kurulması, işletilmesi ve kullanılmasına ilişkin, (EU)515/2014 sayılı Regülasyonu değiştiren ve (EC)1986/2006 sayılı Regülasyon, 2007/533/JHA sayılı Konsey Kararı ve 2010/261/EU sayılı Konsey Kararını kaldıran Avrupa Parlamentosu ve Konseyi'nin Regülasyon Teklifi, COM(2016) 883 final, Brüksel, 21 Aralık 2016.
[853] *A.g.e.*, sf.15.
[854] Avrupa Birliği Konseyi (2004), Vize Bilgi Sistemi'ni (VIS) kuran 8 Haziran 2004 tarihli ve 2004/512/EC sayılı Konsey Kararı, OJ 2004 L 213; Vize Bilgi Sistemi (VIS) ve kısa dönemli vizelerde Üye Devletler arasında veri paylaşımına ilişkin Avrupa Parlamentosu ve Konseyi'nin 9 Temmuz 2008 tarihli ve (EC)767/2008 numaralı Regülasyonu, OJ 2008 L 218 (VIS Regülasyonu); Avrupa Birliği Konseyi (2008), terör suçlarının ve diğer ağır suç fiillerinin önlenmesi, tespit edilmesi ve soruşturulması amaçları için Europol ve Üye Devletlerin belirlenen otoriteleri tarafından Vize Bilgi Sistemi'ne (VIS) başvurulması için erişime ilişkin 23 Haziran 2008 tarihli ve 2008/633/JHA sayılı Konsey Kararı, OJ 2008 L 218.

ve usulleri düzenler. Ayrıca vizenin iptal edilmesi, geri alınması veya uzatılması kararları dahil olmak üzere başvurulara dair verilen kararları düzenlemektedir[855]. VIS Regülasyonu temel olarak başvuru sahibi, vizesi, fotoğrafları, parmak izleri, önceki başvurularla bağlantılar ve kendisine eşlik eden kişilerin başvuru dosyalarına ilişkin verileri veya kişilerin davet edilmesine ilişkin verileri kapsamaktadır[856]. Verilere danışılması için erişim yetkisi vize otoritelerine ve dış sınır geçiş noktaları, göç kontrolleri ve sığınma kontrolleri için yetkili otoritelere sağlanmışken VIS'e veri girilmesi, değiştirilmesi veya silinmesi amacıyla erişim sadece vize otoritelerine olacak şekilde sınırlandırılmıştır.

Bazı şartlar altında yetkili ulusal polis otoriteleri ve Europol, terör ve suç fiillerinin önlenmesi, tespit edilmesi ve bunlarla savaşılması amacıyla VIS'e girilen veriye erişim talebinde bulunabilmektedir[857]. VIS'in ortak vize politikasının oluşturulmasına destek olmak üzere tasarlanan bir araç olduğu düşünülürse, 3.2.Bölüm'de açıklandığı üzere kişisel verilerin sadece spesifik, belirli ve meşru amaçlar için işlenmesini ve işlemenin verinin işlenmesine ilişkin amaçlara bağlı olarak, uygun ve ilgili olması ve aşırı olmamasını gerektiren sınırlılık ilkesi, VIS'in bir kolluk aracına dönüşmesi halinde ihlal edilmiş olacaktır. Bu nedenle yerel kolluk otoriteleri ve Europol'ün VIS veri tabanına düzenli erişimi sağlanmamıştır. Erişime ancak olay bazında ve sıkı güvenlikler ile izin verilebilir. Bu otoriteler tarafından VIS'e erişim ve danışmanın şartları ve güvenlik tedbirleri 2008/633/JHA sayılı Konsey Kararı ile düzenlenmektedir[858].

Bunların yanında VIS Regülasyonu veri sahiplerinin haklarını düzenlemektedir. Bu haklar şu şekildedir:

- Sorumlu Üye Devlet tarafından, Üye Devlet içerisinde kişisel verileri işlemeye yetkili veri sorumlusunun kimliği ve iletişim bilgileri, VIS bünyesinde kişisel verilerin hangi amaçlarla işleneceği, verilerin hangi kişi kategorilerine aktarılacağı (alıcılar) ve veri saklama süresi hakkında bilgilendirilme hakkı. Bunlara ek olarak vize başvurusu yapan kişilerin, kişisel verilerinin başvurularının incelenmesi için VIS tarafından toplanmasının zorunlu olduğu konusunda bilgilendirilmeleri gerekmektedir. Üye Devletler aynı zamanda bu kişileri, verilerine erişim, düzeltme veya silme haklarının varlığı ve bu hakları kullanmalarına imkan veren prosedürler hakkında bilgilendirmelidir[859].

- VIS bünyesinde kaydedilen kendilerine ilişkin kişisel verilere erişim hakkı[860].

- Yanlış verilerin düzeltilmesi hakkı[861].

- Hukuka aykırı saklanan verilerin silinmesi hakkı[862].

---

[855] VIS Regülasyonu, Madde 1.
[856] Vize Bilgi Sistemi (VIS) ve kısa dönemli vizelerde Üye Devletler arasında veri paylaşımına ilişkin Avrupa Parlamentosu ve Konseyi'nin 9 Temmuz 2008 tarihli ve (EC)767/2008 numaralı Regülasyonu, OJ 2008 L 218 (VIS Regülasyonu) Madde 5.
[857] Avrupa Birliği Konseyi (2008), terör suçlarının ve diğer ağır suç fiillerinin önlenmesi, tespit edilmesi ve soruşturulması amaçları için Europol ve Üye Devletlerin belirlenen otoriteleri tarafından Vize Bilgi Sistemi'ne (VIS) başvurulması için erişime ilişkin 23 Haziran 2008 tarihli ve 2008/633/JHA sayılı Konsey Kararı, OJ 2008 L 218
[858] *A.g.e.*
[859] VIS Regülasyonu, Madde 37.
[860] *A.g.e.*, Madde 38(1).
[861] *A.g.e.*, Madde 38(2).
[862] *A.g.e.*, Madde 38(2).

VIS'in gözetiminin sağlanması adına VIS SCG kurulmuştur. VIS SCG, EDPS'nin ve yerel gözetim otoritelerinin temsilcilerinden oluşmaktadır ve yılda iki kere toplanırlar. Bu grup 28 AB Üye Devleti ve İzlanda, Lihtenştayn, Norveç ve İsviçre'nin temsilcilerinden oluşmaktadır[863].

Eurodac

Eurodac, Avrupa Parmak İzlerinin İncelenmesi Birimi anlamına gelmektedir. Eurodac, AB Üye Ülkelerinin birinde sığınma talep eden üçüncü ülke vatandaşlarının ve vatansız kişilerin parmak izi verilerini barındıran merkezi bir sistemdir[864]. Sistem 2725/2000 sayılı Konsey Regülasyonu'nun kabul edilmesi üzerine Ocak 2003'ten beri kullanılmakta ve 2015'te yeniden yapılandırılmıştır. Amacı temel olarak, (EC)604/2013 sayılı Regülasyon kapsamında belirli sığınma başvurularının incelenmesinde hangi Üye Devletin sorumlu olacağının belirlenmesine destek olmaktır. Bu regülasyon, üçüncü ülke vatandaşları ve vatansız kişilerce Üye Ülkelerden birinde yapılan uluslararası koruma başvurusunun incelenmesi için yetkili Üye Devletlerin belirlenmesi için kriterleri ve mekanizmaları belirlemektedir (Dublin III Regülasyonu)[865]. Eurodac'taki kişisel veriler temelde Dublin III Regülasyonu'nun uygulanmasını sağlama amacına hizmet etmektedir[866].

Yerel kolluk otoriteleri ve Europol, suça ilişkin soruşturmalar ile bağlantısı olan Eurodac'ta bulunan parmak izlerini ancak terör ve diğer ağır suç fillerinin önlenmesi, tespit edilmesi veya soruşturulması amaçları için karşılaştırabilmektedirler. Eurodac'ın AB'nin sığınma politikasının uygulanmasını desteklemek için tasarlanmış bir araç olması ve kolluk aracı olmaması nedeniyle kolluk otoritelerinin veri tabanına erişimleri ancak spesifik olaylarda, spesifik hallerde ve katı şartlar altında mümkündür[867]. Dublin III Regülasyonu'nun uygulanması amacıyla kullanılan veriler Genel Veri Koruma Regülasyonu tarafından korunmaktayken, kolluk amaçlarıyla verinin ikincil kullanımlarında Polis ve Ceza Yargılaması Otoriteleri için Veri Koruma Direktifi uygulanmaktadır. Eurodac Değişiklik Regülasyonu uyarınca Üye Devlet veya Europol tarafından elde edilen kişisel verilerin herhangi bir üçüncü ülkeye, uluslararası organizasyon veya AB içerisinde veya dışarısında kurulmuş bir özel hukuk kişisine aktarımı yasaklanmıştır[868].

Eurodac, parmak izlerinin saklanması ve karşılaştırılması için eu-LISA tarafından işletilen bir

---

[863] Bkz. Avrupa Veri Koruma Denetçisi'nin Eurodac'a ilişkin internet sitesi.

[864] Dublin Anlaşması'nın etkili kullanımı için parmak izlerinin karşılaştırılması için Eurodac'ın kurulmasına ilişkin 11 Aralık 2000 tarihli ve (EC) 2725/2000 sayılı Konsey Regülasyonu, OJ 2000 L 316; Dublin Anlaşması'nın etkili kullanımı için parmak izlerinin karşılaştırılması için Eurodac'ın kurulmasına ilişkin (EC) 2725/2000 sayılı Konsey Regülasyonu'nun uygulanması için birtakım kuralları belirleyen 28 Şubat 2002 tarihli ve (EC) 407/2002 sayılı Konsey Regülasyonu, OJ 2002 L 62 (Eurodac Regülasyonları), üçüncü ülke vatandaşları ve vatansız kişilerce Üye Ülkelerden birinde yapılan uluslararası koruma başvurusunun incelenmesi için yetkili Üye Devletlerin belirlenmesi için kriterleri ve mekanizmaları belirleyen (EU) 604/2013 sayılı Regülasyonun etkili uygulanması ve emniyet amaçlarıyla Üye Ülkelerin kolluk otoritelerinin ve Europol'un Eurodac verilerini ile karşılaştırma için talepleri için parmak izlerinin karşılaştırılması için "Eurodac"ın kurulmasına ilişkin ve özgürlük, güvenlik ve adalet alanlarında büyük ölçekli bilgi teknolojileri sistemleri için bir Avrupa Bürosu kuran (EU)1077/2011 sayılı Regülasyonu1077/2011 sayılı Regülasyon'u değiştiren Avrupa Parlamentosu ve Konseyi'nin 26 Haziran 2013 tarihli ve (EU) 603/2013 sayılı Regülasyonu, OJ 2013 L 180, sf. 1 (Eurodac Değişiklik Regülasyonu).

[865] Üçüncü ülke vatandaşları ve vatansız kişilerce Üye Ülkelerden birinde yapılan uluslararası koruma başvurusunun incelenmesi için yetkili Üye Devletlerin belirlenmesi için kriterleri ve mekanizmaları belirleyen Avrupa Parlamentosu ve Konseyi'nin 26 Haziran 2013 tarihli ve (EU) 604/2013 sayılı Regülasyon, OJ 2013 L 180, sf.1, Madde 1(1).

[866] Eurodac Değişiklik Regülasyonu, OJ 20131 L 180, sf.1, Madde 1(1).

[867] *A.g.e.*, Madde 1(2).

[868] *A.g.e.*, Madde 35.

merkez birim ve Üye Devletler ile merkez veri tabanı arasında elektronik veri aktarımı için bir sistemden oluşmaktadır. Üye Devletler, kendi bölgelerinde sığınma talep eden ve en az 14 yaşında olan tüm kişilerin ve kendi dış sınırlarını izinsiz şekilde geçerken yakalanan en az 14 yaşındaki AB vatandaşı olmayanların veya vatansız kişilerin parmak izlerini alır ve iletir. Üye Devlet ayrıca kendi topraklarında izinsiz bir şekilde kalan AB vatandaşı olmayan kişiler ile vatansız kişilerin parmak izlerini alır ve iletir.

Herhangi bir Üye Devlet Eurodac'a danışabilmekte ve parmak izi verileri ile karşılaştırma talep edebilmekte olsa da sadece parmak izini alan ve bunları merkez birime ileten Üye Devlet, düzelterek, ekleme yaparak veya silerek bu verileri değiştirebilir[869]. Eu-LISA veri korumasının denetlenmesi ve veri korumasının sağlanması için tüm veri işleme faaliyetlerinin kaydını tutar[870]. Yerel denetim otoriteleri, veri sahiplerine haklarının kullanımında destek olur ve yol gösterir[871]. Parmak izi verisinin toplanması ve iletilmesi yerel mahkemelerin yasal denetimine tabidir[872]. AB Kuruluşları Veri Koruma Regülasyonu[873] ve EDPS tarafından denetim, Eurodac'a ilişkin olarak eu-LISA tarafından işletilen Merkezi Sistem'in işleme faaliyetlerine uygulanır[874]. Hukuka aykırı bir işleme faaliyetinden ve Eurodac regülasyonuna uygun olmayan herhangi bir fiilden dolayı bir kişinin zarar görmesi halinde bu kişinin, zarardan sorumlu Üye Devletten tazminat alma hakkı vardır[875]. Ancak belirtilmesi gerekir ki sığınma talep eden kişiler genellikle uzun ve riskli yolculuklar geçirmiş özellikle hassas bir gruptur. Bu hassaslıkları ve sığınma başvurularının incelenmesi beklenmesi süresindeki istikrarsız durumları nedeniyle uygulamada bu kişilerin, özellikle tazminat haklarını kullanmaları zor olabilmektedir.

Eurodac'ı kolluk amaçları ile kullanmak için Üye Devletler, erişim talebinde bulunacak otoriteler ile karşılaştırma için yapılan taleplerin hukuka uygunluklarını kontrol edecek otoriteler kurmak zorundadırlar[876]. Yerel otoritelerin ve Europol'ün Eurodac parmak izi verilerine erişimleri çok katı şartlara bağlanmıştır. Talepte bulunan taraf, ancak verileri ulusal parmak izi veri tabanı ve VIS gibi diğer müsait bilgi sistemlerinde karşılaştırdıktan sonra gerekçeli elektronik talepte bulunmak zorundadır. Karşılaştırmanın orantılı olmasını sağlayan bir üstün kamu güvenliği olması gerekmektedir. Karşılaştırma gerçekten gerekli, olay özeli ile ilgili olmalı, karşılaştırmanın, Eurodac sistemi kapsamında parmak izi toplanmasına tabi kategori kapsamında terör suçu veya diğer ağır suç fiillerinin şüphelisi, faili veya mağduru olduğuna ilişkin doğrulanmış bir şüphenin olduğu haller olmak üzere suç fiilinin önlenmesi, tespit edilmesi veya soruşturulmasına önemli derecede katkıda bulunmasına ilişkin geçerli temellerin mevcut olması gerekmektedir. Karşılaştırma sadece parmak izi ile yapılmalıdır. Europol da parmak izini toplayan Üye Devletin iznini olmak zorundadır.

Sığınma başvurusuna ilişkin Eurodac'ta saklanan kişisel veriler, ilgili kişinin AB vatandaşlığı kazanması halleri dışında parmak izinin alınma tarihinden itibaren 10 yıllık bir süreyle tutulmaktadır. Bu durumda veri derhal silinmelidir. Dış sınırların yetkisiz bir şekilde geçilmesi sırasında yakalanan yabancılara ilişkin veriler 18 ay boyunca saklanır. Bu kişinin kalma izni

---

[869] *A.g.e.*, Madde 27.
[870] *A.g.e.*, Madde 28.
[871] *A.g.e.*, Madde 29.
[872] *A.g.e.*, Madde 29.
[873] Topluluğun kuruluşları ve organları tarafından kişisel verilerin işlenmesine ilişkin bireylerin korunması ve bu verilerin serbest dolaşımına ilişkin Avrupa Parlamentosu ve Konseyi'nin 18 Aralık 2000 tarihli ve (EC) 45/2001 sayılı Regülasyonu, OJ 2001 L 8.
[874] Eurodac Değişiklik Regülasyonu, OJ 2013 L 180, sf.1, Madde 31.
[875] *A.g.e.*, Madde 37.
[876] Roots, L. (2015), "Yeni EURODAC Regülasyonu: Gayrı Resmi Ayrımcılık Kaynağı olarak Parmak İzleri", *Tallinn Teknoloji Üniversitesi Avrupa Çalışmaları Baltık Gazetesi*, Vol. 5, No.2, sf. 108-129.

alması, AB sınırlarını terk etmesi veya bir Üye Devletin vatandaşlığını kazanması halinde bu veriler derhal silinir. Sığınma sağlanan kişilerin verileri, terör ve diğer ağır suç fiillerinin önlenmesi, tespit edilmesi ve soruşturulması kapsamında karşılaştırma için 3 yıllık süre ile bulundurulmaya devam edilir.

Tüm AB Üye Devletlerinin yanında İzlanda, Norveç, Lihtenştayn ve İsviçre de uluslararası anlaşma nezdinde Eurodac'ı kullanmaktadır.

Eurodac'ın denetiminin sağlanması için Eurodac SCG kurulmuştur. Yılda iki kere toplanan EPDS'nin ve yerel denetim otoritelerinin temsilcilerinden oluşmaktadır. Bu grup, 28 AB Üye Devletinin ve İzlanda, Lihtenştayn, Norveç ve İsviçre'nin temsilcilerinden oluşmaktadır[877].

Genel Bakış

Mayıs 2016'da Komisyon, Ortak Avrupa Sığınma Sistemi'nin (CEAS)[878] işleyişinin iyileştirilmesi amacını taşıyan reformun bir parçası olarak yeni bir Eurodac Değişiklik Regülasyonu üzerine teklifte bulunmuştur. Teklif edilen değişiklik, asıl Eurodac veri tabanın kapsamını büyük ölçüde genişletmesi sebebiyle önemlidir. Eurodac aslında, AB içerisinde sığınma başvurularının incelenmesinde hangi Üye Devletin sorumlu olacağının belirlenmesini sağlamak için parmak izi delillerini sağlayarak CEAS'ın uygulanmasını desteklemek amacıyla kurulmuştur. Teklif edilen değişiklik, kanuna uygun olmayan göçmenlerin ülkelerine iadesini sağlamak için veri tabanının kapsamını genişletmektedir[879]. Yerel otoriteler, AB'de hukuka aykırı olarak kalan üçüncü taraf ülke vatandaşlarının veya AB'ye hukuka aykırı olarak giren kişilerin belirlenmesi amacıyla, bu kişilerin geri gönderilmesi için Üye Devletlere destek olmak adına delil elde etmek için veri tabanına başvurabilecektir. Buna ek olarak, mevcut düzenleme sadece parmak izlerinin toplanması ve saklanmasını gerektirmekteyken teklif, kişilerin, başka bir tür biyometrik veri olan yüz resimlerinin toplanmasını da getirmektedir[880]. Teklif aynı zamanda biyometrik verilerinin alınabileceği çocukların alt yaş sınırını, 14 yıldan, 2013 regülasyonundaki minimum yaş olan 6 yıla[881] indirmektedir. Teklifin genişletilmiş kapsamı, veri tabanına dahil olabilecek daha çok kişinin gizlilik haklarına ve veri korumasına müdahale teşkil edeceği anlamına gelmektedir. Bu müdahalenin dengelenmesine adına teklif ve Avrupa Parlamentosu'nun LIBE Komitesi[882] tarafından teklif edilen değişiklikler, veri koruma

[877] Bkz. Avrupa Veri Koruma Denetçisi'nin Eurodac'a ilişkin internet sitesi.
[878] Avrupa Komisyonu, üçüncü ülke vatandaşları ve vatansız kişilerce Üye Ülkelerden birinde yapılan uluslararası koruma başvurusunun incelenmesi için yetkili Üye Devletlerin belirlenmesi için kriterleri ve mekanizmaları belirleyen Avrupa Parlamentosu ve Konseyi'nin 26 Haziran 2013 tarihli ve (EU) 604/2013 sayılı Regülasyon'nun etkili uygulanması, yasadışı kalan üçüncü ülke vatandaşlarının ve vatansız kişilerin belirlenmesi için parmak izlerinin karşılaştırılması için "Eurodac"ın kurulmasına ve kolluk amaçlarıyla Üye Devletlerin kolluk otoriteleri ile Europol tarafından Eurodac verilerinin karşılaştırılması için taleplere dair Avrupa Parlamentosu ve Konseyi'nin Regülasyon Teklifi (değişiklik), COM(2016) final, 4 Mayıs 2016.
[879] Bkz. Teklife ilişkin açıklamalı bilgi notu, sf.3.
[880] Avrupa Komisyonu, üçüncü ülke vatandaşları ve vatansız kişilerce Üye Ülkelerden birinde yapılan uluslararası koruma başvurusunun incelenmesi için yetkili Üye Devletlerin belirlenmesi için kriterleri ve mekanizmaları belirleyen Avrupa Parlamentosu ve Konseyi'nin 26 Haziran 2013 tarihli ve (EU) 604/2013 sayılı Regülasyon'nun etkili uygulanması, yasadışı kalan üçüncü ülke vatandaşlarının ve vatansız kişilerin belirlenmesi için parmak izlerinin karşılaştırılması için "Eurodac"ın kurulmasına ve kolluk amaçlarıyla Üye Devletlerin kolluk otoriteleri ile Europol tarafından Eurodac verilerinin karşılaştırılması için taleplere dair Avrupa Parlamentosu ve Konseyi'nin Regülasyon Teklifi (değişiklik), COM(2016) final, 4 Mayıs 2016, Madde 2(1).
[881] *Ibid.*, Madde 2(2).
[882] Avrupa Parlamentosu, *üçüncü ülke vatandaşları ve vatansız kişilerce Üye Ülkelerden birinde yapılan uluslararası koruma başvurusunun incelenmesi için yetkili Üye Devletlerin belirlenmesi için kriterleri ve mekanizmaları belirleyen Avrupa Parlamentosu ve Konseyi'nin 26 Haziran 2013 tarihli ve (EU) 604/2013 sayılı Regülasyon'nun etkili uygulanması, yasadışı kalan üçüncü ülke vatandaşlarının ve vatansız kişilerin belirlenmesi*

şartlarının güçlendirilmesini amaçlamaktadır. El kitabının hazırlanması sırasında teklife ilişkin görüşmeler Parlamento ve Konsey'de devam etmektedir.

Eurosur

Avrupa Sınır Takip Sistemi (Eurosur)[883], hukuka aykırı göç ve sınır ötesi suçların tespit edilmesi, önlenmesi ve bunlarla mücadele edilmesi ile Schengen dış sınırlarının kontrolünün geliştirilmesi için tasarlanmıştır. Yerel iş birliği merkezleri ile yeni entegre sınır idaresi konseptini geliştirmek ve uygulamakla görevli AB birimi olan Frontex arasında bilgi değişiminin ve operasyonel iş birliğinin geliştirilmesine hizmet etmektedir[884]. Genel amaçları şu şekildedir:

- Fark edilmeden AB'ye giren hukuka aykırı göçmen sayısının azaltılması;
- Denizde daha çok hayatın kurtarılması ile hukuka aykırı göçmenlerin ölüm sayısının azaltılması;
- Sınır ötesi suçların önlenmesine katkıda bulunarak AB genelinde iç güvenliğin artırılması[885].

Eurosur, çalışmalarına, tüm dış sınırı olan Üye Devletlerde 2 Aralık 2013, diğer devletlerde 1 Aralık 2014 tarihinde başlamıştır. Regülasyon, Üye Devletlerin dış toprakları, deniz ve hava sahalarının denetimine uygulanmaktadır. Üye Devletler ve Frontex sadece gemi kimlik numaralarını paylaşmaya yetkili oldukları için Eurosur kişisel verileri çok dar bir kapsamda paylaşmakta ve işlemektedir. Eurosur, devriyelerin ve olayların konumu gibi operasyonel bilgi değişiminde bulunmaktadır ve paylaşıma konu bilgiler kural olarak kişisel veri içeremezler[886]. Kişisel verilerin Eurosur çerçevesinde paylaşıldığı istisnai durumlarda regülasyon, veri korumasına ilişkin genel AB hukuki çerçevenin tamamen uygulanacağını öngörmektedir[887].

Böylece Eurosur, özellikle kişisel veri paylaşımlarının Polis ve Ceza Yargılaması Otoriteleri için Veri Koruma Direktifi'nde ve Genel Veri Koruma Regülasyonu'nde öngörülen kriterlere ve güvenliklere uygun olması gerektiğini belirterek verilerin korunması hakkını güvence altına almaktadır[888].

Gümrük Bilgi Sistemi

---

için parmak izlerinin karşılaştırılması için "Eurodac"ın kurulmasına ve kolluk amaçlarıyla Üye Devletlerin kolluk otoriteleri ile Europol tarafından Eurodac verilerinin karşılaştırılması için taleplere dair Avrupa Parlamentosu ve Konseyi'nin regülasyon teklifine ilişkin rapor, PE 597.620v03-00, 9 Haziran 2017.

[883] Avrupa Sınır Takip Sistemini (Eurosur) kuran Avrupa Parlamentosu ve Konseyi'nin 22 Ekim 2013 tarihli ve (EU)1052/2013 sayılı Regülasyonu, OJ 2013 L 295.

[884] Avrupa Sınır ve Sahil Güvenliğine dair ve Avrupa Parlamentosu ve Konseyi'nin (EU)2016/399 sayılı Regülasyonu'nu değiştiren ve Avrupa Parlamentosu ve Konseyi'nin (EC)863.2007 sayılı Regülasyonu'nu kaldıran Avrupa Parlamentosu ve Konseyi'nin 14 Eylül 2016 tarihli ve (EU)2916/1624 sayılı Regülasyonu, (EC)2007/2004 sayılı Konsey Regülasyonu ve 2005/267/EC sayılı Konsey Kararı, OJ L 251.

[885] Ayrıca bkz. Avrupa Komisyonu (2008), Komisyon tarafından Avrupa Parlamentosu'na, Konsey'ine, Avrupa Ekonomik ve Sosyal Komitesi'ne ve Bölgelerin Komitesi'ne Bildirim: Avrupa Sınır Takip Sistemi'nin (Eurosur) kurulmasının değerlendirilmesi, COM(2008) 68 final, Brüksel, 13 Şubat 2008; Avrupa Komisyonu (2011), Avrupa Sınır Takip Sistemi'nin (Eurosur) kuran Avrupa Parlamentosu ve Konsey'inin Regülasyon Teklifine ilave Etki Değerlendirmesi, Kadro çalışma belgesi, SEC(2011) 1536 final, Brüksel, 12 Aralık 2011, sf.18.

[886] Avrupa Komisyonu, EUROSUR: Schengen dış sınırlarının korunması – göçmenlerin hayatlarının korunması. Kısaca EUROSUR, 29 Kasım 2013.

[887] 1052/2013 sayılı Regülasyon, Gerekçe 13 ve Madde 13.

[888] *A.g.e.*, Gerekçe 13 ve Madde 13.

Bir başka AB seviyesinde kurulmuş önemli bilgi sistemi Gümrük Bilgi Sistemi'dir (CIS)[889]. İç pazarın oluşturulması sırasında, AB toprakları içerisinde dolaşan mallara ilişkin tüm kontroller ve formaliteler kaldırılmıştır ancak bunun sonucunda yüksek seviyede dolandırıcılık riski ile karşılaşılmıştır. Bu risk, Üye Devletlerin gümrük idareleri arasında artırılmış iş birliği ile dengelenmiştir. CIS'ın amacı, yerel ve AB gümrük ve tarım mevzuatlarının ağır ihlallerinin Üye Devletlerce önlenmesi, soruşturulması ve kovuşturulmasına destek olunmasıdır. CIS, iki hukuki işlem ile kurulmuş, farklı hukuki zeminlerde kabul edilmiştir: (EC)515/97 sayılı Konsey Regülasyonu, gümrük birliği ve ortak tarım politikası kapsamında dolandırıcılıkla mücadele edilmesi için farklı yerel idari otoriteler arasındaki iş birliğine ilişkin iken 2009/917/JHA sayılı Konsey Kararı ise ciddi gümrük mevzuatı ihlallerinin önlenmesi, soruşturulması ve kovuşturulmasına destek sağlamayı amaçlar. Bu durum, CIS'in sadece kolluk ile ilgilenmediği anlamına gelmektedir.

CIS'te bulunan bilgiler, tutulan, el konulan ve haczedilmiş emtia, ulaşım araçları, işletmeler, kişiler, mal ve nakit paralara ilişkin kişisel verileri içerir. İşlenmesi mümkün veri kategorileri açıkça belirlenmiştir ve ilgili kişilerin ismi, vatandaşlığı, cinsiyeti, doğum yeri ve tarihi, verilerinin sisteme dahil olmasındaki sebep ve ulaşım aracının kayıt numarasını kapsar[890]. Bu bilgiler ancak belirli soruşturmaların izlenmesi, raporlanması veya yürütülmesi amaçlarıyla veya gümrük hükümlerini ihlal etmekten şüphelenilen kişilere ilişkin stratejik veya operasyonel analizler için kullanılabilir.

CIS'e erişim, Europol ve Eurojust'a olduğu gibi yerel gümrük, vergi, tarım, kamu sağlığı ve polis otoritelerine tanınmıştır.

Kişisel verilerin işlenmesi, Genel Veri Koruma Regülasyonu, AB Kuruluşları Veri Koruma Regülasyonu, Modernize Edilmiş Sözleşme 108 ve Polis Tavsiye Kararı'na uygun olması gerektiği gibi, 515/97 sayılı Regülasyon ve 2009/917/JHA sayılı Konsey Kararı'nda belirtilen spesifik kurallara uygun olmalıdır. CIS'in (EC)45/2001 sayılı Regülasyon'a uygunluğunu denetlemekten EDPS sorumludur. CIS, yılda en az bir kere CIS'e ilişkin denetim konularına ilişkin yetkisi olan yerel veri koruma denetim otoritelerinin tümünü toplantıya çağırır.

AB Bilgi Sistemlerinin Birlikte Çalışabilirliği

Göç idaresi, AB'nin dış sınırlarının entegre sınır yönetimi ve terörizm ve sınır ötesi suçlarla mücadele önemli zorluklar barındırmaktadır ve globalleşmiş bir dünyada oldukça karmaşık hale gelmiştir. Son yıllarda AB, AB'nin değerleri ve temel hakları tehlikeye düşürmeden güvenliğin sağlanması ve korunması için yeni bir kapsayıcı anlayış üzerine çalışmaktadır. Bu çabalarında yerel kolluk otoriteleri ve Üye Devletler ile ilgili AB kurumları arasında etkin bilgi değişimi anahtar rol oynamaktadır[891]. Sınır idaresi ve iç güvenliğe ilişkin mevcut AB bilgi

[889] Avrupa Birliği Konseyi (1995), gümrük amaçlarıyla bilgi teknolojilerinin kullanılmasına ilişkin Anlaşmayı düzenleyen Avrupa Birliği Konseyi tarafından değiştirilen (2009) 26 Temmuz 1995 tarihli Konsey İşlemi, OJ 1995 C 136, Üye Devletlerin idari otoriteleri arasında ortak yardım ve iş birliği ve gümrük ve tarıma ilişkin hukukunun doğru uygulanmasını sağlamak üzere Komisyona ilişkin 13 Mart 1997 tarihli ve 515/97 sayılı Regülasyon, gümrük amaçları ile bilgi teknolojilerinin kullanılmasına ilişkin 30 Kasım 2009 tarihli ve 2009/917/JHA sayılı Konsey Kararı, OJ 2009 L 323 (CIS Kararı).

[890] Bkz. CIS Kararı, Madde 24, 25 ve 28.

[891] Avrupa Komisyonu (2016), Komisyondan Avrupa Parlamentosu ve Konseyi'ne Bildirim: Sınır ve Güvenlik için Daha Güçlü ve Daha Akıllı Bilgi Sistemleri, COM(2016) 295 final, Brüksel, 6 Nisan 2016, Avrupa Komisyonu (2016), Komisyondan Avrupa Parlamentosu, Avrupa Konseyi ve Konseyi'ne Bildirim: Hareketlilik dünyasında Güvenliğin Artırılması: terörizm ile mücadelede gelişmiş bilgi değişimi ve daha güçlü dış sınırlar, COM(2016) 602 final, Brüksel, 14 Eylül 2016, Avrupa Komisyonu (2016) Yasa dışı kalan üçüncü ülke vatandaşlarının geri döndürülmesi için Schengen Bilgi Sisteminin kullanılmasına ilişkin Avrupa Parlamentosu ve

sistemlerinin kendilerine ait amaçları, kuruluşa ilişkin bir yapısı, veri sahipleri ve kullanıcıları vardır. AB, birlikte çalışabilirliğin potansiyellerini keşfederek SIS II, VIS ve Eurodac gibi farklı bilgi sistemleri arasında parçalara ayrılmış AB veri yönetiminin işlevselliğindeki eksikliklerin üstesinden gelinmesi üzerinde çalışmaktadır[892]. Temel amaç, gizlilik, verilerin korunması ve diğer temel haklara saygı ile denge korunurken yetkili polis, gümrük ve adli otoritelerin sistematik olarak görevlerini yerine getirmek için gerekli bilgilere sahip olmalarını sağlamaktır.

Birlikte çalışabilirlik, "bilgi sistemlerinin veri değişiminde bulunma ve bilginin paylaşılmasını sağlayabilme kabiliyetleri"dir[893]. Bu paylaşım, Genel Veri Koruma Regülasyonu, Polis ve Ceza Yargılaması Otoriteleri için Veri Koruma Direktifi, AB Temel Haklar Bildirgesi ve tüm diğer ilgili kurallar tarafından garanti edilen erişim ve kullanıma dair mecburi katı kuralları ihlal etmemelidir. Veri yönetimine için herhangi bir entegre çözüm, amaçla sınırlılık, tasarımda gizlilik ve varsayılan olarak gizlilik ilkelerini etkilememelidir[894].

Üç temel bilgi sisteminin -SIS II, VIS ve Eurodac- işlevselliklerinin iyileştirilmesi yanında Komisyon, 2020'ye kurulması beklenen[895], üçüncü ülke vatandaşları için dördüncü bir merkezi sınır idare sistemi kurulmasını teklif etmiştir: Giriş-Çıkış Sistemi (EES)[896]. Komisyon aynı zamanda, ileri düzensiz göç ve güvenlik kontrollerinin sağlanması için AB'de vizesiz gezen kişilere dair bilgilerin toplanması için bir sistem olan Avrupa Seyahat Bilgi ve İzin Sistemi'nin (ETIAS)[897] kurulması için bir teklifte bulunmuştur.

9. Özel veri türleri ve ilgili veri koruma kuralları

Bazı hallerde, Modernize Edilmiş Sözleşme 108 veya Genel Veri Koruma Regülasyonu'nun genel kurallarının daha detaylı bir şekilde belirli olaylara uygulanması Avrupa seviyesinde özel hukuki araçlar oluşturulmuştur.

9.1. Elektronik Haberleşme

Konseyi'nin Regülasyon Teklifi. Ayrıca bkz. Avrupa Parlamentosu, Avrupa Konseyi ve Konsey Komisyonu'ndan Bildirim: etkili ve gerçek bir Güvenlik Birliği'ne doğru yedinci ilerleme raporu, COM(2017) 261 final, Brüksel, 16 Mayıs 2017.

[892] Avrupa Birliği Konseyi (2005), Lahey Programı: Avrupa Birliği'nde Özgürlük, Güvenlik ve Adaletin Güçlendirilmesi, OJ 2005 C 53, Avrupa Komisyonu (2010), Komisyon tarafından Avrupa Parlamentosu ve Konseyi'ne Bildirim: özgürlük, güvenlik ve adalet alanlarında bilgi yönetimine genel bir bakış, COM(2010) 385 final, Avrupa Komisyonu (2016), Komisyon tarafından Avrupa Parlamentosu ve Konseyi'ne Bildirim: Sınır ve Güvenlik için Daha Güçlü ve Daha Akıllı Bilgi Sistemleri, COM(2016) 205 final, Brüksel, 6 Nisan 2016, Avrupa Komisyonu (2016), Bilgi Sistemleri ve Birlikte Çalışabilirlik üzerine Yüksek Seviye Uzman Grubu'nu düzenleyen 17 Haziran 2016 tarihli Komisyon Kararı, OJ 2016 C 257.

[893] Avrupa Komisyonu (2016), Komisyon tarafından Avrupa Parlamentosu ve Konseyi'ne Bildirim: Sınır ve Güvenlik için Daha Güçlü ve Daha Akıllı Bilgi Sistemleri, COM(2016) 205 final, Brüksel, 6 Nisan 2016, sf. 14.

[894] *A.g.e.*, sf.4-5

[895] Avrupa Komisyonu (2016), Komisyon'dan Avrupa Parlamentosu ve Konseyi'ne Bildiri: Sınırlar ve Güvenlik İçin Daha Güçlü ve Daha Akıllı Bilgi Sistemleri, COM(2016), 205 final, Brüksel, 4 Nisan 2016, sf. 5.

[896] Avrupa Komisyonu (2016), Avrupa Birliği'nin dış sınırlarını geçen üçüncü ülke vatandaşlarının giriş ve çıkış verilerinin ve girişin reddedilmesi verilerinin kaydedilmesi için bir Giriş/Çıkış Sistemi (EES) kuran ve kolluk amaçlarıyla EES'ye erişimin şartlarını belirleyen ve (EC)767/2008 sayılı Regülasyon ile (EU)1077/2011 sayılı Regülasyonları değiştiren Avrupa Parlamentosu ve Konseyi'nin Yönetmelik Teklifi, COM(2016) 194 final, Brüksel, 6 Nisan 2016.

[897] Avrupa Komisyonu (2016), Avrupa Seyahat Bilgi ve İzin Sistemi'ni (ETIAS) kuran ve (EU) 515/2014, (EU)2016/399, (EU)2016/794 ve (EU)2016/1624 sayılı Regülasyonları değiştiren Avrupa Parlamentosu ve Konseyi'nin Yönetmelik Teklifi, COM(2016) 731 final, 16 Kasım 2016.

AB	Ele Alınan Konular	Avrupa Konseyi
Genel Veri Koruma Regülasyonu Gizlilik ve Elektronik Haberleşme Direktifi	**Elektronik haberleşme**	Modernize Edilmiş Sözleşme 108 Telekomünikasyon Hizmetleri Tavsiye Kararı
Genel Veri Koruma Regülasyonu, Madde 89	**İstihdam ilişkisi**	Modernize Edilmiş Sözleşme 108 İstihdam Tavsiye Kararı AİHM, Copland/Birleşik Krallık, No.62617/00, 2007
Genel Veri Koruma Regülasyonu, Madde 9(2)(h) ve (i)	**Sağlık verisi**	Modernize Edilmiş Sözleşme 108 Sağlık Verisi Tavsiyesi AİHM, Z/Finlandiya, No. 22009/93, 1997
Klinik Çalışmalar Regülasyonu	**Klinik çalışmalar**	
Genel Veri Koruma Regülasyonu, Madde 6(4), Madde 89	**İstatistik**	Modernize Edilmiş Sözleşme 108 İstatistiki Veri Tavsiye Kararı
Avrupa istatistiklerine ilişkin (EC) 223/2009 sayılı Regülasyon CJEU, C-524/06, Huber/ Bundesrepublik Deutschland [GC], 2008	**Resmi istatistik**	Modernize Edilmiş Sözleşme 108 İstatistiki Veri Tavsiye Kararı
Finansal araçlarda pazarlara ilişkin 2014/65/EU sayılı Direktif Tezgah üstü türevleri, merkezi karşı taraflar ve veri depolama kuruluşlarına ilişkin (EU)648/2012 sayılı Regülasyon Kredi derecelendirme kuruluşlarına ilişkin (EC) 1060/2009 sayılı Regülasyon İç pazarda ödeme hizmetlerine ilişkin 1007/64/EC sayılı Direktif	**Finansal veri**	Modernize Edilmiş Sözleşme 108 Ödemeler ve diğer ilgili işlemler için kullanılan 90(19) sayılı Tavsiye Kararı AİHM, Michaud/Fransa, No.12323/11, 2012

Kilit Noktalar

- Telefon hizmetlerin özel olarak değinen telekomünikasyon alanındaki özel veri koruma kuraları 1995 Avrupa Konseyi Tavsiye Kararı'nda yer almaktadır.
- Avrupa düzeyinde iletişim hizmetlerinin sağlanmasına ilişkin kişisel veri işlenmesi, gizlilik ve elektronik haberleşmeye ilişkin Direktif ile düzenlenmektedir.
- Elektronik iletişimin gizliliği sadece iletişimin içeriğine ilişkin olmayıp aynı zamanda kimin kiminle ne zaman ve ne kadar süreyle iletişimde bulunduğu gibi meta veri ve verinin nereden iletildiği gibi konum verilerini de kapsar.

İletişim ağlarının, bu ağlarda gerçekleşen iletişimlerin dinlenmesi ve takip edilmesi açısından güçlü teknik imkanlar sunmalarından dolayı kullanıcıların özel alanlarına hukuka aykırı müdahale edilmesi potansiyeli yüksektir. Dolayısıyla komünikasyon hizmetlerindeki kullanıcılar için söz konusu özel riske hitap eden özel veri koruma düzenlemeleri gerekli görülmüştür.

1995 yılında Avrupa Konseyi, telefon hizmetlerini özellikle düzenleyen telekomünikasyon alanında veri koruması için bir Tavsiye Kararı yayınlamıştır[898]. Buna göre, telekomünikasyon bağlamında kişisel verilerin toplanması ve işlenmesi amaçları sınırlı olmalıdır: bir kullanıcının ağa bağlanması, telekomünikasyon hizmetinin kullanılabilir kılınması, faturalandırma, doğrulama, optimal teknik operasyonun sağlanması ve ağ ile servisin geliştirilmesi.

İletişim ağlarının doğrudan pazarlama mesajlarının gönderilmesi için kullanılmasına ayrıca dikkat gösterilmiştir. Kural olarak doğrudan pazarlama mesajları, bunları almayı istemediğini açıkça belirten kullanıcılara yönlendirilemeyecektir. Önceden kaydedilmiş reklam mesajlarının iletilmesi için otomatik arama araçları ise sadece kullanıcının açık rızasını verdiği hallerde kullanılabilir. Bu alanda detaylı kurallar iç hukuk tarafından belirlenmektedir.

AB hukuku çerçevesinde, 1997'deki ilk denemeden sonra 2002 yılında gizlilik ve elektronik haberleşme Direktifi kabul edilmiş, 2009'da değişmiştir. Bunun amacı, telekomünikasyon sektöründe eski Veri Koruma Direktifi'nin düzenlemelerine eklemeler ve uygun hale getirmeler yapılması idi[899].

Gizlilik ve elektronik telekomünikasyon Direktifi'nin uygulanması kamusal elektronik ağlardaki telekomünikasyon hizmetleri ile sınırlıdır.

Gizlilik ve elektronik telekomünikasyon Direktifi, haberleşme sırasında üretilen üç temel veri kategorisini ayırmaktadır:

- Haberleşme sırasında gönderilen mesajların içeriğini oluşturan veriler – bu veriler kesinlikle gizlidir;

- Haberleşmenin tarafları, zamanı ve süresi gibi haberleşmenin kurulması ve devam ettirilmesi için gerekli veri – meta veri denilen, direktifte "trafik verisi" olarak geçen- ;

- Meta veri içerisinde haberleşme cihazının konumuna ilişkin spesifik veriler – konum verileri denilen veriler- mevcuttur. Bu veriler aynı zamanda haberleşme aletinin kullanıcısının konumu hakkında verilerdir.

Trafik verisi, hizmet sağlayıcı tarafından ancak faturalandırma ve hizmetin teknik olarak sunulması için kullanılabilir. Ancak veri sahibinin onayı ile bu veriler, kullanıcının konumunun bir sonraki metro durağı veya eczaneye ilişkin kullanılması veya bulunduğu yerdeki hava

---

[898] Avrupa Konseyi, Bakanlar Komitesi (1995), üye devletlere telefon hizmetlerini özellikle düzenleyen telekomünikasyon alanında kişisel verilerin korumasına ilişkin Rec(95)4 sayılı tavsiye, 7 Şubat 1995.

[899] Elektronik telekomünikasyon ağları ve hizmetlerine ilişkin evrensel hizmet ve kullanıcıların haklarına ilişkin 2002/22/EC sayılı Direktifi, elektronik telekomünikasyon sektöründe kişisel verilerin işlenmesine ve gizliliğin korunmasına ilişkin 2002/58/EC sayılı Direktifi ve tüketicinin korunması mevzuatının uygulanması için sorumlu yerel otoriteler arasında işbirliğine ilişkin 2006/2004 sayılı Regülasyonu değiştiren 25 Kasım 2009 tarihli ve 2009/136/EC sayılı Avrupa Parlamentosu ve Konseyi'nin Direktifi ile değişik elektronik telekomünikasyon sektöründe kişisel verilerin işlenmesine ve gizliliğin korunmasına ilişkin Avrupa Parlamentosu ve Konseyi'nin 12 Temmuz 2002 tarihli ve 2002/58/EC sayılı Direktifi, OJ 2002 L 201 (Gizlilik ve elektronik telekomünikasyon Direktifi), OJ 2009 L 337.

durumuna ilişkin bilgilerin verilmesi gibi katma değerli hizmetler sunan sorumlulara ifşa edilebilir.

E-Gizlilik Direktifi'nin 15 Maddesine göre elektronik ağlardaki komünikasyona ilişkin verilere başka bir erişim, AİHS Madde 8(2)'de belirtildiği ve AB Temel Haklar Bildirgesi Madde 8 ve 51'de teyit edildiği üzere verilerin korunması hakkına meşru müdahale için gereklilikleri sağlamalıdır. Bu tarz bir erişim, suçların soruşturulması amacıyla erişimi içerebilir.

Gizlilik ve elektronik telekomünikasyon Direktifi'nde yapılan 2009 değişikliği aşağıdakileri getirmiştir:

- Doğrudan pazarlama amaçlı e-posta atılmasına ilişkin sınırlandırma SMS, MMS ve diğer benzer uygulamalara da getirilmiştir; pazarlama e-postaları ön onay alınmadıkça yasaktır. Bu tür bir onayın yokluğunda ancak e-posta adreslerini veren ve itiraz etmeyen eski müşteriler pazarlama e-postalarına konu olabilir.

- İstenmeyen ileti yasağının ihlali halinde Üye Devletlere hukuki çareler sağlama yükümlülüğü getirilmiştir[900].

- Bilgisayar kullanıcısının onayı olmaksızın çerez (cookie) kullanımı ile bilgisayar kullanıcısının hareketlerini takip eden ve kaydeden yazılımlara artık izin verilmemektedir. Yeterli korumanın sağlanması adına onayın nasıl açıklanması ve alınması gerektiğine ilişkin düzenlemeleri iç hukuk gerçekleştirecektir[901].

Veriye izinsiz erişim, kayıp veya imha sonucunda bir veri ihlali meydana geldiğinde yetkili denetim makamı derhal bilgilendirilmelidir. Veri ihlalinin sonucu kullanıcılar nezdinde olası bir zarar teşkil ettiği hallerde kullanıcıların bilgilendirilmesi gerekmektedir[902].

Veri Saklama Direktifi[903], haberleşme hizmet sağlayıcıları meta veriyi saklamakla yükümlü kılar. Ancak bu direktif CJEU tarafından iptal edilmiştir (daha fazla bilgi için lütfen Bölüm 8.3'e bakınız.).

Genel Bakış

Ocak 2017'de Avrupa Komisyonu, eski e-Gizlilik Direktifi'nin yerine geçmesi için yeni bir e-Gizlilik Regülasyonu teklifi kabul etmiştir. Amaç aynı kalacak olup "özellikle özel hayata ve haberleşmeye saygı hakları ile kişisel verilerin işlenmesine ilişkin olarak gerçek kişilerin korunması olmak üzere elektronik haberleşme hizmetlerinin sunulmasında ve kullanılmasında gerçek ve tüzel kişilerin temel hak ve özgürlüklerinin" korunmasıdır. Yeni teklif aynı zamanda Birlik içerisinde elektronik haberleşme verilerinin ve elektronik haberleşme hizmetlerinin serbest dolaşımını da sağlamaktadır[904]. Genel Veri Koruma Regülasyonu öncelikle AB Temel

[900] Bkz. Değişik direktif, Madde 13.
[901] Bkz. *A.g.e.*, Madde 5; ayrıca bkz. Madde 29 Çalışma Grubu (2012), Çerez onay istisnasına ilişkin 04/2012 sayılı Görüş, WP 194, Brüksel, 7 Haziran 2012.
[902] Ayrıca bkz. Madde 29 Çalışma Grubu (2011), Mevcut AB kişisel veri ihlali çerçevesi ve gelecekteki politika gelişmeleri için tavsiyelere dair 01/2011 sayılı Çalışma Belgesi, WP 184, Brüksel, 5 Nisan 2011.
[903] Kamusal elektronik haberleşme hizmetlerinin veya kamusal haberleşme ağlarının sağlanmasına ilişkin üretilen ve işlenen verilerin saklanmasına dair ve 2002/58/EC sayılı Direktifi değiştiren 15 Mart 2006 tarihli ve 2006/24/EC sayılı Avrupa Parlamentosu ve Konseyi'nin Direktifi, OJ 2006 L 105.
[904] Elektronik haberleşmede özel hayata saygı ve kişisel verilerin korunmasına ilişkin ve 2002/58/EC sayılı Direktifi kaldıran Avrupa Parlamentosu ve Konseyi'nin Regülasyon Teklifi (Gizlilik ve Elektronik Haberleşme Regülasyonu, (COM(2017) 10 final), Madde 1.

Haklar Bildirgesi'nin 8inci maddesine değinmekte iken teklif edilen regülasyon Bildirge'nin 7nci maddesini AB ikincil düzenlemesine dahil etmeyi amaçlamaktadır.

Regülasyon bir önceki direktifin yeni teknolojiler ve pazar gerçeklerini içermekte, kapsamlı ve Genel Veri Koruma Regülasyonu ile uyumlu bir çerçeve inşa etmektedir. Bu anlamda e-Gizlilik Regülasyonu, Genel Veri Koruma Regülasyonu'nu kişisel veri teşkil eden elektronik haberleşme verisine göre düzenleyerek özel düzenleme niteliğindedir. Yeni regülasyon, elektronik iletilerin içeriği ve illa kişisel veri olmayan meta veri dahil olmak üzere "elektronik haberleşme verileri"nin işlenmesini kapsamaktadır. Coğrafi kapsamı, AB içerisinde elde edilen verinin AB dışında işlendiği haller dahil olmak üzere AB ile sınırlıdır ve OTT haberleşme hizmetleri sağlayıcıları da kapsar. Bunlar, içeriği, hizmeti veya uygulamayı, ağ operatörü veya internet hizmet sağlayıcının (ISP) doğrudan dahil olması söz konusu olmadan internet üzerinden sunan sağlayıcılardır. Bu tür sağlayıcılara örnekler arasında Skype (sesli ve görüntülü arama), WhatsApp (mesajlaşma), Google (arama), Spotify (müzik) veya Netflix (video içerikler) bulunmaktadır. Genel Veri Koruma Regülasyonu'nun uygulama mekanizmaları yeni regülasyona uygulanacaktır.

E-Gizlilik Regülasyonu'nun, Genel Veri Koruma Regülasyonu'nun tüm 28 Üye Devlette uygulanabilir hale gelmiş olduğu 25 Mayıs 2018 tarihinden önce kabul edilmesi planlanmaktadır. Ancak bu durum Avrupa Parlamentosu ve Konseyi'nin ikisinin de kabulüne bağlıdır[905].

9.2. Çalışan verisi

Kilit Noktalar

- İş ilişkisinde veri koruması için özel kurallar, Avrupa Konseyi İstihdam Verisi Tavsiye Kararı'nda ifade edilmiştir.
- Genel Veri Koruma Regülasyonu'nde istihdam ilişkisinin özellikle belirtildiği tek yer hassas verinin işlenmesi bağlamındadır.
- Çalışanların verilerinin işlenmesinde hukuki temel teşkil eden ve özgürce verilmesi gereken rızanın geçerliliği, iş veren ile işçi arasındaki ekonomik dengesizlik göz önünde bulundurulduğunda sorgulanabilir niteliktedir. Rızaya ilişkin şartlar dikkatlice değerlendirilmelidir.

İstihdam bağlamında veri işlenmesi, kişisel verilerin korunmasına dair genel AB mevzuatına tabidir. Ancak bir düzenleme[906] özellikle (diğerlerinin yanında) istihdam bağlamında Avrupa kuruluşlarının işlediği kişisel verilerin korunması ile ilgilenmektedir. Genel Veri Koruma Regülasyonu'nde istihdam ilişkisine özellikle Madde 9(2)'de, istihdam alanında veri sorumlusu veya veri sahibinin belirli haklarını kullanmaları veya yükümlülüklerini yerine getirmeleri için kişisel verilerin işlenebileceğini belirtmek suretiyle değinilmiştir.

Genel Veri Koruma Regülasyonu kapsamında işçi, işlenmesine/saklanmasına serbestçe rızasını verdiği verileri ve verilerinin ne amaçlarla saklandığını net bir şekilde ayırt edebilir durumda

[905] Daha fazla bilgi için bkz. Avrupa Komisyonu (2017), "*Komisyon, tüm elektronik haberleşmeler için yüksek seviye gizlilik kuralları teklif ediyor ve AB kuruluşları için veri koruma kurallarını güncelliyor*", basın duyurusu, 10 Ocak 2017.

[906] Birlik kuruluşları ve organları tarafından kişisel verilerin işlenmesine ilişkin bireylerin korunması ve bu verilerin serbest dolaşımına ilişkin Avrupa Parlamentosu ve Konseyi'nin 18 Aralık 2000 tarihli ve (EC)45/2001 sayılı Regülasyonu, OJ 2001 L 8.

olmalıdır. İşçi aynı zamanda rızasını vermeden önce hakları ve verilerin saklanma süresinin ne kadar olacağı hakkında bilgilendirilmelidir. Gerçek kişilerin haklarına ve özgürlüklerine yüksek risk teşkil edecek bir kişisel veri ihlali söz konusu olursa iş veren bu ihlali işçiye bildirmelidir. Düzenlemenin 88'inci maddesi Üye Devletlerin, işçinin haklarının ve özgürlüklerinin istihdam bağlamındaki kişisel verilerine dair olmak üzere korunması için daha detaylı kurallar belirlemesine izin verir.

Örnek: *Worten* Davası'nda[907] kişisel veri teşkil eden verilerde günlük çalışma ve dinlenme aralıklarını içerek çalışma zamanı kayıtları yer almaktaydı. İç hukuk, bir işvereni, çalışma şartlarının denetlenmesinde görevli yerel otoritelere çalışma zamanı kayıtlarını sunmasını gerekli tutabilir. Bu ise ilgili kişisel verilere doğrudan erişim anlamına gelmektedir. Ancak kişisel verilere erişim, çalışma şartlarına ilişkin mevzuatın yerel otoritelerce denetlenmesi için gereklidir[908].

Avrupa Konseyi'ne gelinecek olursa, İstihdam Verileri Tavsiye Kararı 1989'da çıkarılmış ve 2015'de revize edilmiştir[909]. Tavsiye, hem özel hem kamu sektöründe kişisel verilerin istihdam amaçlarıyla işlenmesine ilişkindir. İşleme, şeffaflık ilkesi ve çalışma yerine izleme sistemlerinin yerleştirilmesinden önce çalışanların temsilcilerine danışılması gibi birtakım prensipler ve kısıtlamalara uygun olmalıdır. Tavsiye aynı zamanda iş verenlerin, çalışanların internet kullanımlarının izlenmesi yerine filtreler gibi önleyici tedbirler alması gerektiğini belirtmektedir.

İstihdam bağlamına özel en sık karşılaşılan veri koruma problemlerinin bir incelemesi Madde 29 Çalışma Grubu'nun bir çalışma belgesinde bulunabilir[910]. Çalışma grubu istihdam verilerinin işlenmesinde hukuki zemin olarak rızanın önemini incelemiştir[911]. Rızayı talep eden iş veren ile rızayı veren işçi arasındaki ekonomik dengesizliğin rızanın özgürce verilip verilmediğine ilişkin genellikle şüphe doğurduğunu değerlendirmiştir. Bu nedenle rızanın veri işlemede hukuki zemin olduğu hallerde şartların, istihdam bağlamında rızanın geçerliliği incelenirken dikkatle değerlendirilmesi gerekmektedir.

Günümüzün tipik çalışma ortamlarındaki ortak veri koruma problemi, iş yerinde çalışanların elektronik iletilerinin meşru bir şekilde denetlenmesinin kapsamıdır. Bu problemin kolay bir çözümü olarak işteyken haberleşme vasıtalarının özel amaçlarla kullanımının yasaklanması öne sürülmektedir. Ancak bu tür bir genel yasaklama orantılı ve gerçekçi olmayabilir. AİHM'in Copland/Birleşik Krallık ve Bărbulescu/Romanya kararları bu bağlamla özellikle ilgilenir niteliktedir.

Örnek: Copland/Birleşik Krallık kararında[912], lise çalışanının telefon, e-posta ve internet

[907] CJEU, C-342/12, Worten – Equipamentos para o Lar SA v. Autoridade para as Condições de Trabalho (ACT), 30 Mayıs 2013, para.19.
[908] *A.g.e.*, para.43.
[909] Avrupa Konseyi, Bakanlar Komitesi (2015), İstihdam bağlamında kişisel verilerin işlenmesine ilişkin Üye Devletlere Tavsiye Kararı Rec(2015)5, Nisan 2015.
[910] Madde 29 Çalışma Grubu (2017), İşte verilerin işlenmesi 2/2017 sayılı Görüş, WP 249, Brüksel, 8 Haziran 2017.
[911] Madde 29 Çalışma Grubu (2005), 24 Ekim 1995 tarihli 95/46/EC sayılı Direktif'in Madde 26(1)'in ortak yorumuna ilişkin çalışma belgesi, WP 114, Brüksel, 25 Kasım 2005.
[912] AİHM, Copland/Birleşik Krallık, No.62617/00, 3 Nisan 2007.

kullanımları, lise vasıtalarının özel amaçlarla aşırı kullanımının olup olmadığının belirlenmesi adına gizlice izlenmekteydi. AİHM, işyeri tesisi içerisinden yapılan telefon aramalarının özel hayat ve haberleşme kavramları kapsamında olduğuna hükmetmiştir. Bu nedenle iş yerinden yapılan bu tür aramalar ve e-postalar, kişisel internet kullanımının izlenmesinden doğan bilgiler de dahil olmak üzere, AİHS'in 8inci maddesi tarafından korunmaktadır. Diğer taraftan iş verenlerin çalışanların telefon, e-posta ve internet kullanımlarını izlemesine imkan veren şartların düzenlendiği bir düzenleme bulunmamaktadır. Bu nedenle müdahale hukuka uygun değildir. Mahkeme, AİHS'in 8inci maddesinin ihlal edildiğine hükmetmiştir.

Örnek: Bărbulescu/Romanya[913] kararında davacı, iş saatlerinde iş yerindeki interneti, iç düzenlemelere aykırı olarak kullanmaktan dolayı uzaklaştırılmıştır. İş vereni haberleşmeyi takip etmekteymiş. Tamamen özel nitelikteki mesajları gösteren kayıtlar yerel dava sürecinde elde edilmiştir. Madde 8'i uygulanabilir bulmakla beraber AİHM, iş verenin kısıtlayıcı düzenlemelerinin davacıyı haklı bir gizlilik beklentisine sürükleyip sürüklemediğini sorgulamıştır ancak iş verenin talimatlarının iş yerindeki özel sosyal hayatın sıfıra indirilmesi sonucu doğuramayacağına karar vermiştir.

Esasa bakıldığında, Taraf Ülkeler'in, iş verenin iş yerinde işçilerinin profesyonel nitelikte olmayan elektronik ve diğer haberleşmelerini düzenleyebileceği şartların belirlendiği hukuki çerçevenin belirlenmesindeki değerlendirmelerde geniş bir takdir alanına sahip olması gerekmektedir. Buna rağmen yerel otoriteler, yazışmaların ve diğer haberleşmelerin izlenmesi için, kapsam ve süresinden bağımsız olarak düzenlemelerin iş veren tarafından önceden bildirilmesi, kötüye kullanmaya karşı uygun ve yeterli güvenlik tedbirlerini de sağlamak zorundadırlar. Orantılılık ve keyfiyete karşı usuli güvenceler önemli görülmüş ve AİHM şartlara bağlı olarak birtakım faktörler belirlemiştir. Bunların arasında iş veren tarafından yapılan izlemenin kapsamı ve işçinin özel hayatına müdahalenin derecesi; işçi için sonuçları; ve uygun güvencelerin sağlanıp sağlanmadığı vardır. Bunlara ek olarak yerel otoriteler, iletileri izlenen işçinin, en azından esasa ilişkin olacak şekilde yargılama yetkisi mevcut bir yargı organları önündeki çarelere erişimi olup olmadığını denetlemesi gerekmektedir.

Bu davada AİHM, yerel otoritelerin davacının özel hayata ve haberleşmeye saygı hakkının korunması için yeterli güvenceyi sağlamamaları ve bu nedenle ilgili menfaatler arasında adil bir denge sağlanmasında başarısız olması nedeniyle 8inci maddenin ihlali olduğuna hükmetmiştir.

Avrupa Konseyi İstihdam Tavsiye Kararı uyarınca istihdam amaçlarıyla toplanan kişisel veriler doğrudan işçinin kendisinden elde edilmelidir.

İşe alım için kişisel verilerin toplanması, adayların uygunluğunun ve kariyer potansiyellerinin değerlendirilmesi için gerekli olan bilgi ile sınırlı olmalıdır.

[913] AİHM, Bărbulescu/Romanya, No.61496/08, 5 Eylül 2017, para.121.

Tavsiye aynı zamanda her bir işçinin performansına veya potansiyeline ilişkin yargı içeren verilerden özellikle bahsetmektedir. Yargı içeren veriler, adil ve dürüst değerlendirmelere dayanmalıdır ve oluşturuluş biçimleri itibarıyla aşağılayıcı olmamalıdırlar. Bu durum, adil veri işleme ve verinin doğruluğu prensiplerine dayanmaktadır.

İşçi-iş veren ilişkisinde verilerin korunmasında özellikli bir husus ise işçilerin temsilcilerinin rolüdür. Bu tür temsilciler, kişisel verileri ancak işçilerin menfaatlerini savunabilmelerine imkan tanıması veya toplu sözleşmelerde belirtilen yükümlülüklerin yerine getirilmesi veya denetlenmesi için bu veri gerekli ise elde edebilir.

İstihdam amacıyla toplanan hassas kişisel veriler ancak özellikli hallerde ve iç hukukun belirttiği güvenceler doğrultusunda işlenebilir. İş verenler çalışanlara veya iş başvurusunda bulunanlara sağlık durumunu sorabilir veya ancak gerekli olduğunda tıbbi olarak bu kişileri muayene edebilir. Bu durum şu amaçlarla söz konusu olabilir: iş için uygunluklarını değerlendirmek, önleyici tıbbın gerekliliklerini yerine getirmek, veri sahibi veya diğer çalışanların veya bireylerin hayati menfaatlerini korumak, sosyal imkanlardan yararlanmasını sağlamak, veya adli taleplere cevap vermek. İlgili çalışan dışındaki kaynaklardan sağlık verisi, açık ve bilgilendirilmiş rızanın alınması veya iç hukukun imkan verdiği haller dışında elde edilemez.

İstihdam Tavsiye Kararı kapsamında işçiler, kişisel verilerinin işlenmesinin amaçlarını, toplanan kişisel verilerin türlerini, verilerin düzenli olarak iletileceği kişilerin bilgilerini ve bu ifşanın hukuki amacı ve sebebini bilme hakkı vardır. Elektronik haberleşmeye ancak güvenlik veya başka bir meşru neden temelinde iş yerinden erişilebilir ve bu tür bir erişim ancak işçinin bu tür haberleşmelere iş verenin erişebileceğinin bilgilendirilmesinden sonra sağlanabilir.

İşçilerin kendilerinin istihdam verilerine erişimi olması gerektiği gibi bunların değiştirilmesi veya silinmesi haklarına da sahip olması gerekmektedir. Yargı içeren verilerin işlenmesi halinde işçiler bununla beraber yargıyı onaylama hakkına da sahip olmalıdırlar. Ancak bu haklar geçici olarak iç soruşturmalar nedeniyle sınırlandırılabilirler. Bir işçinin istihdam kişisel verilerine erişimine, düzeltmesine veya silinmesine izin verilmemesi halinde yerel hukuk bu tür retlere uygun prosedürler sağlamalıdır.

9.3. Sağlık verisi

Kilit Noktalar

- Sağlık verileri hassas verilerdir ve bu nedenle özel korumadan faydalanırlar.

Veri sahibinin sağlığına ilişkin kişisel veriler, Genel Veri Koruma Regülasyonu'nun Madde 9(1) ve Modernize Edilmiş Sözleşme 108'in Madde 6'sına göre hassas veridir. Bu nedenle sağlığa ilişkin veriler hassas olmayan verilere göre daha katı bir veri işleme rejimine tabidir. Genel Veri Koruma Regülasyonu, Madde 9(2) kapsamında izin verilmedikçe genetik veri ve biyometrik verilerin olduğu gibi "sağlığa ilişkin kişisel veriler"in ("veri sahibinin geçmiş, şimdiki ve ilerideki fiziki veya akli sağlık durumuna ilişkin bilgi veren veri sahibinin sağlık durumuna ilişkin her türlü veri" olarak anlaşılmak üzere)[914] işlenmesini yasaklamaktadır. İki tip veri de "özel veri kategorileri" listesine eklenmiştir[915].

[914] Genel Veri Koruma Regülasyonu, Gerekçe 35.
[915] *A.g.e.*, Madde 2.

Örnek: Z/Finlandiya davasında[916], davacının HIV virüsü taşıyıcısı olan eski kocası birçok cinsel suç işlemiştir. Mağdurları bilerek HIV riskine maruz bıraktığı temel alınarak insan öldürme suçundan mahkum edilmiştir. Yerel mahkeme tüm yargılama ve dava dosyasının 10 yıl boyunca davacı tarafından daha uzun bir süre talebi gelmedikçe gizli tutulmasına karar vermiştir. Temyiz mahkemesi bu talebi reddetmiş ve verdiği kararda hem davacının hem eski kocasının tam adlarına yer vermiştir. AİHM, çoğu toplumda HIV'la ilişkilendirilen damgalamalar düşünülürse özellikle HIV enfeksiyonuna ilişkin bilgiler söz konusu olduğunda, sağlık verilerinin korunmasının özel ve aile hayatının gizliliğine saygı haklarının kullanılabilmesi için temelde önemli olması nedeniyle müdahaleyi demokratik bir toplumda gerekli bulmamıştır. Bu nedenle Mahkeme, davacının kimliği ve sağlık durumunu belirtilen temyiz mahkemesinin kararına erişime 10 yıllık süre dolmadan izin verilmesini AİHS'in 8inci maddesine aykırı bulmuştur.

AB hukuku kapsamında Genel Veri Koruma Regülasyonu'nun Madde(2)(h), önleyici tıp, tıbbi teşhis, bakım veya tedavi sağlanması veya sağlık hizmetlerinin yönetilmesi amaçlarıyla gerekli olması halinde sağlık verilerinin işlenmesine izin vermektedir. İşlemeye izin verilmesi ancak mesleki sır saklama yükümlülüğü altında olan sağlık profesyoneli veya denk bir yükümlülük altında olan başka kişiler tarafından gerçekleştirilmesi halinde geçerlidir[917].

Avrupa Konseyi hukuku altında 1997 Avrupa Konseyi Sağlık Verisi Tavsiye Kararı, sağlık alanında veri işlenmesine Sözleşme 108'in prensiplerini daha detaylı uygulamaktadır[918]. Teklif edilen kurallar, sağlık verisinin işlenmesindeki meşru amaçlar, sağlık verisi kullanan kişilerin mesleki gizlilik yükümlülükleri ve veri sahiplerinin şeffaflık, erişim, düzeltme ve silme haklarına ilişkin Genel Veri Koruma Regülasyonu'nun kurallarına uygundur. Bunun yanında sağlık görevlileri tarafından hukuka uygun olarak işlenen sağlık verileri, "AİHS Madde 8 kapsamında güvence altına alınan özel hayata saygı ile çelişen ifşaları önlemek için yeterli güvenceler" alınmadıkça kolluk otoritelerine aktarılması mümkün değildir[919]. İç hukuk da "keyfiyete karşı yeterli hukuki korumayı içeren ve yeterli derecede belirginlik ile düzenlenmelidir"[920].

Bunların yanında Sağlık Verisi Tavsiye Kararı doğmamış çocukların ve ehliyetsiz kişilerin sağlık verilerine ve genetik veri işlenmesine ilişkin düzenlemeler içermektedir. Genellikle anonimleştirmeyi gerektirmekle beraber bilimsel araştırmalar verilerin gerekenden uzun süre saklanması için açıkça kabul edilmiş bir sebeptir. Sağlık Verisi Tavsiye Kararı Madde 12, araştırmacıların kişisel veriye ihtiyaç duyduğu ve anonimleştirilmiş verilerin yeterli olmadığı haller için detaylı bir düzenleme teklif etmektedir.

Maskeleme, bilimsel ihtiyaçların karşılanması ve aynı zamanda ilgili hastaların korunması için uygun bir yöntem olabilir. Veri koruması bağlamında maskeleme konsepti detaylı olarak Bölüm2.1.1.'de açıklanmıştır.

---

[916] AİHM, Z/Finlandiya, No. 22009/93, 25 Şubat 1997, para. 94 ve 112; ayrıca bkz. AİHM, M.S/İsviçre, No. 20837/92, 27 Ağustos 1997; AİHM, L.L./Fransa, No. 7508/02, 10 Ekim 2006; AİHM, I/Finlandiya, No. 20511/03, 17 Temmuz 2008; AİHM, K.H ve diğerleri/Slovakya, No. 32881/04, 28 Nisan 2009; AİHM, Szuluk/Birleşik Krallık, No. 36936/05, 2 Haziran 2009.

[917] Ayrıca bkz. AİHM, Biriuk/Litvanya, No.23373/03, 25 Kasım 2008.

[918] Avrupa Konseyi, Bakanlar Komitesi (1997), Sağlık verisinin korunmasına ilişkin üye devletlere Rec(97)5 sayılı tavsiye, 13 Şubat 1997. Belirtelim ki bu Tavsiye Kararı revize edilme sürecindedir.

[919] AİHM, Avilkina ve diğerleri/Rusya, No. 1585/09, 6 Haziran 2013, para.53.

[920] AİHM, L.H./Letonya, No. 52019/07, 29 Nisan 2014, para. 59.

Genetik testler sonucundaki verilere ilişkin 2016 Avrupa Konseyi Tavsiye Kararı aynı zamanda sağlık alanındaki veri işlenmesine de uygulanmaktadır[921]. Bu tavsiye, bilgi ve iletişim teknolojilerinin tıbbi tedaviyi kolaylaştırmak için kullanıldığı eSağlık alanında büyük önem taşımaktadır. Bunun bir örneği, bir tıbbi tedavi sağlayıcıdan diğerine hastaların ebeveynlik testi sonuçlarının gönderilmesidir. Bu tavsiye, kişilerin sağlık, fiziki bütünlük, yaş veya ölümüne ilişkin risklere karşı sigortalamak için kişisel verileri sigortacılık amaçlarıyla işlenen kişilerin haklarının korunmasını amaçlamaktadır. Sigortacılar sağlığa ilişkin verileri işlemelerini meşrulaştırmalıdır ve işleme, ilgili riskin niteliğine ve önemine orantılı olmalıdır. Bu tür verilerin işlenmesi kişilerin rızasına tabidir. Sigortacılar aynı zamanda sağlığa ilişkin verilerin saklanmasında uygulanan güvenceler getirmelidir.

Belgelendirilen araştırma alanlarında yeni ilaçların hastalar üzerindeki etkilerin değerlendirilmesini kapsayan klinik çalışmalarda dikkate değer olası veri koruma sonuçları söz konusudur. İnsan kullanımı için tıbbi ürünlerin klinik çalışmaları, insan kullanımı için tıbbi ürünlere dair klinik çalışmalara ilişkin ve 2001/20/EC sayılı Direktifi kaldıran Avrupa Parlamentosu ve Konseyi'nin 16 Nisan 2014 tarihli ve (EU)536/2014 sayılı Regülasyonu (Klinik Çalışmalar Regülasyonu)[922] ile düzenlemektedir. Klinik Çalışmalar Regülasyonu'nun temel unsurları şu şekildedir:

- AB portalı aracılığı ile geliştirilmiş uygulama prosedürü[923];
- Klinik çalışmalar için uygulamanın değerlendirmesi için son gün belirlemeleri[924];
- Üye Devletlerin hukuklarına uygun ve değerlendirmenin parçası olan bir etik komitesi[925]; ve
- Klinik çalışmaların ve bunların sonuçlarının şeffaflığının artırımı[926].

Genel Veri Koruma Regülasyonu, klinik çalışmalarda bilimsel araştırmalara katılım için verilen rıza nezdinde (EU)536/2014 sayılı Regülasyon'un uygulanacağını belirtmektedir[927].

Sağlık sektöründe kişisel verilere ilişkin AB seviyesinde beklemekte olan birçok başka mevzuat ve girişim söz konusudur[928].

Elektronik Sağlık Kayıtları

Elektronik sağlık kayıtları, "bir kişinin geçmiş veya mevcut fiziki ve akli sağlık durumunun bulunduğu ve bu verilerin tıbbi tedaviler ve diğer yakından ilgili amaçlar için hazır bulundurulduğu elektronik formattaki kapsamlı bir sağlık kaydı veya benzer belgelendirme"

[921] Avrupa Konseyi, Bakanlar Komitesi (2016), genetik testler sonucundaki veriler dahil olmak üzere sigorta amacıyla sağlığa ilişkin kişisel verilerin işlenmesine ilişkin üye devletlere Rec(2016)8 sayılı Tavsiye Kararı, 26 Ekim 2016.
[922] insan kullanımı için tıbbi ürünlere dair klinik çalışmalara ilişkin ve 2001/20/EC sayılı Direktifi kaldıran Avrupa Parlamentosu ve Konseyi'nin 16 Nisan 2014 tarihli ve (EU)536/2014 sayılı Regülasyonu (Klinik Çalışmalar Regülasyonu), OJ 2014 L 158.
[923] Klinik Çalışmalar Regülasyonu, Madde 5(1).
[924] *A.g.e.*, Madde 5(2)-(5).
[925] *A.g.e.*, Madde 2(11).
[926] *A.g.e.*, Madde 9(1) ve Gerekçe 67.
[927] Genel Veri Koruma Regülasyonu, Gerekçe 156 ve 161.
[928] EDPS (2013), Komisyon'un "eSağlık Aksiyon Planı 2012-2020 – 21inci yüzyıl için inovatif sağlık hizmeti" Bildirimine ilişkin Avrupa Veri Koruma Denetçisi'nin Görüşü, Brüksel, 27 Mart 2013.

olarak tanımlanmaktadır[929]. Elektronik sağlık kayıtları, hastaların sağlık geçmişinin elektronik versiyonlarıdır ve bu kişilere ilişkin tıbbi geçmiş, problemler ve sağlık koşulları, ilaçlar ve tedaviler gibi tahlil ve laboratuvar sonuçları ve kayıtları gibi klinik verileri içerebilmektedir. Tüm kayıtlardan salt çıktı veya özetlere kadar değişebilen bu elektronik dosyalara genel pratisyen hekimler, eczacılar ve diğer sağlık hizmetleri profesyonellerince erişilebilmektedir. "eSağlık" konsepti de bu sağlık kayıtlarına değinmektedir.

Örnek: Bay A, sigortacı olan B şirketi ile bir sigorta poliçesi imzalamıştır. Sigortacı, Bay A'dan, mevcut sağlık sorunları veya hastalıklar gibi birtakım sağlıkla ilgili bilgiler toplamaktadır. Sigortacı 'nın sağlığa ilişkin kişisel verilerini diğer verilerden ayrı depolamalıdır. Sigortacı aynı zamanda sağlığa ilişkin kişisel verileri diğer kişisel verilerden ayrı saklamalıdır. Bu durum, sadece A'nın dosyası ile ilgilenen kişinin A'nın sağlığa ilişkin verilerine erişebileceği anlamına gelmektedir.

Ancak erişim, elektronik sağlık dosyalarından düzgün depolama ve veri sahibi tarafından erişim gibi birtakım veri koruma problemleri doğabilmektedir.

Elektronik sağlık kayıtlarına ek olarak, mobil sağlığın (mSağlık) sağlık hizmetini değiştirebilecek, etkinliğini ve niteliğini artırabilecek bir potansiyeli gelişmekte ve hızlıca büyümekte olan bir alan olduğu düşünülerek 10 Nisan 2014'te Avrupa Komisyonu mSağlık üzerine içerisinde teklifler bulunduran bir çalışma yayınlamıştır. Bu terim, mobil telefon, hasta takip cihazları, kişisel dijital asistan ve diğer kablosuz aletler ile tıbbi cihazlara veya sensörlere bağlanabilecek uygulamalar (örneğin sağlık durumunun iyi olmasına ilişkin uygulamalar) dahil olmak üzere mobil cihazlar tarafından desteklenen tıbbi ve kamu sağlığı uygulamalarını kapsamaktadır[930]. Çalışma, mSağlığın gelişmesinin ortaya çıkarabileceği kişisel verilerin korunması hakkına ilişkin risklerin altını çizmektedir ve sağlık verisinin hassas niteliği göz önünde bulundurulduğunda bu gelişmenin hasta verileri için, şifreleme ve güvenlik risklerinin yönetilmesi için uygun hasta doğrulamaları gibi spesifik ve uygun güvenlik önlemleri içermesi gerektiğini belirtmektedir. Veri sahibinin bilgilendirilmesi yükümlülüğü, güvenlik ve kişisel verilerin hukuka uygun olarak işlenmesi dahil olmak üzere kişisel veri koruma kuralları ile uyumluluk, mSağlık çözümlerine güvenin oluşturulmasında çok önemlidir[931]. Bu amaçla endüstri tarafından, veri koruma, öz düzenleme ve ortak düzenleme, bilgi ve iletişim teknolojileri ve sağlık hizmeti alanlarında uzman temsilcileri barındıran geniş kapsamlı ilgililerin girdileri temelinde Davranış Kuralları düzenlenmiştir[932]. El kitabının hazırlanması sırasında taslak davranış kuralları Madde 29 Çalışma Grubu'nun yorumuna sunulmuş ve resmi onayını beklemektedir.

9.4. Araştırma ve istatistiki amaçlarla veri işlenmesi

Kilit Noktalar

[929] Elektronik sağlık kaydının sınır ötesi birlikte çalışabilmesine ilişkin 2 Temmuz 2008 tarihli Komisyon Tavsiye Kararı, Madde 3(c).
[930] Avrupa Komisyonu (2014), Mobil Sağlığa (mSağlık) ilişkin teklifli belge, COM(2014) 219 final, Brüksel, 10 Nisan 2014.
[931] *A.g.e.*, sf.8.
[932] Mobil sağlık uygulamaları için gizliliğe ilişkin taslak Davranış Kuralları, 7 Haziran 2016.

- İstatistiki, bilimsel veya tarihi araştırma amaçları için toplanan veriler, başka bir amaç için kullanılamaz.

- Herhangi bir amaçla hukuka uygun olarak toplanan veriler, yeterli güvencelerin mevcut olması halinde istatistiki, bilimsel veya tarihi araştırma amaçları ile işlenebilir. Bu amaçla verilerin üçüncü taraflara aktarımından önce anonimleştirilmesi veya maskelenmesi bu güvenceleri sağlayabilir.

AB hukuku verilerin, veri sahiplerinin hakları ve özgürlükleri için yeterli güvencelerin mevcudiyeti halinde istatistiki, bilimsel veya tarihi araştırma amaçları ile işlenmesine izin vermektedir. Bunlar maskelemeyi içerebilmektedir[933]. Araştırmanın meşru amaçlarının gerçekleşmesini imkansız hale getirmesi veya buna ciddi şekilde zarar vermesi halinde AB hukuku veya iç hukuk veri sahiplerinin haklarının birtakım uygulama dışı tutulmalara tabi olmasını düzenleyebilir[934]. Bu istisnalar veri sahiplerinin erişim hakkı, düzeltme hakkı, işlemenin kısıtlanması hakkı ve itiraz etme hakkına ilişkin olabilir.

Veri sorumlusu tarafından hukuka uygun olarak herhangi bir amaçla toplanan verilerin aynı sorumlu tarafından kendi istatistiki, bilimsel veya tarihi araştırma amaçları için tekrar kullanılması mümkün olmakla beraber bu veriler, veri sahibinin rızası olduğu veya iç hukuk tarafından özellikle öngörüldüğü haller dışında, üçüncü taraflara istatistiki, bilimsel veya tarihi araştırma amaçları için aktarılmadan önce bağlama göre anonimleştirme veya maskeleme gibi tedbirlere tabi tutulmalıdır. Maskelemeye konu veriler, anonim verilerin aksine, Genel Veri Koruma Regülasyonu'ne tabi olmaya devam etmektedir[935].

Dolayısıyla düzenleme, araştırma gelişmelerinin kısıtlanmasını engellemek ve TFEU madde 179'de belirtilen Avrupa araştırma alanına ulaşma amacına uygunluk için, genel veri koruma kurallarına ilişkin araştırmaya özel uygulamalar öngörmektedir. Teknolojik gelişmeler ve göstergeler, temel araştırma, uygulamalı araştırma ve özel fonlu araştırmalar dahil olmak üzere bilimsel araştırma amaçları için kişisel verilerin işlenmesine dair geniş bir tanım öngörmektedir. Ayrıca kayıtlardaki veri topluluklarının önemine ve veri toplanması anında kişisel verilerin bilimsel araştırma amacıyla takip eden işlemelerinin tamamen belirlenmesindeki olası zorluğa değinmektedir[936]. Bu nedenle düzenleme, yeterli güvencelerin sağlanması halinde veri sahiplerinin rızasını aramaksızın bu amaçlarla kişisel verilerin işlenmesine izin vermektedir.

İstatistiki amaçlarla verilerin kullanılmasına önemli bir örnek, resmi istatistiklere ilişkin iç hukuk veya AB hukuku uyarınca yerel ve AB istatistik kurumları tarafından elde edilen resmi istatistiklerdir. Bu kanunlara göre, vatandaşlar ve işletmeler genellikle ilgili istatistik kurumuna veri paylaşımında bulunmakla yükümlüdürler. İstatistik kuruluşlarında çalışan memurlar, verilerin istatistik kurumlarına verilmesinde gereken yüksek seviyede vatandaş güveni için gereklilikleri nedeniyle düzgün bir şekilde uyulması gereken özel mesleki sır yükümlülükleri ile bağlıdırlar[937].

---

[933] Genel Veri Koruma Regülasyonu, Madde 89(1).
[934] *A.g.e.*, Madde 89(2).
[935] *A.g.e.*, Gerekçe 26.
[936] *A.g.e.*, Gerekçe 33, 157 ve 159.
[937] *A.g.e.*, Madde 90.

Avrupa istatistiklerine ilişkin (EC)223/2009 sayılı Regülasyon (Avrupa İstatistik Regülasyonu) resmi istatistikler bağlamında veri korumaya ilişkin temel kuralları belirler ve bu nedenle iç hukuk seviyesinde getirilen resmi istatistik düzenlemelerine ilişkin olarak dikkate alınabilir[938]. Düzenleme, resmi istatistiki faaliyetlerin yeterli derecede net hukuki temeli olması gerektiğine ilişkin prensibi korumaktadır[939].

Örnek: Huber/ Bundesrepublik Deutschland davasında Almanya'ya taşınan bir Avusturyalı iş adamı, yabancı vatandaşların kişisel verilerin Almanya otoriteleri tarafından toplanması ve merkezi kayıtta aynı zamanda istatistiki amaçlarla tutulması Veri Koruma Direktifi kapsamındaki haklarını ihlal ettiğine ilişkin şikayette bulunmuştur. 95/46 sayılı Direktif'in tüm Üye Devletlerde eşit seviyede veri koruma sağlamayı hedeflediği düşünülerek CJEU, AB içerisinde yüksek seviye bir koruma sağlamak amacıyla, Madde 7(e)'de geçen gereklilik konseptinin Üye Devletler arasında değişemeyeceğini belirtmiştir. Bu nedenle bu konseptin AB hukuku içerisinde kendi bağımsız anlamı vardır ve 95/46 sayılı Direktif'in amacını tam olarak yansıtacak şekilde yorumlanmalıdır. İstatistiki amaçlarda esasen anonim verilerin kullanılmasının gerektiğini belirterek CJEU, Alman sicilinin Madde 7(e) kapsamında gereklilik şartına uygun davranmadığına hükmetmiştir.

Avrupa Konseyi bağlamında ise kamu yararı olduğu hallerde verilerin bilimsel, tarihi veya istatistiki amaçlarla işlenmesi mümkündür ve yeterli güvencelere tabi olmalıdır[940]. Verilerin istatistiki amaçlarla işlenmesinde veri sahiplerinin hakları da, hak ve özgürlüklerinin ihlal edilmesine ilişkin görülür bir risk olmaması halinde kısıtlanabilmektedir[941].

1997'de düzenlenen İstatistiki Veri Tavsiye Kararı, kamu ve özel sektörde istatistiki faaliyetlerin gerçekleştirilmelerini kapsamaktadır[942].

İstatistiki amaçlarla veri sorumlusu tarafından toplanan veriler, bir başka amaç için kullanılamazlar. İstatistiki olmayan amaçlarla toplanan veriler istatistiki kullanımlar için uygundur. İstatistiki Veri Tavsiye Kararı ayrıca, sadece istatistiki amaçlarla olduğu hallerde verilerin üçüncü taraflarla paylaşılmasına izin vermektedir. Bu tür durumlarda taraflar istatistik için meşru ikincil kullanımların kapsamı konusunda anlaşmalı ve bunları yazıya dökmelidirler. Bu durum -gerekmesi halinde- veri sahibinin rızasının yerine geçmeyeceği için, verinin kötüye kullanılması riskinin azaltılması için iç hukuklarda belirlenen, aktarımdan önce verileri anonimleştirme veya maskeleme gibi uygun güvenceler gerekmektedir.

İstatistiki araştırma görevlileri, iç hukuk uyarınca -resmi istatistikler için genellikle söz konusu olan- özel mesleki sır saklama yükümlülükleri altında olmalıdır. Bu yükümlülük aynı zamanda, veri sahiplerinden veya diğer kişilerden veri toplamakla görevliler ise, raportörler ve diğer kişisel veri toplayanları da kapsamalıdır.

---

[938] Avrupa Parlamentosu ve Konseyi'nin 11 Mart 2009 tarihli ve (EC)223/2009 sayılı Regülasyonu

[939] Bu prensip, Avrupa İstatistik Regülasyonu'nun 11inci maddesine uygun olarak kişisel verilerin temkinli kullanımı dahil olmak üzere resmi istatistiklerin nasıl gerçekleştirileceğine dahil etik yönlendirme içerecek Eurostat'ın Davranış Kuralları'nda daha detaylandırılacaktır.

[940] Modernize Edilmiş Sözleşme 108, Madde 5(4)(b).

[941] *A.g.e.*, Madde 11(2).

[942] Avrupa Konseyi, Bakanlar Komitesi (1997), istatistiki amaçlarla toplanan ve işlenen kişisel verilerin korunmasına ilişkin üye devletlere Rec(97)18 sayılı Tavsiye Kararı, 30 Eylül 1997.

Kişisel veri kullanarak istatistiki araştırma yapılmasına kanunen izin verilmiyor ise bunu meşrulaştırmak için veri sahiplerinin verilerinin işlenmesine rıza göstermeleri veya bu kişilere itiraz etme imkanı tanınması gerekebilir. Kişisel veriler raportörler tarafından istatistiki amaçlarla toplanmış ise bu kişiler iç hukuk uyarınca verilerin sağlanmasının zorunlu olup olmadığına ilişkin açıkça bilgilendirilmelidirler.

İstatistiki bir çalışmanın anonimleştirilmiş veriler kullanılarak gerçekleştirilmesi mümkün değil ise ve kişisel verilere ihtiyaç varsa; bu amaçla toplanan veriler en yakın zamanda anonimleştirilmelidir. En azından istatistiki çalışmanın sonuçları, kesinlikle bir risk teşkil etmediği haller dışında, herhangi bir veri sahibinin belirlenebilmesine elverişli olmamalıdır.

İstatistiki analizin tamamlanmasından sonra, kullanılan kişisel veriler silinmeli veya anonimleştirilmelidir. Bu gibi durumlarda İstatistiki Veri Tavsiye Kararı, kişinin belirlenmesine ilişkin verilerin diğer verilerden ayrı saklanması gerektiğini tavsiye etmektedir. Bu demektir ki, mesela, şifreleme anahtarı veya tanımlayıcı eş anlamlılarının bulunduğu liste diğer verilerden ayrı depolanmalıdır.

9.5. Finansal veri

Kilit Noktalar

- Modernize Edilmiş Sözleşme 108 veya Genel Veri Koruma Regülasyonu kapsamında finansal veriler hassas veri olarak nitelendirilmemekle birlikte bunların işlenmesi, doğruluğun ve veri güvenliğinin sağlanması için özel güvencelerin alınmasını gerektirmektedir.

- Elektronik ödeme sistemlerinin, tasarımdan önce veya sonra gizlilik veya veri koruma gibi özellikle yerleşik veri korumaya ihtiyacı vardır.

- Bu alana özgü veri koruma problemleri, kimlik doğrulama mekanizmalarının kullanılması gerekmesi nedeniyle ortaya çıkabilmektedir.

Örnek: Michaud/Fransa davasında[943], Fransız avukat olan davacı, Fransız hukuku altında müvekkillerinin olası para aklama faaliyetlerine ilişkin şüphelerini raporlama yükümlülüğünü gündeme getirmiştir. AİHM, avukatların, profesyonel iletişimleri aracılığı ile sahip oldukları başka bir kişiye ait bilgileri idari otoritelere raporlamakla yükümlü tutulmasının avukatların, profesyonel veya iş niteliğindeki faaliyetleri de kapsaması nedeniyle AİHS Madde 8 kapsamında haberleşme ve özel hayatlarına saygı haklarına müdahale olduğunu belirtmiştir. Ancak müdahale hukuka uygun olarak yapılmıştır ve düzensizliğin ve suçun önlenmesi gibi meşru bir amaç uğruna gerçekleşmiştir. Avukatların şüpheli aktiviteleri ancak oldukça sınırlı hallerde bildirmeleri gerekmesi nedeniyle AİHM bu yükümlülüğü orantılı bulmuştur ve Madde 8'in ihlal edilmediğini belirtmiştir.

[943] AİHM, Michaud/Fransa, No.12323/11, 6 Aralık 2012. Ayrıca bkz. AİHM, Niemietz/Almanya, No. 13710/88, 16 Aralık 1992, para. 29, ve AİHM, Halford/Birleşik Krallık, No. 20605/92, 25 Haziran 1997, para. 42.

Örnek: M.N. ve diğerleri/San Marino davasında[944], İtalyan vatandaşı davacı, soruşturma altında olan bir şirket ile emanet sözleşmesi akdetmiştir. Bu durum, soruşturma altındaki şirketin (elektronik) belgelerinin kopyalarının aranması ve bunlara el konulması anlamına gelmektedir. Davacı, San Marino mahkemesine şikayette bulunarak kendisi ile iddia edilen suçlar arasında hiçbir bağ olmadığını ileri sürmüştür. Ancak mahkeme, davacının "ilgili taraf" olmaması nedeniyle bu şikayeti kabul edilemez bulmuştur. AİHM, davacının bir "ilgili taraf" ile karşılaştırıldığında adli koruma anlamında önemli derecede aleyhine olduğunu belirtmekle beraber verileri halen arama ve el koyma operasyonlarına konu olmaktadır. Bu nedenle Mahkeme Madde 8'in ihlal edildiğine karar vermiştir.

Örnek: G.S.B./İsviçre davasında[945], davacının banka hesabı detayları ABD veri otoritesine, ABD ile İsviçre arasındaki idari iş birliği anlaşması temelinde gönderilmiştir. AİHM, davacının gizlilik hakkına müdahalenin hukuken öngörülmesi ve meşru bir amaç için gerçekleştirilmesi ve ilgili kamu yararı ile orantılı olduğu nedenleri ile bu aktarımın Madde 8'in ihlalini oluşturmadığına karar vermiştir.

Ödemeye ilişkin (Sözleşme 108'de belirtildiği üzere) genel veri koruma çerçevesindeki başvurular, Avrupa Konseyi tarafından 1990 tarihli Rec(90)19 sayılı Tavsiye Kararı ile geliştirilmiştir[946]. Bu tavsiye kararı, özellikle ödeme kartları ile yapılan ödemeler bağlamında verilerin hukuka uygun olarak toplanılması ve kullanılmasının kapsamını netleştirmektedir. Ayrıca yerel kanun koyuculara, ödeme verilerinin üçüncü taraflarla paylaşılmasına, verinin saklanmasına dair sınırlar, şeffaflık, veri güvenliği ve sınırlar arası veri akışına ve denetim ve çarelere ilişkin tavsiyelerde bulunmaktadır. Avrupa Konseyi aynı zamanda, vergi verilerinin aktarımı sürecine dair öneriler ve dikkate alınması gereken konuları içeren vergi verilerinin aktarımına ilişkin bir Görüş[947] hazırlamıştır.

AİHM, özellikle bireylerin banka hesaplarına ilişkin detaylar olmak üzere finansal verinin aktarımına, kanun tarafından öngörülmüş olması, meşru bir amaç uğruna olması ve ilgili kamu yararı ile oranlı olması hallerinde AİHS Madde 8 altında izin vermektedir[948].

AB hukuku nezdinde, kişisel verilerin işlenmesini içeren elektronik ödeme sistemleri, Genel Veri Koruma Regülasyonu'ne uygun olmalıdır. Bu nedenle bu sistemler tasarım ile ve varsayılan olarak veri koruması ilkelerini sağlamak zorundadır. Tasarımda veri koruması, veri sorumlularını, veri koruma prensiplerinin yerine getirilmesi için uygun teknik ve idari tedbirleri uygulamakla yükümlü tutar. Varsayılan olarak veri koruması, veri sorumlularının sadece spesifik amaç için gerekli olan kişisel verilerin işlenmesini güvence altına alması anlamında gelmektedir (bkz. Bölüm 4.4). Finansal veriler açısından CJEU, aktarılmış vergi verisinin kişisel veri sayılacağını belirtmiştir[949]. Madde 29 Veri Koruma Çalışma Grubu buna ilişkin Üye

[944] AİHM, M.N. ve diğerleri/San Marino, No. 28005/12, 7 Temmuz 2015.
[945] AİHM, G.S.B./İsviçre, No. 28601/11, 22 Aralık 2015.
[946] Avrupa Konseyi, Bakanlar Komitesi (1990), ödeme ve diğer ilgili operasyonlar için kullanılan kişisel verilerin korunmasına ilişkin R(90)19 sayılı Tavsiye Kararı, 13 Eylül 1990.
[947] Avrupa Konseyi, Sözleşme 108'in Danışman Komitesi (2014), idari ve vergisel amaçlarla devletler arası verilerin otomatik aktarımı mekanizmalarına veri korumanın etkilerine ilişkin görüş, 4 Haziran 2014.
[948] AİHM, G.S.B./İsviçre, No.28601/11, 22 Aralık 2015.
[949] CJEU, C-201/14, Smaranda Bara ve diğerleri/Casa Naţională de Asigurări de Sănătate ve diğerleri, 1 Ekim 2015, para. 29.

Devletlere yönelik, otomatik yollarla vergi amaçlı otomatik kişisel veri aktarımında veri koruma kurallarına uygunluğun sağlanması için kriterler dahil olmak üzere rehber yayınlamıştır[950]. Buna ek olarak finans pazarını ve kredi kuruluşları ile yatırım şirketlerinin faaliyetlerini düzenlemek amacıyla çıkartılan birçok hukuki enstrüman mevcuttur[951]. Diğer hukuki araçlar, içeriden bilgi alıp satma ile pazarın manipüle edilmesi ile mücadeleyi desteklemektedir[952]. Veri korumasına etkisi olan temel alanlar şu şekildedir:

- Finansal işlemlerin kayıtlarının saklanması;
- Kişisel verilerin üçüncü ülkelere aktarılması;
- Yetkili otoritelerin telefon ve veri trafiği kayıtlarını talep etme yetkileri dahil olmak üzere telefon konuşmalarının veya elektronik haberleşmelerin kaydedilmesi;
- Yaptırımların ilan edilmesi dahil olmak üzere kişisel bilgilerin ifşa edilmesi;
- Yerinde denetim ve belgelere el konulması için özel mülke girilmesi dahil olmak üzere yetkili otoritelerin denetim ve soruşturma yetkileri;
- Bilgi ifşası (whistle-blowing) gibi ihlal bildirim mekanizmaları; ve
- Üye Devletlerin yetkili otoriteleri ile Avrupa Menkul Kıymetler ve Piyasalar Otoritesi (ESMA) arasında iş birliği.

Kaçınılmaz bir şekilde kişisel veri akışına neden olan bu alandaki diğer problemlere de, veri sahiplerinin finansal durumlarına ilişkin veri toplanması[953] ve bankacılık transferleri ile sınır ötesi ödemeler dahil olmak üzere ayrıca değinilmiştir[954].

---

[950] Madde 29 Veri Koruma Çalışma Grubu (2015), vergi amaçları ile kişisel verilerin devletler arasında otomatik değişimine ilişkin WP29'un bildirgesi, 14/EN WP 230.

[951] Finansal araçlar pazarlarına ilişkin ve 2002/92/EC ve 2011/61/EU sayılı Direktifleri değiştiren Avrupa Parlamentosu ve Konseyi'nin 15 Mayıs 2014 tarihli ve 2014/65/EU sayılı Direktifi, OJ 2014 L 173; Finansal araçlar pazarlarına ilişkin ve (EU)648/2012 sayılı Regülasyonu değiştiren Avrupa Parlamentosu ve Konseyi'nin 15 Mayıs 2014 tarihli (EU)600/2014 sayılı Regülasyonu, OJ 2014 L 173; kredi kuruluşlarının faaliyetlerine erişime ve kredi kuruluşları ile yatırım şirketlerinin dikkatli denetimine ilişkin, 2002/87/EC sayılı Direktifi değiştiren ve 2006/48/EC sayılı Direktifi kaldıran Avrupa Parlamentosu ve Konseyi'nin 26 Haziran 2013 tarihli ve 2013/36/EU sayılı Direktifi, OJ 2013 L 176.

[952] Piyasa bozucu eylemlere ilişkin (piyasa bozucu eylemler regülasyonu) ve Avrupa Parlamentosu ve Konseyi'nin 2003/6/EC sayılı Direktifi ile Komisyonun 2003/124/EC, 2003/125/EC ve 2004/72/EC sayılı Direktiflerini kaldıran Avrupa Parlamentosu ve Konseyi'nin 16 Nisan 2014 tarihli ve (EU)596/2014 sayılı Regülasyonu, OJ 2014 L 173.

[953] Kredi derecelendirme kurumlarına ilişkin Avrupa Parlamentosu ve Konseyi'nin 16 Eylül 2009 tarihli ve 1060/2009 sayılı Regülasyonu, OJ 2009 L 302, ve yakın zamanda Avrupa Denetim Otoritesinin (Avrupa Sigorta ve Meslek Sigortası Otoritesi) ve Avrupa Denetim Otoritesi (Avrupa Menkul Kıymetler ve Piyasalar Otoritesi) yetkilerine ilişkin 2003/71/EC ve 2009/138/EC sayılı Direktifleri ve (ECI1060/2009, (EU)1094/2010 ve (EU) 1095/2010 sayılı Regülasyonları değiştiren Avrupa Parlamentosu ve Konseyi'nin 16 Nisan 2014 tarihli ve 2014/51/EU sayılı Direktifi, OJ 2014 L 153; Kredi puanlama kurumlarına ilişkin 1060/2009 sayılı Regülasyonu değiştiren Avrupa Parlamentosu ve Konseyi'nin 462/2013 sayılı ve 12 Mayıs 2013 tarihli Regülasyonu, OJ 2013 L 146.

[954] Merkezi kuruluşlara bağlı bankalara, birtakım öz kaynaklar, büyük riskler, denetim düzenlemelere ve kriz yönetimine ilişkin 2006/48/EC, 2006/49/EC ve 2007/64/EC sayılı Direktifleri değiştiren Avrupa Parlamentosu ve Konseyi'nin 16 Eylül 2009 tarihli ve 2009/111/EC sayılı Direktifi tarafından değiştirilmiş iç pazarda ödeme hizmetlerine ilişkin, 97/7/EC, 2002/65/EC, 2005/60/EC ve 2006/48/EC sayılı Direktifleri değiştiren ve 97/5/EC sayılı Direktifi kaldıran Avrupa Parlamentosu ve Konseyi'nin 13 Kasım 2007 tarihli ve 2007/64/EC sayılı Direktifi, OJ 2007 L 319,

10. Kişisel Verilerin Korunmasında Güncel Zorluklar

Dijital çağ ya da bilgi teknolojisi çağı, bilgisayar, internet ve dijital teknolojilerin yaygın kullanımıyla karakterize edilmiştir. Kişisel veriler de dahil olmak üzere çok büyük miktarda verinin toplanmasını ve işlenmesini içermektedir. Kişisel verilerin küreselleşmiş bir ekonomide toplanması ve işlenmesi, sınır ötesi veri akışlarının sayıca artması anlamına gelmektedir. Bu tür işleme faaliyetleri günlük yaşamda önemli ve görünür faydalar sağlayabilir: arama motorları kayda değer miktarda bilgi ve birikime erişimi kolaylaştırır, sosyal ağ hizmetleri, dünyanın dört bir yanındaki insanların iletişim kurmalarını, toplumsal, çevresel ve siyasal meseleler hakkındaki görüşlerini ifade etmelerini ve destek toplamalarını sağlarken, şirketler ve tüketiciler ekonomiyi canlandıran etkili ve verimli pazarlama tekniklerinden yararlanır. Teknoloji ve kişisel verilerin işlenmesi, devlet makamları için suç ve terörle mücadelede vazgeçilmez birer araçtır. Benzer şekilde, büyük veri – örüntüleri tanımlamak ve davranışları öngörmek için büyük miktarlarda bilginin toplanması, saklanması ve analizi – "toplum için üretkenliği, kamu sektörü performansını ve sosyal katılımı arttıran önemli bir değerli kaynağı olabilir"[955].

Çok sayıda faydalarına rağmen, büyük miktarlarda kişisel bilgi toplanıp giderek daha karmaşık ve kesif yollarla işlendiğinden, dijital çağ ayrıca gizlilik ve veri korunması konusunda da zorluklar doğurmaktadır. Teknolojik ilerleme, kolayca kontrol edilebilecek ve örüntüleri aramak için daha fazla analiz edilebilecek veri kümelerinin geliştirilmesine veya insan davranışına ve özel hayata dair benzersiz bir içgörü sağlayabilen algoritmalara dayanan kararların benimsenmesine yol açmıştır.[956]

Yeni teknolojiler güçlüdür ve özellikle yanlış ellere düşerse tehlikeli olabilir. Bu teknolojilerden istifade edebilecek kitlesel gözetim faaliyetleri yürüten devlet makamları, bu teknolojilerin bireylerin hakları üzerindeki belirgin etkisine bir örnektir. Edward Snowden'ın, 2013'te, bazı eyaletlerde istihbarat teşkilatlarının büyük ölçekli internet ve telefon gözetim programlarının işletilmesi konusundaki ifşaatı, gözetleme faaliyetlerinin mahremiyet, demokratik yönetim ve ifade özgürlüğü için tehlikeleri hakkında önemli endişelere yol açtı. Kişisel bilgilerin küresel olarak saklanmasına ve işlenmesine izin veren kitlesel gözetim ve teknolojiler ve verilere toplu erişim özel hayatın gizliliği hakkının özüne dokunabilir.[957] Ayrıca, siyasi kültür üzerinde olumsuz bir etkiye, demokrasi, yaratıcılık ve inovasyon üzerinde ise ürpertici bir etkiye sahip olabilir.[958] Devletin sürekli olarak vatandaşların davranış ve hareketlerini takip edip analiz ediyor olabileceği korkusu, onların belirli konularda görüşlerini ifade etmelerini engelleyebilir ve ihtiyat ve temkinle sonuçlanabilir.[959] Bu zorluklar, yeni teknolojilerin toplum üzerindeki potansiyel etkilerini analiz etmek için bir dizi kamu makamını, araştırma merkezini ve sivil toplum kuruluşunu teşvik etmiştir. 2015 yılında, Avrupa Veri

[955] Avrupa Konseyi, Sözleşme 108 Danışma Kurulu, *Büyük veri dünyasında kişisel verilerin işlenmesi hususunda bireylerin korunmasına ilişkin rehber*, T-PD(2017)01, Strazburg, 23 Ocak 2017.

[956] Avrupa Parlamentosu, Büyük verinin temel haklar üzerindeki etkileri hakkında karar: gizlilik, veri koruma, ayrımcılık yasağı, güvenlik ve hukuki yaptırım, (P8_TA-PROV(2017)0076, Strazburg, 14 Mart 2017.

[957] Bkz. Birleşmiş Milletler, Genel Kurul, *Terörle mücadelede insan haklarının ve temel özgürlüklerin desteklenmesi ve korunmasına ilişkin Özel Raportör raporu*, Ben Emmerson, A/69/397, 23 Eylül 2014, para. 59. Ayrıca bkz. AİHM, *Kitle gözetimi hakkında bilgi notu*, Temmuz 2017.

[958] Avrupa Veri Koruma Denetçisi (2015), Büyük verinin zorluklarının üstesinden gelmek, Görüş 7/2015, Brüksel, 19 Kasım 2015.

[959] Özellikle bkz. Avrupa Birliği Adalet Divanı, C-293/12 ve C-594/12, *Digital Rights Ireland Ltd/İletişim, Denizcilik ve Doğal Kaynaklar Bakanlığı ve Diğerleri ve Kärntner Landesregierung ve Diğerleri* [Yüce Divan], 8 Nisan 2014, para. 37.

Koruma Denetçisi, büyük verinin ve Nesnelerin İnterneti'nin etik üzerindeki etkisini değerlendirmeyi amaçlayan birçok girişim başlatmıştır. Özellikle, "AB'ye teknolojinin toplum ve ekonomi için faydalarını fark etme imkanı veren ve aynı zamanda bireylerin haklarını ve özgürlüklerini, özellikle de özel hayatın gizliliği ve verilerin korunması haklarını güçlendiren, dijital etik üzerine açık ve bilgiye dayalı bir tartışma"yı teşvik etmeyi amaçlayan bir Etik Danışma Grubu kurmuştur.[960]

Kişisel verilerin işlenmesi aynı zamanda şirketlerin elindeki güçlü bir araçtır. Günümüzde, bir kişinin sağlık veya mali durumunu gösteren ayrıntılı bilgiler, daha sonrasında şirketler tarafından bireyler hakkında önemli kararlar almak için kullanılan uygulanacak sağlık sigortası primi veya kredibilite gibi bilgiler ortaya çıkabilir. Verilerin işlenme teknikleri, politikacılar veya kurumlar tarafından seçimleri etkilemek için kullanıldığında – örneğin seçmenlerin iletişiminin "mikro-hedefleme" vasıtasıyla – demokratik süreçler üzerinde de etkili olabilir. Başka bir deyişle, mahremiyet başlangıçta bireyleri kamu makamlarının haksız müdahalesine karşı koruma hakkı olarak algılanırken, modern çağda özel aktörlerin güçleri tarafından da tehdit edilebilir. Bu, bireylerin günlük yaşamlarını etkileyen kararlarda teknolojinin kullanımı ve öngörücü analizler hakkında sorular ortaya koymakta ve herhangi bir kişisel veri işlenmesinin temel hak gereksinimlerine saygılı olmasını sağlama ihtiyacını güçlendirmektedir.

Verilerin korunması esasında teknolojik, toplumsal ve siyasi değişime bağlıdır. Gelecekteki zorlukların kapsamlı bir listesi bu nedenle yapılamaz. Bu bölüm, büyük veri, internet sosyal ağlar ve AB'nin Dijital Ortak Pazarı ile ilgili belirli alanlara değinmektedir. Bu alanların verilerin korunması perspektifinden eksiksiz bir değerlendirmesi olmayıp, yeni veya revize edilmiş insan faaliyetleri ile verilerin korunması arasındaki muhtemel etkileşimlerin çokluğunu vurgulamaktadır.

10.1. Büyük veri, algoritmalar ve yapay zeka

Kilit noktalar

- Bilgi ve iletişim teknolojilerindeki yıkıcı yenilikler, toplumsal ilişkilerin, iş dünyasının, özel ve kamu hizmetlerinin dijital olarak birbirine bağlandığı yeni bir yaşam tarzı şekillendirmektedir ve bu sayede çoğu kişisel olmak üzere giderek artan miktarda veri üretmektedir.

- Hükümetler, teşebbüsler ve vatandaşlar gittikçe artan şekilde, verilerin kendileri için değerli varlıklar haline geldiği veri odaklı bir ekonomide faaliyet göstermektedir.

- Büyük veri kavramı, hem veriye hem de onunla ilgili mantıksal analize işaret etmektedir.

- Büyük veri analiziyle işlenmiş kişisel veriler AB ve Avrupa Konseyi mevzuatı dahilindedir.

- Verilerin korunması kurallarına ve haklarına getirilen istisnalar, seçilen haklarla ve bir hakkın uygulanmasının imkansız olacağı veya veri sorumlularınca orantısız çaba

[960] Avrupa Veri Koruma Denetçisi, Veri korumanın ahlaki boyutlarına ilişkin bir dış danışma grubu oluşturma kararı, ("Etik Danışma Grubu"), 3 Aralık 2015, Başlangıç 5.

gerektireceği belirli durumlarla sınırlıdır.

- Belirli durumlar dışında, tamamen otomatikleştirilmiş karar süreci genellikle yasaktır.

- Bireyler arasındaki farkındalık ve kontrol, hakların uygulanmasının sağlanmasında kilit öneme sahiptir.

Gittikçe dijitalleşen dünyamızda, her faaliyet toplanabilir, işlenebilir ve değerlendirilebilir veya analiz edilebilir dijital bir iz bırakır. Yeni bilgi ve iletişim teknolojileriyle, giderek daha fazla veri toplanmakta ve kaydedilmektedir.[961] Yakın zamana kadar hiçbir teknoloji, veri yığınını analiz edememiş, değerlendirememiş ya da ondan kullanışlı sonuçlar çıkaramamıştır. Veriler değerlendirilemeyecek kadar çok, eğilimleri ve alışkanlıkları belirlemek için ise fazla karmaşık, hızlı ve zayıf yapılandırılmıştır.

10.1.1. Büyük veri, algoritmalar ve yapay zekanın tanımlanması

Büyük veri

"Büyük veri" terimi, içeriğe bağlı olarak çeşitli kavramlara işaret edebilecek bir terimdir. Genellikle "toplama, işleme ile yeni ve öngören bilgileri büyük hacimde, yüksek hızda ve çeşitte verilerden elde etme hususunda artan teknolojik kabiliyeti"[962] kapsamaktadır. Bu nedenle büyük veri kavramı hem verilerin kendilerini hem de veri analizini içermektedir.

Verilerin kaynakları çeşitli türlerdendir ve insanlar ile kişisel verilerini, makineleri veya sensörleri, iklim bilgilerini, uydu görüntülerini, dijital resimleri ve videoları veya GPS sinyallerini içermektedir. Bununla birlikte, verilerin ve bilgilerin büyük bir kısmı kişisel verilerdir; ad, fotoğraf, e-posta adresi, banka bilgileri, GPS izleme verileri, sosyal ağ sitelerindeki gönderiler, tıbbi bilgiler veya bilgisayarın IP adresi.[963]

Büyük veri aynı zamanda veri yığınlarının ve mevcut bilgilerin işlenmesi, analizi ve değerlendirilmesi anlamına gelmektedir; başka bir deyişle, büyük veri analizi amacıyla kullanışlı bilgiler edinme. Bu, toplanan verilerin ve bilgilerin, aslen amaçlananlardan daha başka amaçlarla, örneğin istatistiksel eğilimler veya reklam gibi daha özel hizmetlerde kullanılabileceği anlamına gelmektedir. Aslında, büyük verileri toplamak, işlemek ve değerlendirmek için teknolojilerin mevcut olduğu hallerde, her türlü bilgi birleştirilebilir ve yeniden değerlendirilebilir: finansal işlemler, kredibilite, tıbbi tedavi, özel tüketim, mesleki faaliyet, takip ve gidilen rotalar, internet kullanımı, elektronik kartlar ve akıllı telefonlar, görüntülü izleme veya iletişimin izlenmesi. Büyük veri analizi, örneğin tüketicilere uyarlanmış hizmetler sunmak için, beraberinde gerçek zamanlı olarak değerlendirilebilecek ve kullanılabilecek yeni bir nicel veri boyutu getirmektedir.

---

[961] Avrupa Komisyonu, Komisyon'dan Avrupa Parlamentosu, Konsey, Avrupa Ekonomik ve Sosyal Komitesi ve Bölgeler Komitesi'ne gelişen veri ekonomisine yönelik bildirim, COM(2014) 442 final, Brüksel, 2 Temmuz 2014.
[962] Avrupa Konseyi, Sözleşme 108 Danışma Kurulu, *Büyük veri dünyasında kişisel verilerin işlenmesi hususunda bireylerin korunmasına ilişkin rehber*, s. 2; Avrupa Komisyonu, Komisyon'dan Avrupa Parlamentosu, Konsey, Avrupa Ekonomik ve Sosyal Komitesi ve Bölgeler Komitesi'ne gelişen veri ekonomisine yönelik bildirim, COM(2014) 442 final, Brüksel, 2 Temmuz 2014, s. 4; Uluslararası Telekomünikasyon Birliği (2015), Tavsiye Y.3600. Büyük Veri – Bulut bilişim tabanlı gereksinimler ve yetenekler.
[963] AB Komisyonu AB Veri Koruma Reformu ve Büyük Veri Üzerine Bilgi Notu; [963] Avrupa Konseyi, Sözleşme 108 Danışma Kurulu, *Büyük veri dünyasında kişisel verilerin işlenmesi hususunda bireylerin korunmasına ilişkin rehber*, s. 2.

Algoritmalar ve yapay zeka

Yapay zeka (AI) "akıllı üstlenici" olarak çalışan makinelerin zekasını ifade etmektedir. Akıllı bir üstlenici olarak, bazı cihazlar, yazılımın desteğiyle, ortamlarını algılayabilir ve algoritmalara göre işlem yapabilir. Bir makine normalde gerçek kişilerle ilişkilendirilen – öğrenme ve problem çözme gibi – "bilişsel" işlevleri taklit ettiği zaman AI terimine başvurulmaktadır.[964] Modern teknolojiler ve yazılımlar, karar vermeyi taklit etmek için, cihazların "otomatik kararlar" vermek için kullandıkları algoritmaları kullanmaktadır. Bir algoritma en iyi hesaplama, işleme ve değerlendirme ile otomatik muhakeme ve karar verme için adım adım ilerleyen bir prosedür şeklinde tanımlanmaktadır.

Büyük veri analizlerine benzer şekilde, AI ve ürettiği otomatik karar verme, büyük miktarlarda verinin derlenmesini ve işlenmesini gerektirir. Bu veriler cihazın kendisinden (frenlerin ısısı, yakıt vb.) veya çevresinden gelebilir. Örneğin profilleme, önceden belirlenmiş örüntülere veya faktörlere göre otomatik karar vermeye dayanan bir süreçtir.

Örnek: Profilleme ve hedeflemeli reklamcılık

Büyük veriye dayalı profilleme, "bir kişilik türünün karakteristik özelliklerini" yansıtan örüntüler aramayı (örneğin, online alışveriş şirketleri, bir müşterinin daha önce alışveriş sepetine koyduğu ürünlerden toplanan bilgilere dayanarak "bunları da beğenebilirsin" ürünleri önerdiğinde) içermektedir. Ne kadar fazla veri olursa, mozaik o kadar net olur. Örneğin, akıllı telefon, bireylerin bilinçli veya bilinçsiz bir şekilde her bir kullanımla tamamladıkları güçlü bir ankettir.

Çağdaş psikografi – kişilikler üzerinde çalışmanın bilimi – ele aldığı karakter türlerini belirlemesi sebebiyle OCEAN ["Okyanus"] metodunu kullanmaktadır. "Büyük Beşli" karakter boyutları, Açıklık [Openness] (kişi yeniliğe ne kadar açık), Sorumluluk Duygusuyla Hareket Etme [Conscientiousness] (kişi mükemmeliyetçiliğe ne kadar yakın), Dışadönüklük [Extraversion] (kişi ne kadar sosyal), Kabul Edilebilirlik [Agreeableness] (kişi ne kadar kabul edilebilir) ve Nevrotiklik [Neuroticism] (kişi ne kadar savunmasız) ile ilgilidir. Bu bilgi, söz konusu kişiyi, ihtiyaçlarını ve çekincelerini, nasıl davranacaklarını vb. gösterir. Daha sonra, kişi hakkında, veri simsarlarından, sosyal ağlardan (gönderilerdeki ve fotoğraflardaki "beğeniler" de dahil) online dinlenen müziklere veya GPS ve izleme verilerine mevcut herhangi bir kaynaktan edinilen diğer bilgilerle tamamlanmaktadır.

Büyük veri analizi teknikleriyle oluşturulan profil yığını daha sonra benzer örüntüleri tanımlamak ve kişilik kümeleri oluşturmak için karşılaştırılmaktadır. Buna bağlı olarak, belirli kişiliklerin davranış ve tutumları hakkındaki bilgi tersine çevrilmektedir. Büyük veriye erişim ve büyük verinin kullanımıyla, bireyin kişiliğini tanımlamak için kullanılan davranış ve tutum hakkında bilgi ile kişilik testi tersine çevrilmektedir. Sosyal ağlardaki "beğeniler", veri izleme, dinlenen müzik veya izlenen filmler hakkındaki birleşik bilgilerin elde edilmesiyle, bir bireyin kişiliğinden işletmelerin o kişinin "kişiliğine" göre özelleştirilmiş reklam ve/veya bilgiyi iletmelerini sağlayacak net bir resim ortaya çıkabilir. Hepsinden önemlisi, bu bilgiler gerçek zamanlı olarak işlenebilir.[965]

---

[964] Stuart Russel ve Peter Norvig, *Yapay Zeka: Modern Bir Yaklaşım* (2. Basım), 2003, Upper Saddle River, New Jersey: Prentice Hall, ss. 27, 32–58, 968–972; Stuart Russel ve Peter Norvig, *Yapay Zeka: Modern Bir Yaklaşım* (3. Basım), 2009, Upper Saddle River, New Jersey: Prentice Hall, s. 2.

[965] İşleme teknikleri ve yeni yazılım, bir kişinin neyi sevdiği, alışveriş yaparken ya da gerçek zamanlı olarak bir online alışveriş sepetine neleri eklediği ile ilgili bilgileri değerlendirir ve toplanan bilgilere dayanarak ilgisini

10.1.2. Büyük verinin faydalarının ve risklerinin dengelenmesi

Modern işleme teknikleri, büyük miktarda veriyle başa çıkabilir, hızlı bir şekilde yenilerini içeri aktarabilir, kısa cevap süresi (karmaşık taleplerde dahi) açısından bilgilerin gerçek zamanlı olarak işlenmesini sağlayabilir, çoklu ve eşzamanlı talepler için olasılık sağlayabilir ve farklı bilgi türlerini (fotoğraflar, metinler veya sayılar) analiz edebilir. Bu teknolojik yenilikler veri ve bilgi yığınlarını gerçek zamanlı olarak yapılandırmayı, işlemeyi ve değerlendirmeyi mümkün kılmaktadır.[966] Daha küçük ölçekli bir analizde ulaşılması imkansız olacak sonuçlara şimdi mevcut ve analiz edilen veri miktarını katlanarak arttırarak ulaşılabilmektedir. Büyük veri, hem işletmeler hem de tüketiciler için yeni hizmetlerin ortaya çıkabileceği yeni bir iş alanı geliştirilmesine yardımcı olmuştur. AB vatandaşlarının kişisel verilerinin değeri, 2020 yılına kadar yaklaşık 1 trilyon Euro'ya ulaşma potansiyeline sahiptir.[967] Bu nedenle, büyük veri, işletmeler ve hükümetlerin yanı sıra bireylere de fayda sağlayabilecek yeni toplumsal, ekonomik veya bilimsel bilgiler için veri yığınının değerlendirilmesinden kaynaklanan yeni fırsatlar sunabilir.[968]

Büyük veri analitiği, farklı kaynaklar ve veri kümeleri arasındaki örüntüleri ortaya çıkarabilir ve bilim ile tıp gibi alanlarda kullanışlı bilgiler sağlar. Örneğin bu durum sağlık, gıda güvenliği, akıllı ulaşım sistemleri, enerji verimliliği veya şehir planlama gibi alanlarda söz konusudur. Bu gerçek zamanlı bilgi analizi, uygulanan sistemleri geliştirmek için kullanılabilir. Araştırmada, özellikle büyük miktarda verinin bugüne kadar yalnızca elle işletilerek değerlendirildiği disiplinlerde, büyük miktarda veri ve istatistiksel değerlendirmenin birleştirilmesiyle yeni görüşler elde edilebilir. Mevcut bilgi yığını ile karşılaştırmalara dayanarak, bireysel hastalara özel yeni tedaviler geliştirilebilir. Şirketler, büyük veri analizinin, rekabet avantajı kazanmalarını, potansiyel tasarruf üretmelerini ve bireysel müşteri hizmetleri aracılığıyla doğrudan yeni iş alanları yaratmalarını sağlayacağını ummaktadır. Devlet kurumları ceza yargılamasında iyileşmeler elde etmeyi ummaktadır. Komisyon'un Avrupa'daki Dijital Ortak Pazar Stratejisi, AB'deki ekonomik büyüme, inovasyon ve dijitalleşme için katalizör görevi görecek veri güdümlü teknolojiler, hizmetler ve büyük verinin potansiyelini kabul etmektedir.[969]

Bununla birlikte, büyük veri genellikle "üç [V]" özelliğiyle ilgili riskler de taşır: İşlenen verilerin hacmi [volume], hızı [velocity] ve çeşitliliği [variety]. Hız veri işleme süratini ifade ederken, hacim işlenen veri miktarını, çeşitlilik ise veri türlerinin farklılığını ve sayısını ifade etmektedir. Veri korumayla ilgili özel hususlar, özellikle, bireyler ve/veya gruplarla ilgili karar

çekebilecek "ürünler" önerebilir.

[966] Büyük Veri'nin işlenmesi için yazılım geliştirme halen erken bir aşamadadır. Bununla birlikte, özellikle bireylerin faaliyetlerine ilişkin gerçek zamanlı olarak veri ve bilgi yığınlarının analizi için analitik programlar geliştirilmiştir. Büyük Veri'yi yapılandırılmış bir şekilde analiz etme ve işleme imkanı, profilleme ve hedefli reklamcılık için yeni yöntemler sağlamıştır. Avrupa Komisyonu, Komisyon'dan Avrupa Parlamentosu, Konsey, Avrupa Ekonomik ve Sosyal Komitesi ve Bölgeler Komitesi'ne gelişen veri ekonomisine yönelik bildirim, COM(2014) 442 final, Brüksel, 2 Temmuz 2014.; AB Komisyonu AB Veri Koruma Reformu ve Büyük Veri Üzerine Bilgi Notu *Büyük veri dünyasında kişisel verilerin işlenmesi hususunda bireylerin korunmasına ilişkin rehber*, 23 Ocak 2017, s. 2.

[967] AB Komisyonu AB Veri Koruma Reformu ve Büyük Veri Üzerine Bilgi Notu

[968] Uluslararası Veri Koruma ve Gizliliği Komiserleri Konferansı (2014), Büyük Veri hakkında karar ve Avrupa Komisyonu, Komisyon'dan Avrupa Parlamentosu, Konsey, Avrupa Ekonomik ve Sosyal Komitesi ve Bölgeler Komitesi'ne gelişen veri ekonomisine yönelik bildirim, COM(2014) 442 final, Brüksel, 2 Temmuz 2014, s. 2; AB Komisyonu AB Veri Koruma Reformu ve Büyük Veri Üzerine Bilgi Notu *Büyük veri dünyasında kişisel verilerin işlenmesi hususunda bireylerin korunmasına ilişkin rehber*, 23 Ocak 2017, s. 1.

[969] Büyük verinin temel haklar üzerindeki etkileri hakkında 14 Mart 2017 tarihli Avrupa Parlamentosu kararı: gizlilik, veri koruma, ayrımcılık yasağı, güvenlik ve hukuki yaptırım, (2016/2225 (INI)).

alma amacıyla yeni ve öngören bilgiler elde etmek için büyük veri kümelerinde büyük veri analizleri kullanıldığında ortaya çıkmaktadır.[970] Büyük verilere ilişkin veri koruma ve gizliliği riskleri Avrupa Veri Koruma Denetçisi ve Madde 29 Çalışma Grubu (WP29) görüşlerinde, Avrupa Parlamentosu kararlarında ve Avrupa Konseyi politikası dokümanlarında vurgulanmıştır.[971]

Riskler, büyük verinin bilgi yığınına erişimi olan kişiler tarafından toplumdaki bireylerin veya belirli grupların manipülasyonu, ayrımcılığa uğraması veya baskılanması yoluyla yanlış kullanılmasını içerebilir.[972] Bireysel davranışlar ilgili bilgi veya kişisel veri yığınlarının toplandığı, işlendiği ve değerlendirildiği hallerde bunların istismarı özel hayatın gizliliğinin ötesine geçen belirgin temel hak ve özgürlük ihlallerine yol açabilir. Gizliliğin ve kişisel verinin ne kadar etkilenmiş olabileceğinin ölçülmesi tam olarak mümkün değildir. Avrupa Parlamentosu, büyük verinin toplam etkisinin kanıta dayalı değerlendirmesini yapmak için bir metodoloji eksikliği tespit etmiştir ancak büyük veri analizlerinin hem kamu hem de özel sektörde kayda değer bir yatay etkiye sahip olabileceğini gösteren kanıtlar da vardır.[973]

Avrupa Genel Veri Koruma Regülasyonu, profilleme de dahil olmak üzere otomatik karar verme işlemine tabi tutulmama hakkına dair hükümler içermektedir.[974] Gizlilik hususu, itiraz etme hakkının tatbikinin, veri sahiplerinin kendi görüşlerini açıklamalarına ve karara karşı koymalarına imkan tanıyan insan müdahalesini gerektirdiği hallerde ortaya çıkmaktadır.[975] Bu, örneğin, herhangi bir insan müdahalesinin mümkün olmadığı veya algoritmaların çok karmaşık olduğu ve söz konusu verilerin miktarının bireylere belirli kararlar için gerekçeler sağlayamayacak kadar büyük ve/veya bilgilerin, bireylerin rızalarını almak için eski olması durumunda, kişisel veriler için yeterli düzeyde koruma sağlama zorluklarına yol açabilir. Yapay zeka (AI) kullanımının ve otomatik karar vermenin bir örneği ipotek başvurularındaki son gelişmelerde veya işe alım süreçlerinde bulunmaktadır. Başvuranların başvuruları önceden belirlenmiş parametrelere veya faktörlere uymadığı gerekçesiyle reddedilmekte veya geri çevrilmektedir.

10.1.3. Verilerin korunmasına ilişkin meseleler

Veri koruma açısından, ana meseleler, bir yandan işlenen kişisel verilerin hacmi ve çeşitliliğine diğer yandan ise işleme ve sonuçlarına ilişkindir. Veri yığınlarını karar alma amacıyla bir kaynağa dönüştürmek için karmaşık algoritmaların ve yazılımların uygulanması, bilhassa profilleme ve etiketleme durumlarında özellikle bireyleri ve grupları etkilemekte ve sonuç olarak birçok veri koruma sorununu gündeme getirmektedir.[976]

---

[970] Avrupa Konseyi, Sözleşme 108 Danışma Kurulu, *Büyük veri dünyasında kişisel verilerin işlenmesi hususunda bireylerin korunmasına ilişkin rehber*, 23 Ocak 2017, s. 2.
[971] Örneğin bkz. Avrupa Veri Koruma Denetçisi (2015), Büyük verinin zorluklarının üstesinden gelmek, Görüş 7/2015, Brüksel, 19 Kasım 2015; Avrupa Veri Koruma Denetçisi (2016), Büyük veri çağında temel hakların tutarlı uygulanması, Görüş 8/2016, 23 Eylül 2016; Avrupa Parlamentosu (2016), Büyük verinin temel haklar üzerindeki etkileri hakkında karar: gizlilik, veri koruma, ayrımcılık yasağı, güvenlik ve hukuki yaptırım, P8_TA (2017)0076, Strazburg, 14 Mart 2017; Avrupa Konseyi, Sözleşme 108 Danışma Kurulu, *Büyük veri dünyasında kişisel verilerin işlenmesi hususunda bireylerin korunmasına ilişkin rehber*, T-PD(2017)01, Strazburg, 23 Ocak 2017.
[972] Uluslararası Veri Koruma ve Gizliliği Komiserleri Konferansı (2014), Büyük veri hakkında karar.
[973] Büyük verinin temel haklar üzerindeki etkileri hakkında 14 Mart 2017 tarihli Avrupa Parlamentosu kararı: gizlilik, veri koruma, ayrımcılık yasağı, güvenlik ve hukuki yaptırım, (2016/2225 (INI)).
[974] Avrupa Genel Veri Koruma Regülasyonu, md. 22.
[975] A.g.e., md. 22(3).
[976] Avrupa Konseyi, Sözleşme 108 Danışma Kurulu, *Büyük veri dünyasında kişisel verilerin işlenmesi hususunda bireylerin korunmasına ilişkin rehber*, 23 Ocak 2017, s. 2.

Sorumluların ve işleyenlerin tanımlanması ve bunların sorumlulukları

Büyük veri ve yapay zeka (AI), sorumluların ve işleyenlerin tanımlanması ve bunların sorumlulukları ile ilgili muhtelif sorular doğurmaktadır: Bu kadar büyük miktarda veri toplanıp işlendiğinde, verinin sahibi kimdir? Veriler akıllı makineler ve yazılımlar tarafından işlendiğinde, sorumlu kimdir? İşlemedeki her aktörün sorumlulukları tam olarak nelerdir? Ve büyük veri hangi amaçlar için kullanılabilir?

Yapay zeka (AI) bağlamında sorumluluk meselesi, bir yapay zeka (AI) kendi geliştirdiği veri işlemeye dayanan bir karar verdiğinde, daha da çetrefilli bir hal alacaktır. Avrupa Genel Veri Koruma Regülasyonu, veri sorumlusunun ve veri işleyenin sorumlulukları hakkında hukuki bir çerçeve sunmaktadır. Kişisel verilerin hukuka aykırı işlenmesi, veri sorumlusu ve veri işleyen için sorumluluk doğurmaktadır.[977] Yapay zeka ve otomatik karar verme, işlenen verinin miktarının ve karmaşıklığının kesin olarak belirlenemediği hallerde veri sahiplerinin mahremiyetini etkileyen ihlallerden kimin sorumlu olduğu ile ilgili sorunlar ortaya çıkarmaktadır. Yapay zeka (AI) ve algoritmalar ürün olarak düşünüldüğünde, bu durum, Avrupa Genel Veri Koruma Regülasyonu'nda düzenlenen kişisel sorumluluk ile düzenlenmeyen ürün sorumluluğu arasında sorunlar yaratmaktadır.[978] Bu, örneğin otomatik karar verme de dahil olmak üzere, robotik ve yapay zeka (AI) için kişisel sorumluluk ile ürün sorumluluğu arasındaki boşluğu doldurmadaki sorumluluğu hakkında kurallar gerektirecektir.[979]

Veri koruma ilkeleri üzerinde etki

Yukarıda açıklanan büyük verinin doğası, analizi ve kullanımı, Avrupa veri koruma hukukunun geleneksel, temel ilkelerinin bazılarının uygulanmasını zorlaştırmaktadır.[980] Bu zorluklar temel olarak meşruiyet, veri küçültme, amaç bakımından sınırlandırma ve şeffaflık ilkeleri ile ilgilidir.

Veri küçültme ilkesi kişisel verilerin uygun, ilgili ve işlendikleri amaca göre gerekli olanlarla sınırlı olmasını gerektirir. Bununla birlikte, büyük verilerin iş modeli, çoğu zaman belirtilmemiş amaçlar için daha fazla veri gerektirdiğinden, veri küçültmenin antitezi olabilir.

Aynısı, verinin belirtilen amaçlar için işlenmesini gerektiren amaç bakımından sınırlandırma ilkesi için de geçerlidir ve böyle bir işleme, – veri sahibinin rızası gibi ancak bununla sınırlı olmamak üzere – hukuki bir temele dayanmadıkça, başlangıçtaki toplama amacına uymayan amaçlar için kullanılamaz (bkz. Kısım 4.1.1).

Son olarak, büyük veri uygulamaları toplanan verilerin doğruluğunu kontrol etme ve/veya sürdürme imkanı olmadan çeşitli kaynaklardan veri toplama eğiliminde olduğundan, büyük veri, verilerin doğruluğu ilkesine de meydan okur.[981]

Özel kurallar ve haklar

[977] Avrupa Genel Veri Koruma Regülasyonu, md. 77-79 ve md. 82.
[978] Avrupa Parlamentosu, Robotikte Avrupa Medeni Hukuk Kuralları, İç Politikalar Genel Müdürlüğü, (Ekim 2016), s. 14.
[979] Roberto Viola'nın Avrupa Parlamentosu'ndaki Avrupa Robotik Hukuku Hakkında Medya Semineri'ndeki konuşması. (KONUŞMA 16/02/2017); AI ve robotik için hukuki sorumluluk kuralları hakkında bir teklif amacıyla Komisyon'a yapılan talep hakkında Avrupa Parlamentosu duyurusu.
[980] Avrupa Konseyi, *Büyük veri dünyasında kişisel verilerin işlenmesi hususunda bireylerin korunmasına ilişkin rehber*, T-PD (2017) 01, Strazburg, 23 Ocak 2017.
[981] Avrupa Veri Koruma Denetçisi (2016), Büyük veri çağında temel hakların tutarlı uygulanması, Görüş 8/2016, 23 Eylül 2016, s. 8.

Genel kural, kişisel verilerin büyük veri analizi yoluyla işlenmesinin veri koruma mevzuatı kapsamına girdiği şeklinde kalmaktadır. Yine de, AB ve Avrupa Konseyi hukukunda algoritmik karmaşık veri işlenmesiyle ilgili özel durumlar için özel kurallar veya istisnalar getirilmiştir.

Avrupa Konseyi hukukunda, Modernize Edilen Sözleşme 108, büyük veri çağında veri sahibinin kişisel verileri üzerinde daha etkili bir kontrol yapılmasını sağlamak için veri sahibine yeni haklar vermektedir. Bu, tam da örneğin, Modernize Edilen Sözleşme'nin 1(a), (c) ve (d) maddelerinde, veri sahibinin görüşlerinin dikkate alınmaksızın yalnızca verilerinin otomatik işlenmesine dayanarak kendisini önemli derecede etkileyen bir karara itiraz hakkı olduğu durumdur: talep üzerine, veri sahibinin erişim hakkı, bu tür işlemelerin sonuçlarının kendisine uygulandığı ve itiraz etme hakkının bulunduğu veri işleme altında yatan muhakemenin bilgisini edinme hakkını teşkil etmektedir. Modernize Edilen Sözleşme 108'in diğer hükümleri, bilhassa şeffaflık ve ek yükümlülükler hakkında olanlar, dijital zorlukların üstesinden gelmek için Modernize Edilen Sözleşme 108 ile kurulan koruyucu mekanizmanın tamamlayıcı unsurlarıdır.

AB hukukunda, GDPR'ın 23. maddesinde listelenen hallerin yanı sıra, kişisel verilerin tüm işlenmelerinde şeffaflık sağlanmalıdır. Bu, özellikle internet hizmetleri ve karar verme için algoritmaların kullanılması gibi diğer karmaşık otomatik veri işlemeler ile ilgili olarak önemlidir. Bu noktada, veri işleme sistemlerinin özellikleri veri sahiplerinin verilerine neler olduğunu gerçekten anlamalarını mümkün kılmalıdır. Adil ve şeffaf bir işleme sağlamak için, Avrupa Genel Veri Koruma Regülasyonu veri sorumlusunun veri sahibine profilleme dahil olmak üzere otomatik karar vermede yürütülen mantığa ilişkin anlamlı bilgiler sağlamasını gerektirmektedir.[982] Avrupa Konseyi Bakanlar Komitesi, ağ tarafsızlığı bakımından ifade özgürlüğü hakkı ve özel hayatın gizliliği hakkının korunmasına ve desteklenmesine ilişkin Tavsiye Kararı'nda, internet servis sağlayıcılarının "kullanıcıların içeriğe, uygulamalara ve hizmetlere erişimini ve bunların dağıtımını etkileyebilecek trafik yönetimi uygulamaları hakkında kullanıcılara açık, eksiksiz ve kamuya açık bilgiler sağlamasını" tavsiye etmiştir.[983] Tüm Üye Devletlerde, yetkili makamlar tarafından internet trafik yönetimi uygulamalarına ilişkin raporlar açık ve şeffaf bir şekilde hazırlanmalı ve halka ücretsiz olarak sunulmalıdır.[984]

Veri sorumluları – veriler onlardan toplansa da toplanmasa da – veri sahiplerini yalnızca toplanan veriler ve öngörülen işleme ile ilgili özel bilgiler hakkında bilgilendirmekle kalmamalı (bkz. Kısım 6.1.1), ilgili olduğu yerde, otomatik karar verme işlemelerinin varlığı hakkında, onda "yürütülen mantığa ilişkin anlamlı bilgiler"[985] ve bu işlemelerin amaçları ile olası sonuçlarını da sağlayarak, bilgilendirmelidir. Avrupa Genel Veri Koruma Regülasyonu ayrıca (yalnızca kişisel verilerin veri sahibinden elde edilmediği hallerde), "söz konusu bilgilerin sağlanmasının imkansız olması veya ölçüsüz bir çaba gerektirmesi"[986] halinde sorumlunun veri sahibine bu konu ile ilgili bilgi sağlamakla zorunlu olmadığı hususunu açıklar. Bununla birlikte, Madde 29 Çalışma Grubu'nun (WP29) 2016/679 sayılı Regülasyon'un amaçları doğrultusunda otomatik bireysel karar alma ve profilleme hakkında rehberinde vurgulandığı üzere, işlemenin karmaşıklığı, kendi başına, veri sorumlusunun veri sahibine veri işlemede kullanılan mantıksal analiz ve amaçlar hakkında net açıklamalar yapmasını engellememelidir.[987]

---

[982] Avrupa Genel Veri Koruma Regülasyonu, md. 13 (2) (f).

[983] Avrupa Konseyi, Bakanlar Komitesi (2016), Üye Devletlere ağ tarafsızlığı bakımından ifade özgürlüğü hakkı ve özel hayatın gizliliği hakkının korunmasına ve desteklenmesine ilişkin Tavsiye Kararı CM/Rec(2016), Ocak 2016, para. 5.1.

[984] A.g.e., para 5.2.

[985] Avrupa Genel Veri Koruma Regülasyonu, md. 13 (2) f ve 14 (2) g.

[986] A.g.e., md. 14 (5) b.

[987] Madde 29 Çalışma Grubu (WP29), 2016/679 sayılı Tüzük'ün amaçları doğrultusunda otomatik bireysel karar

Veri sahiplerinin işlemeyi kısıtlama haklarının yanı sıra, kişisel verilerine erişim, kişisel verilerinin düzeltilmesi ve silinmesi hakları benzer bir muafiyet içermez. Bununla birlikte, veri sorumlusunun kişisel verilerinin düzeltilmesi veya silinmesi konusunda veri sahibini bildirim yükümlülüğü (bkz. Kısım 6.1.4) de böyle bir bildirimin "imkansız olması veya ölçüsüz bir çaba gerektirmesi"[988] halinde kaldırılabilir.

Veri sahiplerinin ayrıca, Avrupa Genel Veri Koruma Regülasyonu'nun 21. maddesi (bkz. Kısım 6.1.6) uyarınca, büyük veri analizi halleri de dahil olmak üzere kişisel verilerinin herhangi bir şekilde işlenmesine itiraz etme hakkı vardır. Veri sorumluları, ağır basan meşru menfaatlerini gösterdikleri takdirde bu zorunluluktan muaf tutulabiliyorken, doğrudan pazarlama amaçlı işlemlerde bu tür bir muafiyetten yararlanamazlar.

Bu haklarla ilgili özel istisnalar, veri sorumluları tarafından, kişisel verileri kamu yararına arşivleme amacıyla, bilimsel veya tarihi araştırma amacıyla veya istatistiksel amaçlarla işlerken de gündeme getirilebilir.[989]

Avrupa Genel Veri Koruma Regülasyonu, profilleme ve otomatik karar verme ile ilgili olarak özel kurallar getirmiştir: Madde 22 (1), veri sahibinin, "kendisi ile ilgili hukuki sonuçlar doğuran, yalnızca otomatik işleme faaliyetine dayalı bir karara tabi olmama hakkının bulunduğunu" düzenlemektedir. Madde 29 Çalışma Grubu (WP29) rehberlerinin de altını çizdiği üzere, bu madde tamamen otomatik karar verme konusunda genel bir yasağı belirtmektedir.[990] Veri sorumlusu bu yasaktan yalnızca üç özel halde muaf olabilir: 1) veri sahibi ile veri sorumlusu arasındaki bir sözleşmenin ifası için gerekli olması, 2) AB veya ulusal hukukça izin verilmesi, 3) açık rızaya dayanması.[991]

Bireysel kontrol

Büyük veri analizinin karmaşıklığı ve şeffaflık eksikliği, kişisel verilerin bireysel kontrolü hakkındaki fikirlerin tekrar gözden geçirilmesini gerektirebilir. Bu, bireylerdeki bilgi eksikliğini hesaba katarak, verilen sosyal ve teknolojik bağlama göre uyarlanmalıdır. Bu nedenle, büyük veriyle ilgili verilerin korunmasında, veri kullanımı üzerinde, hangi bireysel kontrolün veri kullanımıyla ilgili risklerin çoklu etki değerlendirmelerinde daha karmaşık bir süreç haline geldiğine göre, daha kapsamlı bir kontrol fikri benimsenmelidir.[992]

Bir büyük veri uygulamasının ne kadar iyi olduğu, test bireylerinin (veya tüketicilerin) isteklerini veya davranışlarını ne kadar iyi tahmin edebileceğine bağlıdır. Büyük veri analizine dayanan mevcut tahmin modelleri daimi olarak iyileştirilmektedir. Son gelişmeler, verilerin yalnızca kişilikleri (örneğin davranış ve tutumlar) kategorize etmek için kullanılmasını değil, ses örüntülerinin ve mesajların yazıldığı yoğunluğun veya vücut sıcaklığının analiz edilmesi ile davranışların analiz edilmesini de içerir. Bu bilgilerin tümü, örneğin bir banka temsilcisiyle görüşme sırasında kredibilitenin değerlendirilmesi için, büyük veri değerlendirmelerinden elde edilen bilgilere karşı, gerçek zamanlı kullanılabilir. Değerlendirme, kredi başvurusunda bulunan kişinin yararları üzerine değil, büyük veri bilgilerinin analizinden ve

alma ve profilleme hakkında rehber, wp251, 3 Ekim 2017, s. 14.
[988] Avrupa Genel Veri Koruma Regülasyonu, md. 19.
[989] A.g.e., md. 89 (2) ve (3).
[990] Madde 29 Çalışma Grubu (WP29), 2016/679 sayılı Tüzük'ün amaçları doğrultusunda otomatik bireysel karar alma ve profilleme hakkında rehber, wp251, 3 Ekim 2017, s. 9.
[991] Avrupa Genel Veri Koruma Regülasyonu, md. 22 (2).
[992] Avrupa Konseyi, Sözleşme 108 Danışma Kurulu, *Büyük veri dünyasında kişisel verilerin işlenmesi hususunda bireylerin korunmasına ilişkin rehber*, T-PD(2017)01, Strazburg, 23 Ocak 2017.

değerlendirilmesinden elde edilen davranışsal özellikler (örneğin; güçlü bir sesle veya pohpohlayan sesle konuşan aday, onun beden dili veya vücut sıcaklığı) üzerinde yapılır.

Profilleme ve hedeflemeli reklamcılık, bireylerin uyarlanmış reklamlara maruz kaldıklarının farkına varmaları halinde, her zaman sorun teşkil etmeyebilir. Profilleme, bireyleri manipüle etmek amacıyla, örneğin siyasi kampanya için belirli kişilikler veya insan grupları aramak amacıyla, kullanıldığında bir problem haline gelir. Mesela, kararsız seçmen grupları, "kişiliklerine" ve tutumlarına göre uyarlanmış siyasi mesajlarla hedeflenebilir. Başka bir sorun, bu tür profillemenin, belirli kişilerin mal ve hizmetlere erişimini reddetmek için kullanılması olabilir. Büyük verilerin ve kişisel bilgilerin suistimaline karşı koruma sağlayabilecek bir güvence maskelemedir (bkz. Kısım 2.1.1).[993] Kişisel verilerin tamamen anonimleştirilmesi durumunda, örneğin veri sahibiyle ilgili izler bırakan hiçbir bilgi bulunmadığında, bu haller Avrupa Genel Veri Koruma Regülasyonu kapsamı dışında kalmaktadır. Veri sahiplerinin ve bireylerin büyük veri işlenmesindeki rızaları da veri koruma hukuku için bir zorluk teşkil etmektedir. Bu, "müşteri deneyimi" nedeniyle haklı olabilecek uyarlanmış reklamlara ve profillemeye tabi olmaya rızayı ve bilgiye dayalı analitik araçları geliştirmek ve iyileştirmek için kişisel veri yığınlarının kullanılmasına rızayı kapsamaktadır. Büyük veri işlemenin algoritmalara tabi hem maskelenmiş hem de anonimleştirilmiş bilgilere dayanabileceği göz önüne alındığında, büyük veri işlenmesiyle ilgili farkındalık veya farkındalık yokluğu, veri sahiplerinin haklarını kullanma yolları ile ilgili birçok soru ortaya çıkarmaktadır. Maskelenmiş veriler Avrupa Genel Veri Koruma Regülasyonu kapsamına girerken, düzenleme, anonimleştirilmiş verilere uygulanmamaktadır. Kişisel verilerin işlenmesindeki bireysel kontrol ve farkındalık, büyük veri analizlerinde çok önemlidir: O olmadan, haklarını etkin bir şekilde kullanmalarını engelleyen veri sorumlusunun veya veri işleyenin kim olduğu hakkında net bir fikirleri olmayacaktır.

10.2. Web 2.0 ve 3.0: sosyal ağlar ve Nesnelerin İnterneti

Kilit noktalar

- Sosyal Ağ Hizmetleri (SNS), bireylerin kendisiyle benzer düşünen kullanıcı ağlarına katılmasını veya ağı oluşturmasını sağlayan çevrimiçi iletişim platformlarıdır.
- Nesnelerin İnterneti, nesnelerin internete bağlanması ve nesnelerin kendi aralarında birbirine bağlanmasıdır.
- Veri sahiplerinin rızası, sosyal ağlarda veri sorumlularınca hukuka uygun veri işlenmesi için en yaygın hukuki dayanaktır.
- Sosyal ağ kullanıcıları genellikle "aynı konut muafiyeti" ile korunmaktadır, lakin bu istisna belirli bağlamlarda kaldırılabilir.
- Sosyal ağ sağlayıcılar "aynı konut muafiyeti" ile korunmaz.
- Tasarımdan veya başlangıçtan itibaren gizlilik, bu alanda veri güvenliğini sağlamak için çok önemlidir.

[993] A.g.e., s. 2.

10.2.1. Web 2.0 ve 3.0'ın tanımlanması

Sosyal Ağ Hizmetleri

İnternet, başlangıçta, bilgisayarları birbirine bağlamak ve veri alışverişi yapmak amaçlarıyla sınırlı imkanlarda mesajlar iletmek için, bireylere yalnızca içeriklerini pasif olarak görme imkanı sunan internet siteleri ile bir ağ olarak tasarlandı.[994] Web 2.0 çağında, internet kullanıcıların etkileşimde bulunduğu, işbirliği yaptığı ve girdi ürettiği bir foruma dönüştürüldü. Bu çağ, şu anda milyonlarca insanın günlük yaşamının önemli bir parçası olan sosyal ağ hizmetlerinin olağanüstü başarısı ve yaygın kullanımı ile karakterize edilmiştir.

Sosyal Ağ Hizmetleri (SNS) veya "sosyal medya" genel olarak, "bireylerin kendisiyle benzer düşünen kullanıcı ağlarına katılmasını veya ağı oluşturmasını sağlayan çevrimiçi iletişim platformlarıdır"[995] şeklinde tanımlanabilir. Bireyler, bir ağa katılmak veya bir ağ oluşturmak için, kişisel veriler sağlamaya ve kendilerine ait bir profil oluşturmaya davet edilir. SNS, kullanıcıların, fotoğraflar ve videolardan görüşlerini açıklamak için kişisel gönderilere ve gazete bağlantılarına kadar uzanan dijital "içerik" üretmelerini sağlar. Bu çevrimiçi iletişim platformları sayesinde kullanıcılar, diğer birçok kullanıcıyla etkileşime girebilir ve iletişim kurabilir. Hepsinden önemlisi, popüler SNS'lerin çoğu kayıt ücreti gerektirmemektedir. SNS sağlayıcıları, kullanıcıların ağa katılmaları için ödeme yapmalarını şart koşmak yerine, gelirlerinin çoğunu hedefli reklamcılıktan elde eder. Reklam verenler, bu sitelerde günlük olarak ortaya çıkan kişisel bilgilerden büyük ölçüde yararlanabilir. Bir kullanıcının yaşı, cinsiyeti, konumu ve ilgi alanları hakkında bilgi sahibi olarak, reklamlarıyla "doğru" insanlara ulaşmalarını sağlar.

Avrupa Konseyi Bakanlar Komitesi, sosyal ağ hizmetlerinde insan haklarının korunmasına ilişkin, belirli bir bölümü veri korumaya değinen ve 2018 yılında internet aracılarının rolleri ve sorumlulukları hakkında bir başka Tavsiye Kararı[996] ile tamamlanan bir Tavsiye Kararı[997] almıştır.

Örnek: Nora çok mutludur, çünkü eşi ona evlenme teklifi etmiştir. İyi haberi arkadaşlarıyla ve ailesiyle paylaşmak ister ve sosyal bir ağ üzerine sevincini ifade eden duygusal bir gönderi yazmaya ve ilişki durumunu "nişanlı" olarak değiştirmeye karar verir. Nora sonraki günlerde hesabına giriş yaptığında, gelinlikler ve çiçekçiler ile ilgili reklamlar görür. Bu neden böyledir?

Gelinlik ve çiçek firmaları, Facebook'ta reklam oluştururken, Nora gibi insanlara ulaşabilmek için bazı parametreler seçtiler. Nora'nın profili, nişanlı, Paris'te reklamları veren gelinlik ve çiçek firmalarının bulunduğu yere yakında yaşayan bir kadın olduğunu gösterdiğinde, ona hemen reklamlar gösterilmektedir.

Nesnelerin İnterneti

Nesnelerin İnterneti (IoT) internetin gelişiminde bir sonraki adımı temsil eder: Web 3.0 çağı. IoT ile cihazlar internete bağlanabilir ve diğer cihazlarla etkileşime girebilir. Bu, nesnelerin ve

---

[994] Avrupa Komisyonu (2016), Avrupa'da Nesnelerin İnterneti'ne Terfi, SWD (2016) 110 final.
[995] Madde 29 Çalışma Grubu (WP29) (2009), Online sosyal ağ oluşturma hakkın Görüş 5/2009, WP 163, 12 Haziran 2009, s. 4.
[996] Avrupa Konseyi, Bakanlar Komitesi, Bakanlar Komitesi'nin internet aracılarının rolleri ve sorumlulukları hakkında Üye Devletlere Tavsiye Kararı CM/Rec(2018)2, 7 Mart 2018.
[997] Avrupa Konseyi, Bakanlar Komitesi, Bakanlar Komitesi'nin sosyal ağ hizmetlerinde insan haklarının korunmasına yönelik Üye Devletlere Tavsiye Kararı CM/Rec(2012)4, 4 Nisan 2012.

insanların iletişim ağları aracılığıyla birbirlerine bağlanmalarını, durumlarını ve/veya çevredeki ortamın durumunu bildirmelerini sağlar.[998] IoT ve bağlı cihazlar zaten bir realitedir ve akıllı şehirlerin, akıllı evlerin ve akıllı işletmelerin oluşturulmasına yol açacak akıllı cihazların yaratılması ve daha da geliştirilmesiyle, önümüzde birkaç yıl içinde büyük ölçüde büyümesi beklenmektedir.

Örnek: IoT özellikle sağlık hizmetleri için faydalı olabilir. Şirketler zaten hasta sağlığının izlenmesine olanak tanıyan cihazlar, sensörler ve uygulamalar yaratmıştır. Giyilebilir bir alarm butonu kullanılması ve evin etrafına diğer kablosuz sensörlerin yerleştirilmesi ile yalnız yaşayan yaşlıların günlük rutinlerini takip etmek ve günlük programlarında ciddi aksamalar tespit edildiğinde uyarılar üretmek mümkündür. Örneğin, düşüş algılama sensörleri yaşlılar tarafından yaygın olarak kullanılmaktadır. Bu sensörler düşmeleri kesin olarak saptayabilir ve kişinin doktoruna ve/veya ailesine düşüş hakkında bilgi verebilir.

Örnek: Barselona, akıllı bir kentin en bilinen örneklerinden biridir. 2012'den bu yana, şehir, akıllı bir toplu taşıma, atık yönetimi, park ve sokak aydınlatması sistemi oluşturmayı amaçlayan yenilikçi teknolojileri uygulamaya alarak kullanmaktadır. Şehir, örneğin atık yönetimini iyileştirmek için akıllı çöp kutuları kullanmaktadır. Bunlar, toplama yollarını optimize etmek için atık seviyelerinin izlenmesini sağlamaktadır. Kutular neredeyse dolduğunda, atık yönetim şirketi tarafından kullanılan yazılım uygulamasına gönderilen sinyalleri mobil iletişim ağı aracılığıyla iletir. Böylece şirket, atıkların toplanması, önceliklendirilmesi ve/veya yalnızca gerçekten boşaltılması gereken depolarda toplama yapılması için en iyi rotayı planlayabilmektedir.

10.2.2. Faydaların ve risklerin dengelenmesi

SNS'nin son on yıldaki muazzam büyümesi ve başarısı önemli faydalarının mevcut olduğunu göstermektedir. Örneğin, hedeflemeli reklamcılık (vurgulanan örnekte açıklandığı gibi), şirketlerin hedef kitlelerine ulaşması ve onlara daha spesifik bir pazar sunması için özellikle yenilikçi bir yoldur. Ayrıca, kendilerine daha alakalı ve ilginç reklamların sunulması tüketicilerin de çıkarına olabilir. Daha da önemlisi, sosyal ağ hizmetleri ve sosyal medyanın toplum üzerinde ve değişimin uygulanmasında olumlu bir etkisi olabilir. Kullanıcılara, iletişim kurma, etkileşime girme, kendilerini etkileyen konularda grup ve etkinlikler organize etme yetkisi verir.

Benzer şekilde, IoT'nin ekonomiye önemli faydalar getirmesi beklenmektedir ve IoT AB'nin bir Dijital Ortak Pazar'ın geliştirilmesine ilişkin stratejisinin bir parçasıdır. AB içinde, 2020'de IoT bağlantı sayısının altı milyara çıkacağı tahmin edilmektedir. Bağlanırlıktaki bu büyümenin, yenilikçi hizmet ve uygulamaların geliştirilmesi yoluyla önemli ekonomik faydalar, daha iyi sağlık hizmetleri, tüketicilerin ihtiyaçlarının daha iyi anlaşılması ve artan verimlilik getirmesi beklenmektedir.

Aynı zamanda, sosyal medya kullanıcıları tarafından üretilen ve ardından hizmet operatörlerince işlenen büyük miktardaki kişisel bilgi göz önüne alındığında, SNS'nin büyümesi, gizliliğin ve kişisel verilerin korunma yolları hakkında artan bir endişe ile birlikte gelmektedir. SNS, özel yaşam hakkını ve ifade özgürlüğünü tehdit edebilir. Bu tehditler şunları içerebilir: "Kullanıcıların hariç tutulmasına yol açabilecek işlemeleri çevreleyen yasal ve usule ilişkin güvencelerin eksikliği; çocukların ve gençlerin zararlı içerik ve davranışlara karşı

[998] Avrupa Komisyonu, Komisyon Personeli Çalışma Belgesi, Avrupa'da Nesnelerin İnterneti'ne Terfi, SWD (2016) 110, 19 Nisan 2016.

yetersiz korunması; başkalarının haklarına saygı duyulmaması; varsayılan gizlilik dostu ayarların eksikliği; kişisel verilerin toplanma ve işlenme amaçları konusunda şeffaflık eksikliği"[999]. Avrupa veri koruma hukuku, sosyal medyanın getirdiği gizlilik/veri koruma sorunlarına yanıt vermeye çalışmıştır. Rıza, tasarımdan ve başlangıçtan itibaren mahremiyet/veri koruma [ÇN: *GDPR uyarınca privacy by design and default*], bireylerin hakları gibi ilkeler, sosyal medya ve ağ hizmetleri bağlamında özellikle önemlidir.

IoT bağlamında, birbirine bağlı çeşitli cihazlardan üretilen büyük miktarda kişisel veri aynı zamanda gizlilik ve verilerin korunması için riskleri de beraberinde getirmektedir. Şeffaflık Avrupa veri koruma hukukunun önemli bir ilkesi olsa da, bağlı cihazların çokluğu nedeniyle, IoT cihazlarından toplanan verileri kimin toplayabildiği, verilere kimin erişebileceği, verileri kimin kullanabileceği her zaman net değildir.[1000] Bununla birlikte, AB ve Avrupa Konseyi hukuku kapsamında, şeffaflık ilkesi, veri sorumlularına veri sahiplerine ait verileri nasıl kullanıldıkları hakkında açık ve net bir dilde bilgilendirme yükümlülüğü getirmektedir. Kişisel verilerinin işlenmesiyle ilgili riskler, kurallar, güvenceler ve haklar ilgili şahıslara açık bir şekilde belirtilmelidir. Ayrıca IoT'ye bağlı cihazlar ve çoklu işleme faaliyetleri ve ilgili veri – böyle bir işlemenin rızaya dayanması halinde – veri işlenmesine açık ve bilgilendirilmiş rıza gereksinimini de karşılayabilirler. Bireyler genellikle bu tür işlemelerin teknik işleyişini ve bu nedenle de rızalarının sonuçlarını anlama konusunda yetersiz kalırlar.

Bir diğer önemli endişe ise, bağlı cihazların güvenlik risklerine karşı özellikle savunmasız oldukları göz önüne alındığında, güvenliktir. Bağlı cihazlar farklı güvenlik seviyelerine sahiptir. Standart Bilgi Teknolojileri (IT) altyapısının ötesinde çalıştıklarından, güvenlik yazılımını barındırmak veya kullanıcıların kişisel bilgilerini korumak için şifreleme, maskeleme veya anonimleştirme gibi teknikleri kullanmak için yeterli işleme gücü ve depolama kapasitesinden yoksun olabilirler.

Örnek: Almanya'da, uygulamacılar, bir oyuncağın çocukların özel hayatına olan saygısı üzerindeki güçlü kaygılarını takiben internete bağlı oyuncağı yasaklamaya karar verdiler. Uygulamacılar, Cayla adındaki internete bağlı oyuncak bebeğin etkin bir şekilde gizli bir casusluk aygıtı olduğunu düşünüyorlardı. Bebek, onunla oynayan çocuğun sesli sorularını dijital cihazdaki bir uygulamaya gönderilmesi, bunun da onu metne çevirmesi ve bir cevap için internette arama yapması ile çalışıyordu. Daha sonra uygulama, onu çocuğa seslendiren bebeğe bir yanıt gönderiyordu. Bu bebek sayesinde çocuğun ve yakındaki yetişkinlerin iletişimleri kaydedilebilir ve uygulamaya aktarılabilirdi. Bebek üreticileri yeterli güvenlik önlemleri almamışlardı, bebek konuşmaların dinlenmesi için herkes tarafından kullanılmış olabilir.

10.2.3. Verilerin korunmasına ilişkin meseleler

Rıza

Avrupa'da, kişisel verilerin işlenmesi, yalnızca Avrupa veri koruma hukuku uyarınca izin verilmesi halinde hukuka uygun kabul edilecektir. SNS sağlayıcıları için veri sahiplerinin rızası genellikle veri işleme için yasal bir dayanak sağlar. Rıza serbestçe verilmeli ve spesifik, bilgilendirilmiş ve açık olmalıdır (bkz. Kısım 4.1.1).[1001] "Serbestçe verilen" temel olarak veri sahiplerinin gerçek ve özgün bir seçim yapma yeteneğine sahip olması gerektiği anlamına gelir. Rıza, açık ve kesin olarak veri işlemenin tüm kapsamına, amaçlarına ve sonuçlarına atıfta

[999] Avrupa Konseyi, Sosyal ağ hizmetlerinde insan haklarının korunmasına yönelik Üye Devletlere Tavsiye Kararı Rec(2012)4, 4 Nisan 2012.
[1000] Avrupa Veri Koruma Denetçisi (2017), Nesnelerin İnterneti'ni Anlamak.
[1001] Avrupa Genel Veri Koruma Regülasyonu, md. 4 ve 7; Modernize Edilen Sözleşme 108, md. 5.

bulunarak anlaşılabilir olduğu durumlarda "spesifik"tir ve "bilgilendirilmiş"tir. Sosyal medya bağlamında, rızanın SNS operatörü ve üçüncü kişiler tarafından gerçekleştirilen tüm işleme türleri için özgür, spesifik ve bilgilendirilmiş olup olmadığı sorgulanabilir.

Örnek: Bireyler çoğu zaman, bir SNS'ye katılmak ve erişmek için, genellikle gerekli spesifikasyonlar veya alternatif seçenekler sağlanmadan, kişisel verilerinin farklı çeşitlerde işlenmesini kabul etmek zorundadır. Bir SNS'ye kaydolmak için davranışsal reklam almaya razı olma gereksinimi buna bir örnek olacaktır. Madde 29 Çalışma Grubu'nun (WP29) rıza tanımına dair Görüş'ünde belirttiği gibi, "bazı sosyal ağların edindiği önemi göz önüne alarak, bazı kullanıcı grupları (ergenler gibi) sosyal etkileşimlerden kısmen dışlanma riskini önlemek için davranışsal reklam almayı kabul edecektir. Kullanıcı, sosyal ağ hizmetine erişiminden bağımsız olarak, davranışsal reklam alma konusunda özgür ve spesifik bir rıza verecek bir konuma getirilmelidir."[1002]

Avrupa Genel Veri Koruma Regülasyonu uyarınca, 16 yaşın altındaki çocukların kişisel verileri, ilke olarak, rızalarına dayanarak işlenemez.[1003] İşleme için rıza gerekliyse, çocuğun ebeveyni veya vasisi tarafından verilmelidir. Çocuklar, veri işlemeyle ilgili risklerin ve sonuçların daha az farkında olmaları nedeniyle özel bir korumayı hak etmektedir. Bu sosyal medya bağlamında çok önemlidir, çünkü çocuklar siber zorbalık, online taciz veya kimlik hırsızlığı gibi bu tür medya kullanımının içerebileceği olumsuz etkilerin bir kısmına karşı daha savunmasızdır.

Tasarımdan ve başlangıçtan itibaren güvenlik ve gizlilik/veri koruma

Kişisel verilerin işlenmesi, işlenen kişisel verilerin yanlışlıkla veya hukuka aykırı bir şekilde imha edilmesine, kaybolmasına, değiştirilmesine, yetkisiz erişimine veya ifşa edilmesine yol açan sürekli bir güvenlik ihlali olasılığını beraberinde getirdiğinden, özü itibariyle güvenlik riskleri yaratmaktadır. Avrupa veri koruma hukuku uyarınca, veri sorumluları ve veri işleyenlerin veri işleme faaliyetlerine yetkisiz müdahaleyi önlemek için uygun teknik ve organizasyonel önlemleri almaları gerekir. Avrupa veri koruma kuralları kapsamına giren sosyal ağ hizmet sağlayıcıları da bu yükümlülüğe uymak zorundadır.

Tasarımdan ve başlangıçtan itibaren gizlilik/veri koruma ilkeleri, veri sorumlularının ürünlerinin tasarımında güvenliği sağlamalarını ve uygun gizlilik ve veri koruma ayarlarını otomatik olarak uygulamalarını gerektirir. Bu, bir kişi bir sosyal ağa katılmaya karar verdiğinde, hizmet sağlayıcının, yeni hizmet kullanıcısı hakkındaki tüm bilgileri, bütün kullanıcıları için otomatik olarak erişilebilir kılamayacağı anlamına gelir. Hizmete katılırken, varsayılan gizlilik ve veri koruma ayarları, bilgilerin yalnızca kişinin seçtiği kişiler tarafından erişilebileceği şekilde olmalıdır. Erişimi listenin dışındaki kişilere genişletmek, yalnızca kullanıcı varsayılan gizlilik ve veri koruma ayarlarını manuel olarak değiştirmek için işlem yaptıktan sonra mümkün olmalıdır. Bu, uygulanan güvenlik önlemlerine rağmen bir veri ihlali olduğu durumlarda da etkili olabilir. Bu gibi durumlarda, hizmet sağlayıcılar, veri sahibinin hak ve özgürlüklerine yüksek risk getirmesi muhtemel olacak şekilde etkilenen kullanıcıları bilgilendirmelidir.[1004]

Tasarımdan ve başlangıçtan itibaren gizlilik/veri koruma, SNS bağlamında özellikle önemlidir, çünkü, çoğu işleme türünde yer alan yetkisiz erişim risklerine ek olarak, kişisel bilgilerin sosyal

[1002] Madde 29 Çalışma Grubu (2011), Rızanın tanımı hakkında Görüş 15/2011, WP 187, 13 Temmuz 2011, s. 18.
[1003] Bkz. Avrupa Genel Veri Koruma Regülasyonu, md.8. AB Üye Devletleri, 13 yaşından küçük olmamak kaydıyla, kanunla daha küçük bir yaş öngörebilirler.
[1004] A.g.e., md. 34.

medyada paylaşılması ek güvenlik riskleri oluşturur. Bunlar genellikle bireylerin, bilgilerine kimlerin erişebilecekleri ve bu kişilerin onu nasıl kullanabileceğini kavrama konusundaki eksikliklerinden kaynaklanmaktadır. Yaygın sosyal medya kullanımı ile kimlik hırsızlığı olayları ve mağdurların sayısı artmıştır.

Örnek: Kimlik hırsızlığı, bir kişinin başka bir kişiye (mağdur) ait bilgileri, verileri veya belgeleri edindiği ve daha sonra bu bilgileri mağdurun adına mal ve hizmet almak amacıyla mağdurun kimliğine bürünmek için kullandığı hadisedir. Örneğin, bir sosyal medya web sitesinde hesabı olan Paul'ü ele alalım. Paul bir öğretmen ve topluluğunun aktif bir üyesi, oldukça dışadönük ve sosyal medya hesabının mahremiyeti ile veri koruma ayarları konusunda özellikle endişeli değildir. Bazen şahsen tanımadığı insanlar da dahil olmak üzere, uzun bir arkadaş listesi vardır. Büyük bir okulda çalıştığı ve okulun futbol takımına koçluk yaptığından oldukça popüler olduğu için, bu insanların büyük olasılıkla ebeveynler veya okuldan arkadaşlar olduğunu düşünmektedir. Paul'ün e-posta adresi ve doğum günü sosyal medya hesabında görüntülenmektedir. Ek olarak, Paul düzenli bir şekilde, "Sabah koşumuzda ben ve Toby" gibi satırlar eşliğinde köpeği Toby'nin fotoğraflarını paylaşmaktadır. Paul e-postasını veya cep telefonu hesabını korumak için en popüler güvenlik sorularından birinin "evcil hayvanınızın adı nedir" olduğunu fark etmedi. Nick, Paul'ün sosyal medya profilinde bulunan bilgileri kullanarak hesaplarını kolayca kırar.

Bireylerin hakları

SNS sağlayıcıları, işlemenin amacı ve kişisel verilerin doğrudan pazarlama amacıyla nasıl kullanılabileceği hakkında bilgi sahibi olma hakkı dahil, bireylerin haklarına (bkz. Kısım 6.1) riayet etmelidir. Bireylere ayrıca sosyal ağ platformunda oluşturdukları kişisel verilere erişim ve silinmesini talep etme hakkı verilmelidir. Bireylerin kişisel verilerin işlenmesine razı olduğu ve online olarak bilgi yüklediği durumlarda dahi, artık sosyal ağın hizmetlerini almak tercih etmiyorlarsa "unutulmayı" isteyebilmelidirler. Veri taşınabilirliği hakkı, kullanıcıların sosyal ağ hizmetleri sağlayıcısına sağladıkları kişisel verilerin bir kopyasını yapılandırılmış, yaygın olarak kullanılan ve makineyle okunabilir bir biçimde almalarını ve verilerini bir sosyal ağ hizmeti sağlayıcısından diğerine aktarmalarını sağlar.[1005]

Veri Sorumluları

Genellikle sosyal medya bağlamında ortaya çıkan zor bir soru, sorumlunun kim olduğu sorusudur: Yani, veri koruma kurallarına uyma yükümlülüğü ve sorumluluğu bulunan kişi kimdir. Sosyal ağ hizmet sağlayıcıları, Avrupa veri koruma hukuku uyarınca sorumlular olarak kabul edilir. Bu, "sorumlu"nun geniş tanımı ve bu hizmet sağlayıcıların bireyler tarafından paylaşılan kişisel verilerin işlenmesi için amaç ve araçları belirlediği gerçeği göz önüne alındığında açıkça görülmektedir. AB hukukuna göre, sorumluların, AB'de kurulmamış olsalar bile AB'deki veri sahiplerine hizmet veriyorlarsa, Avrupa Genel Veri Koruma Regülasyonu hükümlerine uymaları gerekir.

Bununla birlikte, sosyal ağ hizmetlerinin kullanıcıları da sorumlu olarak kabul edilebilir mi? Bireylerin kişisel verileri "tamamen kişisel veya aynı konutta yaşayan aile fertleriyle ilgili faaliyetleri sırasında" işlediği durumlarda, veri koruma kuralları geçerli değildir. Bu, Avrupa veri koruma hukukunda "aynı konutta yaşayan aile fertleri istisnası" olarak bilinir. Ancak bazı durumlarda bir sosyal ağ servisinin kullanıcısı aynı konutta yaşayan aile fertleri istisnası kapsamına girmeyebilir.

[1005] Avrupa Genel Veri Koruma Regülasyonu, md.21.

Kullanıcılar, kişisel bilgilerini gönüllü olarak çevrimiçi ortamlarda paylaşırlar. Bununla birlikte, çevrimiçi paylaşılan bilgiler genellikle diğer kişilerin kişisel bilgilerini de içerir.

Örnek: Paul'ün çok popüler bir sosyal ağ platformunda bir hesabı var. Paul bir aktör olmaya çalışıyor ve hesabını fotoğraf, video ve sanata olan tutkusunu anlatan gönderiler paylaşmak için kullanmakta. Popülerlik onun geleceği için önemli; bu nedenle, profilinin, ağdaki bir üye olup olmadığına bakılmaksızın, yalnızca yakın irtibat listesine değil, tüm internet kullanıcılarının kullanımına sunulması gerektiğine karar vermiştir. Paul, arkadaşı Sarah ile fotoğraflarını ve videolarını onun rızası olmadan paylaşabilir mi? Bir ilkokul öğretmeni olarak Sarah, özel hayatını, işvereninden, öğrencilerinden ve ebeveynlerinden uzak tutmaya çalışmaktadır. Sosyal ağları kullanmayan Sarah'nın, ortak arkadaşları Nick'ten Paul ile bir partideki fotoğrafının online olarak paylaşıldığını öğrendiği bir durum hayal ediniz. Böyle bir durumda, Paul'ün veri işlemesi "aynı konutta yaşayan aile fertleri istisnası" kapsamında olduğu için AB hukuku kapsamına girmeyecektir.

Ancak, kullanıcıların diğer bireyler hakkında onların rızası olmaksızın bilgi yüklemesinin bu kişilerin gizlilik ve veri koruma haklarını ihlal edebileceğinin farkında ve bilincinde olması çok önemlidir. Aynı konutta yaşayan aile fertleri istisnasının geçerli olduğu hallerde bile – örneğin bir kullanıcının yalnızca kendisi tarafından seçilen kişilerin listesine açık olan bir profili varsa – başkalarıyla ilgili kişisel bilgilerin yayınlanması, kullanıcıyı yine de sorumlu yapabilir. Her ne kadar aynı konutta yaşayan aile fertleri istisnası olduğunda veri koruma kuralları geçerli değilse de, hakaret veya kişilik ihlali gibi diğer ulusal kuralların uygulanmasından sorumluluk doğabilir. Son olarak, yalnızca SNS kullanıcıları aynı konutta yaşayan aile fertleri istisnası ile korunmaktadır. Bu tür özel işlemeler için araç sağlayan sorumlular ve işleyenler AB veri koruma hukukuna tabidir.[1006]

Gizlilik ve elektronik haberleşme hakkındaki Direktif'in reformuyla, mevcut yasal çerçevede telekomünikasyon hizmetleri sağlayıcılarına uygulanabilecek veri koruma, gizlilik ve güvenlik kuralları, örneğin OTT (*over-the-top*) hizmetleri de dahil olmak üzere, cihazdan cihaza haberleşmeler ve elektronik haberleşme servislerine de uygulanacaktır.

[1006] A.g.e., Başlangıç hükmü 18.

İlave Okuma

Bölüm 1

Araceli Mangas, M. (ed.) (2008), *Carta de los derechos fundamentales de la Unión Europea*, Bilbao, Fundación BBVA.

Berka, W. (2012), *Das Grundrecht auf Datenschutz im Spannungsfeld zwischen Freiheit und Sicherheit*, Vienna, Manzsche Verlags- und Universitätsbuchhandlung.

Docksey, C. 'Four fundamental rights: finding the balance' [Dört temel hak: dengeyi bulmak], *International Data Privacy Law [Uluslararası Veri Koruma Hukuku]*, 6, No. 3, s. 195–209.

González Fuster, G. ve Gellert, G. (2012), 'The fundamental right of data protection in the European Union: in search of an uncharted right' [Avrupa Birliği'nde veri korumanın temel hakkı: bilinmeyen bir hakkın peşinde], *International Review of Law [Uluslararası Hukuk Dergisi]*, *Computers and Technology [Bilgisayarlar ve Teknoloji]*, 26 (1), s. 73–82.

Gutwirth, S., Poullet, Y., de Hert, P., de Terwange, C. ve Nouwt, S. (Eds.) (2009), *Reinventing Data Protection [Veri Korumayı Yeniden Keşfetmek]*, Springer.

Hijmans, H. (2016), *The European Union as Guardian of Internet Privacy – the Story of Art 16 TFEU [İnternet Gizliliğinin Koruyucusu Olarak Avrupa Birliği – AB'nin İşleyişine Dair Anlaşma'nın 16. Maddesinin Öyküsü]*, Springer.

Hustinx, P. (2016), 'EU Data Protection Law: the review of Directive 95/46/EC and the Proposed General Data Protection Regulation' [AB Veri Koruma Hukuku: 95/46/EC sayılı Direktif'in ve önerilen Genel Veri Koruma Regülasyonu'nun gözden geçirilmesi].

Kranenborg, H. (2015), 'Google and the Right to be Forgotten' [Google ve Unutulma Hakkı], *European Data Protection Law Review [Avrupa Veri Koruma Hukuku Dergisi]*, 1, No. 1, s. 70-79

Lynskey, O. (2014), 'Deconstructing data protection: the 'added-value' of a right to data protection in the EU legal order' [Veri korumayı yapı söküme uğratmak: AB hukuki düzeninde veri koruma hakkının 'katma değer'i], *International and Comparative Law Quarterly [Uluslararası ve Karşılaştırmalı Hukuk Dergisi]*, 63, No. 3, s. 569–597.

Lynskey, O. (2015), *The Foundations of EU Data Protection Law [AB Veri Koruma Hukukunun Temelleri]*, Oxford, Oxford University Press.

Kokott, J. ve Sobotta, C. (2013), 'The distinction between privacy and data protection in the

case law of the CJEU and the ECtHR' [AB Adalet Divanı ve AİHM içtihadında mahremiyet ve veri koruma arasındaki ayrım], *International Data Privacy Law [Uluslararası Veri Koruma Hukuku]*, 3, No. 4, s. 222–228.

EDRi, An introduction to data protection [Veri korumaya giriş], Brüksel.

Frowein, J. ve Peukert, W. (2009), *Europäische Menschenrechtskonvention*, Berlin, N. P. Engel Verlag.

Grabenwarter, C. ve Pabel, K. (2012), *Europäische Menschenrechtskonvention*, Munich, C. H. Beck.

Harris, D., O'Boyle, M., Warbrick, C. ve Bates, E. (2009), *Law of the European Convention on Human Rights [Avrupa İnsan Hakları Sözleşmesi Hukuku]*, Oxford, Oxford University Press.

Jarass, H. (2010), *Charta der Grundrechte der Europäischen Union*, Munich, C. H. Beck.

Mayer, J. (2011), *Charta der Grundrechte der Europäischen Union*, Baden-Baden, Nomos.

Mowbray, A. (2012), *Cases, materials, and commentary on the European Convention on Human Rights [Avrupa İnsan Hakları Sözleşmesi'ne ilişkin davalar, materyaller ve şerh]*, Oxford, Oxford University Press.

Nowak, M., Januszewski, K. ve Hofstätter, T. (2012), *All human rights for all – Vienna manual on human rights [Hepimiz için tüm insan hakları – Viyana insan hakları rehberi]*, Antwerp, intersentia N. V., Neuer Wissenschaftlicher Verlag.

Picharel, C. ve Coutron, L. (2010), *Charte des droits fondamentaux de l'Union européenne et convention européenne des droits de l'homme*, Brüksel, Emile Bruylant.

Simitis, S. (1997), 'Die EU-Datenschutz-Richtlinie – Stillstand oder Anreiz?', *Neue Juristische Wochenschrift*, No. 5, pp. 281–288.

Warren, S. ve Brandeis, L. (1890), 'The right to privacy' [Gizlilik hakkı], *Harvard Law Review [Harvard Hukuk Dergisi]*, 4, No. 5, s. 193–220.

White, R. ve Ovey, C. (2010), *The European Convention on Human Rights [Avrupa İnsan Hakları Sözleşmesi]*, Oxford, Oxford University Press.

Bölüm 2

Acquisty, A., ve Gross R. (2009), 'Predicting Social Security numbers from public data' [Kamusal veriden sosyal güvenlik numarasını öngörmek], Proceedings of the National Academy of Science, 7 Temmuz 2009.

Carey, P. (2009), *Data protection: A practical guide to UK and EU law [Veri koruma: Birleşik Krallık ve AB Hukuku için pratik bir rehber]*, Oxford, Oxford University Press.

Delgado, L. (2008), *Vida privada y protección de datos en la Unión Europea*, Madrid, Dykinson S. L.

de Montjoye, Y.-A., Hidalgo, C. A., Verleysen, M., ve Blondel V. D. (2013), 'Unique in the

Crowd: the Privacy Bounds of Human Mobility' [Kalabalıkta Eşsiz: İnsan Hareketliliğinin Gizlilik Sınırları], *Nature Scientific Reports*, 3, 2013.

Desgens-Pasanau, G. (2012), *La protection des données à caractère personnel*, Paris, LexisNexis.

Di Martino, A. (2005), *Datenschutz im europäischen Recht*, Baden-Baden, Nomos.

González Fuster, G. (2014), *The Emergence of Personal Data Protection as a Fundamental Right in the EU [AB'de Temel Bir Hak Olarak Kişisel Veri Korumanın Doğuşu]*, Springer.

Morgan, R. ve Boardman, R. (2012), *Data protection strategy: Implementing data protection compliance [Veri koruma stratejisi: Veri koruma uyumluluğunu uygulamak]*, London, Sweet & Maxwell.

Ohm, P. (2010), 'Broken promises of privacy: Responding to the surprising failure of anonymization' [Tutulmayan mahremiyet sözleri: Anonimleştirmenin şaşırtıcı başarısızlığına cevap vermek], *UCLA Law Review [UCLA Hukuk Dergisi]*, 57, No. 6, s. 1701–1777.

Samarati, P. ve Sweeney, L. (1998), 'Protecting Privacy when Disclosing Information: k-Anonymity and Its Enforcement through Generalization and Suppression' [Bilgiyi İfşa Ederken Gizliliğin Korunması: k-Anonimlik ve Genelleme ve Bastırma yoluyla Uygulanması], Technical Report [Teknik Rapor] SRI-CSL-98-04.

Sweeney, L. (2002), 'K-Anonymity: A Model for Protecting Privacy' [K-Anonimlik: Gizliliğin Korunmasında Bir Model], *International Journal of Uncertainty, Fuzziness and Knowledge-based Systems [Uluslararası Belirsizlik, Bulanıklık ve Bilgi Tabanlı Sistemler Dergisi]*, 10, No. 5, s. 557–570.

Tinnefeld, M., Buchner, B. ve Petri, T. (2012), *Einführung in das Datenschutzrecht: Datenschutz und Informationsfreiheit in europäischer Sicht*, Munich, Oldenbourg Wissenschaftsverlag.

United Kingdom Information Commissioner's Office (2012), *Anonymisation: managing data protection risk [Anonimleştirme: veri koruma riskini yönetmek]*. Code of practice [Uygulama ilkeleri].

Bölüm 3-6

Brühann, U. (2012), 'Richtlinie 95/46/EG zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr' in: Grabitz, E., Hilf, M. and Nettesheim, M. (eds.), *Das Recht der Europäischen Union*, Band IV, A. 30, Münih, C. H. Beck.

Conde Ortiz, C. (2008), *La protección de datos personales*, Cadiz, Dykinson.

Coudray, L. (2010), *La protection des données personnelles dans l'Union européenne*, Saarbrucken, Éditions universitaires européennes.

Curren, L. ve Kaye, J. (2010), 'Revoking consent: a 'blind spot' in data protection law?' [Rızayı geri almak: veri koruma hukukunda bir 'kör nokta'?], *Computer Law & Security Review [Bilgisayar Hukuku & Güvenlik Dergisi]*, 26, No. 3 s. 273–283.

Dammann, U. ve Simitis, S. (1997), *EG-Datenschutzrichtlinie*, Baden-Baden, Nomos.

De Hert, P. ve Papakonstantinou, V. (2012), 'The Police and Criminal Justice Data Protection Directive: Comment and Analysis' [Polis ve Cezai Yargılama Veri Koruma Direktifi: Yorum ve Analiz], *Computers & Law Magazine of SCL [SCL Bilgisayar ve Hukuk Dergisi]*, 22, No. 6, s. 1–5.

De Hert, P. ve Papakonstantinou, V. (2012), 'The proposed data protection Regulation replacing Directive 95/46/EC: A sound system for the protection of individuals' [95/46/EC sayılı Direktif'in yerini alan önerilen veri koruma tüzüğü: Bireylerin korunmasına yönelik yerinde bir sistem], *Computer Law & Security Review [Bilgisayar Hukuku & Güvenlik Dergisi]*, 28, No. 2, s. 130–142.

Feretti, Federico (2012), 'A European perspective on data processing consent through the re-conceptualization of European data protection's looking glass after the Lisbon treaty: Taking rights seriously' [Lizbon anlaşmasından sonra Avrupa veri korumasının aynasının yeniden kavramsallaştırılması yoluyla veri işleme rızası konusunda bir Avrupa perspektifi: Hakları ciddiye almak], *European Review of Private Law [Avrupa Özel Hukuk Dergisi]*, 20, No. 2, s. 473–506.

FRA (Avrupa Birliği Temel Haklar Ajansı) (2010), *Data Protection in the European Union: the role of National Supervisory authorities (Strengthening the fundamental rights architecture in the EU II) [Avrupa Birliği'nde Veri Koruma: Ulusal Denetim Otoritelerinin Rolü (AB'de temel hak mimarisinin güçlendirilmesi II)]*, Lüksemburg, Avrupa Birliği Yayın Ofisi (Yayın Ofisi).

FRA (2010), *Developing indicators for the protection, respect and promotion of the rights of the child in the European Union (Conference edition) [Avrupa Birliği'nde çocuk haklarının korunması, itibar görmesi ve desteklenmesi için göstergeler geliştirmek (Konferans baskısı)]*, Viyana, FRA.

FRA (2011), *Access to justice in Europe: an overview of challenges and opportunities [Avrupa'da adalete erişim: zorluklara ve fırsatları genel bir bakış]*, Lüksemburg, Yayın Ofisi.

Irish Health Information and Quality Authority (2010), Guidance on Privacy Impact Assessment in Health and Social Care [Sağlık ve Sosyal Bakımda Gizlilik Etki Değerlendirmesi Hakkında Rehberlik].

Kierkegaard, S., Waters, N., Greenleaf, G., Bygrave, L. A., Lloyd, I. ve Saxby, S. (2011), '30 years on – The review of the Council of Europe Data Protection Convention 108' [30 yıl sonra – 108 sayılı Avrupa Konseyi Veri Koruma Sözleşmesi'nin İncelenmesi], *Computer Law & Security Review [Bilgisayar Hukuku & Güvenlik Dergisi]*, 27, No. 3, s. 223–231.

Simitis, S. (2011), *Bundesdatenschutzgesetz*, Baden-Baden, Nomos.

United Kingdom Information Commissioner's Office, *Privacy Impact Assessment [Gizlilik Etki Değerlendirmesi]*.

Bölüm 7

European Data Protection Supervisor [Avrupa Veri Koruma Denetçisi] (2014), Position paper on transfer of personal data to third countries and international organisations by EU institutions

and bodies [AB kurum ve kuruluşları tarafından kişisel verilerin üçüncü ülkelere ve uluslararası kuruluşlara aktarılması hakkında makale].

Gutwirth, S., Poullet, Y., De Hert, P., De Terwangne, C. ve Nouwt, S. (2009), *Reinventing data protection? [Veri korumayı yeniden keşfetmek?]*, Berlin, Springer.

Kuner, C. (2007), *European data protection law [Avrupa veri koruma hukuku]*, Oxford, Oxford University Press.

Kuner, C. (2013), *Transborder data flow regulation and data privacy law [Sınırlararası veri akışı düzenlemesi ve veri gizliliği hukuku]*, Oxford, Oxford University Press.

Article 29 Working Party [Madde 29 Çalışma Grubu] (2005), Working document on a common interpretation of Article 26(1) of Directive 95/46/EC of 24 October 1995 [24 Ekim 1995 tarih ve 95/46/EC sayılı Direktif'in 26(1). maddesinin ortak yorumu hakkında çalışma belgesi].

Bölüm 8

Blasi Casagran, C. (2016) *Global Data Protection in the Field of Law Enforcement, an EU Perspective [Hukuki Yaptırım Alanında Küresel Veri Koruma, AB Perspektifi]*, Londra, Routledge.

Boehm, F. (2012), *Information Sharing and Data Protection in the Area of Freedom, Security and Justice. Towards Harmonised Data Protection Principles for Information Exchange at EU-level [Özgürlük, Güvenlik ve Adalet Alanında Bilgi Paylaşımı ve Veri Koruma. AB düzeyinde Bilgi Alışverişi için Uyumlaştırılmış Veri Koruma İlkelerine Doğru]*, Berlin, Springer.

Europol (2012), *Data Protection at Europol [Europol'de Veri Koruma]*, Lüksemburg, Yayın Ofisi.

Eurojust, *Data protection at Eurojust: A robust, effective and tailor-made regime [Eurojust'ta veri koruma: Sağlam, etkili ve kişiye özel bir rejim]*, Lahey, Eurojust.

De Hert, P. ve Papakonstantinou, V. (2012), 'The Police and Criminal Justice Data Protection Directive: Comment and Analysis' [Polis ve Cezai Yargılama Veri Koruma Direktifi: Yorum ve Analiz], *SCL Bilgisayar & Hukuk Dergisi*, 22, No. 6, s. 1–5.

Drewer, D. ve Ellermann, J. (2012), 'Europol's data protection framework as an asset in the fight against cybercrime' [Siber suçlarla mücadelede bir değer olarak Europol'ün veri koruma çerçevesi], *ERA Forum*, 13, No. 3, s. 381–395.

Gutiérrez Zarza, A. (2015), *Exchange of Information and Data Protection in Cross-border Criminal Proceedings in Europe [Avrupa'daki Sınır Ötesi Ceza İşlemlerinde Bilgi Değişimi ve Veri Koruma]*, Berlin, Springer.

Gutwirth, S., Poullet, Y. ve De Hert, P. (2010), *Data protection in a profiled world [Profillenmiş bir dünyada veri koruma]*, Dordrecht, Springer.

Gutwirth, S., Poullet, Y., De Hert, P. ve Leenes, R. (2011), *Computers, privacy and data protection: An element of choice [Bilgisayarlar, gizlilik ve veri koruma: Bir seçim elemanı]*, Dordrecht, Springer.

Konstadinides, T. (2011), 'Destroying democracy on the ground of defending it? The Data Retention Directive, the surveillance state and our constitutional ecosystem' [Demokrasiyi savunma bahanesiyle onu yok etmek mi? Veri Saklama Direktifi, gözetim devleti ve anayasal ekosistemimiz], *European Law Review [Avrupa Hukuku Dergisi]*, 36, No. 5, s. 722–776.

Santos Vara, J. (2013), *The role of the European Parliament in the conclusion of the Transatlantic Agreements on the transfer of personal data after Lisbon [Lizbon'dan sonra Transatlantik Anlaşmaların sonuçlanmasında Avrupa Parlamentosu'nun kişisel verilerin aktarılması konusundaki rolü]*, Dış İlişkiler Hukuku Merkezi, CLEER Çalışma Belgeleri 2013/2.

Bölüm 9

Büllesbach, A., Gijrath, S., Poullet, Y. ve Hacon, R. (2010), *Concise European IT law [Kısaltılmış Avrupa Bilgi Teknolojileri Hukuku]*, Amsterdam, Kluwer Law International.

Gutwirth, S., Leenes, R., De Hert, P. ve Poullet, Y. (2012), *European data protection: In good health? [Avrupa veri koruma hukuku:Afiyette mi?]*, Dordrecht, Springer.

Gutwirth, S., Poullet, Y. ve De Hert, P. (2010), *Data protection in a profiled world [Profillenmiş bir dünyada veri koruma]*, Dordrecht, Springer.

Gutwirth, S., Poullet, Y., De Hert, P. ve Leenes, R. (2011), *Computers, privacy and data protection: An element of choice [Bilgisayarlar, gizlilik ve veri koruma: Bir seçim elemanı]*, Dordrecht, Springer.

Konstadinides, T. (2011), 'Destroying democracy on the ground of defending it? The Data Retention Directive, the surveillance state and our constitutional ecosystem' [Demokrasiyi savunma bahanesiyle onu yok etmek mi? Veri Saklama Direktifi, gözetim devleti ve anayasal ekosistemimiz], *European Law Review [Avrupa Hukuku Dergisi]*, 36, No. 5, s. 722–776.

Rosemary, J. ve Hamilton, A. (2012), *Data protection law and practice [Veri koruma hukuku ve uygulama]*, Londra, Sweet & Maxwell.

Bölüm 10

El Emam, K. ve Álvarez, C. (2015), 'A critical appraisal of the Article 29 Working Party Opinion 05/2014 on data anonymization techniques' [Madde 29 Çalışma Grubu'nun veri anonimleştirme teknikleri konusundaki 05/2014 Görüşü'nün eleştirel bir değerlendirmesi], *International Data Privacy Law [Uluslararası Veri Gizliliği Hukuku]*, 5, No. 1, s. 73–87.

Mayer-Schönberger, V. ve Cate, F. (2013), 'Notice and consent in a world of Big Data' [Büyük Veri dünyasında bildirim ve rıza], *International Data Privacy Law [Uluslararası Veri Gizliliği Hukuku]*, 3, No. 2, s. 67–73.

Rubistein, I. (2013), 'Big Data: The End of Privacy or a New Beginning?' [Gizliliğin Sonu mu, Yeni Bir Başlangıç mı?], *International Data Privacy Law [Uluslararası Veri Gizliliği Hukuku]*, 3, No. 2, s. 74–87.

İçtihat

Avrupa İnsan Hakları Mahkemesi'nin seçili içtihatları

Kişisel veriye erişim

Gaskin/Birleşik Krallık, No. 10454/83, 7 Temmuz 1989

Godelli/İtalya, No. 33783/09, 25 Eylül 2012

K.H. ve Diğerleri/Slovakya, No. 32881/04, 28 Nisan 2009

Leander/İsveç, No. 9248/81, 26 Mart 1987

M.K./Fransa, No. 19522/09, 18 Nisan 2013

Odièvre/Fransa [BD], No. 42326/98, 13 Şubat 2003

Veri korumayı ifade özgürlüğü ve bilgi edinme hakkı ile dengelemek

Axel Springer AG/Almanya [BD], No. 39954/08, 7 Şubat 2012

Bohlen/Almanya, No. 53495/09, 19 Şubat 2015

Coudec ve Hachette Filipacchi Associés/Fransa [BD], No. 40454/07, 10 Kasım 2015

Magyar Helsinki Bizottság/Macaristan [BD], No. 18030/11, 8 Kasım 2016

Müller ve Diğerleri/İsviçre, No. 10737/84, 24 Mayıs 1988

Vereinigung bildender Künstler/Avusturya, No. 68345/01, 25 Ocak 2007

Von Hannover/Germany (No. 2) [BD], Nos. 40660/08 ve 60641/08, 7 Şubat 2012

Satakunnan Markkinapörssi Oy ve Satamedia Oy/Finlandiya, No. 931/13, 27 Haziran 2017

Veri korumayı din özgürlüğü ile dengelemek

Sinan Işık/Türkiye, No. 21924/05, 2 Şubat 2010

Online veri korumada zorluklar

K.U./Finlandiya, No. 2872/02, 2 Aralık 2008

Veri sahibinin rızası

Elberte/Letonya, No. 61243/08, 13 Ocak 2015

Sinan Işık/Türkiye, No. 21924/05, 2 Şubat 2010

Y/Turkey, No. 648/10, 17 Şubat 2015

Yazışma

Amann/İsviçre [BD], No. 27798/95, 16 Şubat 2000

Association for European Integration and Human Rights ve Ekimdzhiev/Bulgaristan, No. 62540/00, 28 Haziran 2007

Bernh Larsen Holding AS ve Diğerleri/Norveç, No. 24117/08, 14 Mart 2013

Cemalettin Canli/Türkiye, No. 22427/04, 18 Kasım 2008

D.L./Bulgaristan, No. 7472/14, 19 Mayıs 2016

Dalea/Fransa, No. 964/07, 2 Şubat 2010

Gaskin/Birleşik Krallık, No. 10454/83, 7 Temmuz 1989

Haralambie/Romanya, No. 21737/03, 27 Ekim 2009

Khelili/İsviçre, No. 16188/07, 18 Ekim 2011

Leander/İsveç, No. 9248/81, 26 Mart 1987

Malone/Birleşik Krallık, No. 8691/79, 2 Ağustos 1984

Rotaru/Romanya [BD], No. 28341/95, 4 Mayıs 2000

S. ve Marper/Birleşik Krallık [BD], Nos. 30562/04 ve 30566/04, 4 Aralık 2008

Shimovolos/Russia, No. 30194/09, 21 Haziran 2011

Silver ve Diğerleri/Birleşik Krallık, Nos. 5947/72, 6205/73, 7052/75, 7061/75, 7107/75, 7113/75, 25 Mart 1983

The Sunday Times/Birleşik Krallık, No. 6538/74, 26 Nisan 1979

Sabıka kaydı veritabanları

Aycaguer/Fransa, No. 8806/12, 22 Haziran 2017

B.B./Fransa, No. 5335/06, 17 Aralık 2009

Brunet/Fransa, No. 21010/10, 18 Eylül 2014

M.K./Fransa, No. 19522/09, 18 Nisan 2013

M.M./Birleşik Krallık, No. 24029/07, 13 Kasım 2012

Veri güvenliği

Haralambie/Romanya, No. 21737/03, 27 Ekim 2009

K.H. ve Diğerleri/Slovakya, No. 32881/04, 28 Nisan 2009

DNA veritabanları

S. ve Marper/Birleşik Krallık [BD], Nos. 30562/04 ve 30566/04, 4 Aralık 2008

GPS verileri

Uzun/Almanya, No. 35623/05, 2 Eylül 2010

Sağlık verileri

Avilkina ve Diğerleri/Rusya, No. 1585/09, 6 Haziran 2013

Biriuk/Litvanya, No. 23373/03, 25 Kasım 2008

I/Finlandiya, No. 20511/03, 17 Haziran 2008

L.H./Letonya, No. 52019/07, 29 Nisan 2014

L.L./Fransa, No. 7508/02, 10 Ekim 2006

M.S./İsveç, No. 20837/92, 27 Ağustos 1997

Szuluk/Birleşik Krallık, No. 36936/05, 2 Haziran 2009

Y/Türkiye, No. 648/10, 17 Şubat 2015

Z/Finlandiya, No. 22009/93, 25 Şubat 1997

Kimlik

Ciubotaru/Moldova, No. 27138/04, 27 Nisan 2010

Godelli/İtalya, No. 33783/09, 25 Eylül 2012

Odièvre/Fransa [BD], No. 42326/98, 13 Şubat 2003

Mesleki faaliyetlere ilişkin bilgi

G.S.B./İsviçre, No. 28601/11, 22 Aralık 2015

M.N. ve Diğerleri/San Marino, No. 28005/12, 7 Temmuz 2015

Michaud/Fransa, No. 12323/11, 6 Aralık 2012

Niemietz/Almanya, No. 13710/88, 16 Aralık 1992

İletişimin dinlenmesi

Amann/İsviçre [BD], No. 27798/95, 16 Şubat 2000

Brito Ferrinho Bexiga Villa-Nova/Portekiz, No. 69436/10, 1 Aralık 2015

Copland/Birleşik Krallık, No. 62617/00, 3 Nisan 2007

Halford/Birleşik Krallık, No. 20605/92, 25 Haziran 1997

Iordachi ve Diğerleri/Moldova, No. 25198/02, 10 Şubat 2009

Kopp/İsviçre, No. 23224/94, 25 Mart 1998

Liberty ve Diğerleri/Birleşik, No. 58243/00, 1 Temmuz 2008

Malone/Birleşik Krallık, No. 8691/79, 2 Ağustos 1984

Mustafa Sezgin Tanrıkulu/Türkiye, No. 27473/06, 18 Temmuz 2017

Pruteanu/Romanya, No. 30181/05, 3 Şubat 2015

Szuluk/Birleşik Krallık, No. 36936/05, 2 Haziran 2009

Görev sahiplerinin yükümlülükleri

B.B./Fransa, No. 5335/06, 17 Aralık 2009

I/Finlandiya, No. 20511/03, 17 Temmuz 2008

Mosley/Birleşik Krallık, No. 48009/08, 10 Mayıs 2011

Kişisel veri

Amann/İsviçre [BD], No. 27798/95, 16 Şubat 2000

Uzun/Almanya, No. 35623/05, 2010

Bernh Larsen Holding AS ve Diğerleri/Norveç, No. 24117/08, 14 Mart 2013

Fotoğraflar

Sciacca/İtalya, No. 50774/99, 11 Ocak 2005

Von Hannover/Almanya, No. 59320/00, 24 Haziran 2004

Unutulma hakkı

Segerstedt-Wiberg ve Diğerleri/İsveç, No. 62332/00, 6 Haziran 2006

Satakunnan Markkinapörssi Oy and Satamedia Oy/Finlandiya, No. 931/13, 27 Haziran 2017

İtiraz etme hakkı

Leander/İsveç, No. 9248/81, 26 Mart 1987

M.S./İsveç, No. 20837/92, 27 Ağustos 1997

Mosley/Birleşik Krallık, No. 48009/08, 10 Mayıs 2011

Rotaru/Romanya [BD], No. 28341/95, 4 Mayıs 2000

Sinan Işık/Türkiye, No. 21924/05, 2 Şubat 2010

Hassas veri kategorileri

Brunet/Fransa, No. 21010/10, 18 Eylül 2014

I/Finlandiya, No. 20511/03, 17 Temmuz 2008

Michaud/Fransa, No. 12323/11, 6 Aralık 2012

S. ve Marper/Birleşik Krallık [BD], Nos. 30562/04 ve 30566/04, 4 Aralık 2008

Denetim ve uygulama (denetim makamları dahil, farklı aktörlerin rolü)

I/Finlandiya, No. 20511/03, 17 Temmuz 2008

K.U./Finlandiya, No. 2872/02, 2 Aralık 2008

Von Hannover/Almanya, No. 59320/00, 24 Haziran 2004

Von Hannover/Almanya (No. 2) [BD], Nos. 40660/08 ve 60641/08, 7 Şubat 2012

Gözetim yöntemleri

Allan/Birleşik Krallık, No. 48539/99, 5 Kasım 2002

Association for European Integration and Human Rights ve Ekimdzhiev/Bulgaristan, No. 62540/00, 28 Haziran 2007

Bărbulescu/Romanya [BD], No. 61496/08, 5 Eylül 2017

D.L./Bulgaristan, No. 7472/14, 19 Mayıs 2016

Dragojević/Hırvatistan, No. 68955/11, 15 Ocak 2015

Karabeyoğlu/Türkiye No. 30083/10, 7 Haziran 2016

Klass ve Diğerleri/Almanya, No. 5029/71, 6 Eylül 1978

Rotaru/Romanya [BD], No. 28341/95, 4 Mayıs 2000

Szabó ve Vissy/Macaristan, No. 37138/14, 12 Ocak 2016

Taylor-Sabori/Birleşik Krallık, No. 47114/99, 22 Ekim 2002

Uzun/Almanya, No. 35623/05, 2 Eylül 2010

Versini-Campinchi ve Crasnianski/Fransa, No. 49176/11, 16 Haziran 2016

Vetter/Fransa, No. 59842/00, 31 Mayıs 2005

Vukota-Bojić/İsviçre, No. 61838/10, 18 Ekim 2016

Roman Zakharov/Rusya [BD], No. 47143/06, 4 Aralık 2015

Video gözetim

Köpke/Almanya, No. 420/07, 5 Ekim 2010

Peck/Birleşik Krallık, No. 44647/98, 28 Ocak 2003

Ses örnekleri

Wisse/Fransa, No. 71611/01, 20 Aralık 2005

P.G. ve J.H./Birleşik Krallık, No. 44787/98, 25 Eylül 2001

Avrupa Birliği Adalet Divanı'nın seçili içtihatları

Veri Koruma Direktifi'ne ilişkin içtihat

C-13/16, *Valsts policijas Rīgas reģiona pārvaldes Kārtības policijas pārvalde/Rīgas pašvaldības SIA 'Rīgas satiksme'*, 4 Mayıs 2017

[Hukuki işleme prensibi: üçüncü tarafça ileri sürülen meşru menfaat]

C-398/15, *Camera di Commercio, Industria, Artigianato e Agricoltura di Lecce/Salvatore Manni*, 9 Mart 2017

[Kişisel verinin silinmesini isteme hakkı; işlemeye itiraz etme hakkı]

Birleştirilmiş davalar C-203/15 ve C-698/15, *Tele2 Sverige AB/Post- och telestyrelsen ve Secretary of State for the Home Department/Tom Watson ve Diğerleri* [BD], 21 Aralık 2016

[Elektronik haberleşmenin gizliliği; elektronik haberleşme hizmetleri sağlayıcıları; Trafik ve konum verilerinin genel ve ayrım gözetmeksizin saklanmasına ilişkin yükümlülük; mahkeme veya bağımsız idari makam tarafından önceden inceleme yapılmaması; Avrupa Birliği Temel Haklar Şartı; AB hukukuna uygunluk]

C-582/14, *Patrick Breyer/Bundesrepublik Deutschland*, 19 Ekim 2016

['Kişisel veri'nin tanımı; İnternet protokol adresi; verinin bir online medya hizmetleri sağlayıcı tarafından saklanması; sorumlu tarafından izlenen meşru menfaatlerin dikkate alınmasına izin vermeyen ulusal mevzuat]

C-362/14, *Maximilian Schrems/Data Protection Commissioner* [BD], 6 Ekim 2015

[Hukuki işleme prensibi; temel haklar; Safe Harbour Kararı'nın geçersizliği; bağımsız denetim otoritelerinin yetkileri]

C-230/14, *Weltimmo s. r. o. v. Nemzeti Adatvédelmi és Információszabadság Hatóság*, 1 Ekim 2015

[Ulusal denetim otoritelerinin yetkileri]

C-201/14, *Smaranda Bara ve Diğerleri/Casa Naţională de Asigurări de Sănătate ve Diğerleri*, 1 Ekim 2015

[Kişisel verilerin işlenmesi hakkında bilgi sahibi olma hakkı]

C-212/13, *František Ryneš/Úřad pro ochranu osobních údajů*, 11 Aralık 2014

["Veri işleme" ve "sorumlu" kavramı]

C-473/12, *Institut professionnel des agents immobiliers (IPI)/Geoffrey Englebert ve Diğerleri*, 7 Kasım 2013

[Kişisel verilerin işlenmesi hakkında bilgi sahibi olma hakkı]

T-462/12 R, *Pilkington Group Ltd/European Commission*, Order of the President of the General Court, 11 Mart 2013

C-342/12, *Worten – Equipamentos para o Lar SA/Autoridade para as Condições de Trabalho (ACT)*, 30 Mayıs 2013

['Kişisel veri' kavramı; çalışma zamanının kaydı; veri niteliği ile ilgili ilkeler ve veri işlemenin meşrulaştırılması için kriterler; çalışma koşullarının izlenmesinden sorumlu ulusal otorite tarafından erişim; işverenin derhal istişaresine izin verecek şekilde çalışma süresinin kaydını yapma yükümlülüğü]

Birleştirilmiş davalar C-293/12 ve C-594/12, *Digital Rights Ireland Ltd/Minister for Communications, Marine and Natural Resources ve Diğerleri and Kärntner Landesregierung ve Diğerleri* [BD], 8 Nisan 2014

[Veri Saklama Direktifi ile AB birincil hukukunun ihlali; hukuki işleme; amaç ve saklama bakımından sınırlama]

C-288/12, *Avrupa Komisyonu/Macaristan* [BD], 8 Nisan 2014

[Ulusal veri koruma denetçisi ofisinin kaldırılmasının meşruiyeti]

Birleştirilmiş davalar C-141/12 ve C-372/12, *YS/Minister voor Immigratie, Integratie en Asiel ve Minister voor Immigratie, Integratie en Asiel/M ve S*, 17 Temmuz 2014

[Veri sahibinin erişim hakkının kapsamı; bireylerin kişisel verilerin işlenmesi konusunda korunması; 'kişisel veri' kavramı; oturum izni başvurusu sahibine ilişkin veri ve karara hazırlık niteliğindeki idari belgede yer alan hukuki analiz; Avrupa Birliği Temel Haklar Şartı]

C-131/12, Google Spain SL, *Google Inc./Agencia Española de Protección de Datos (AEPD), Mario Costeja González* [BD], 13 Mayıs 2014

[Arama motoru sağlayıcılarının, veri sahibinin talebi üzerine, kişisel verileri arama sonuçlarında göstermekten kaçınmaları; Veri Koruma Direktifi'nin uygulanabilirliği; 'veri işleme' kavramı; 'sorumluların' anlamı; veri korumayı ifade özgürlüğü ile dengelemek; unutulma hakkı]

C-614/10, *Avrupa Komisyonu/Avusturya Cumhuriyeti* [BD], 16 Ekim 2012

[Ulusal denetim otoritesinin bağımsızlığı]

Birleştirilmiş davalar C-468/10 ve C-469/10, *Asociación Nacional de Establecimientos*

Financieros de Crédito (ASNEF) ve Federación de Comercio Electrónico y Marketing Directo (FECEMD)/Administración del Estado, 24 Kasım 2011

[Veri Koruma Direktifi'nin "başkalarının meşru çıkarları" başlıklı 7(f) maddesinin ulusal hukukta doğru şekilde uygulanması]

C-360/10, *Belgische Vereniging van Auteurs, Componisten en Uitgevers CVBA (SABAM)/Netlog NV*, 16 Şubat 2012

[Sosyal ağ sağlayıcılarının, müzik ve görsel-işitsel eserlerin ağ kullanıcıları tarafından yasadışı bir şekilde kullanılmasını önleme yükümlülüğü]

C-70/10, *Scarlet Extended SA/Société belge des auteurs, compositeurs et éditeurs SCRL (SABAM)*, 24 Kasım 2011

[Bilgi toplumu; telif hakkı; internet; 'eş düzeyde' yazılım; İnternet hizmet sağlayıcıları; telif hakkını ihlal eden dosya paylaşımını önleme amacıyla elektronik haberleşmeyi filtrelemek için bir sistem kurulması; iletilen bilgileri izlemek için genel bir yükümlülük olmaması]

C-543/09, *Deutsche Telekom AG/Bundesrepublik Deutschland*, 5 Mayıs 2011

[Yenilenen rızanın gerekliliği]

Birleştirilmiş davalar C-92/09 ve C-93/09, *Volker und Markus Schecke GbR ve Hartmut Eifert/Land Hessen* [BD], 9 Kasım 2010

["Kişisel veri" kavramı; bazı AB tarım fonlarının faydalanıcıları hakkında kişisel veriler yayınlamak için yasal zorunluluğun orantılılığı]

C-553/07, *College van burgemeester en wethouders van Rotterdam/M. E. E. Rijkeboer*, 7 Mayıs 2009

[Veri sahibinin erişim hakkı]

C-518/07, *Avrupa Komisyonu/Almanya Federal Cumhuriyeti* [BD], 9 Mart 2010

[Ulusal denetim otoritesinin bağımsızlığı]

C-73/07, *Tietosuojavaltuutettu/Satakunnan Markkinapörssi Oy ve Satamedia Oy* [BD], 16 Aralık 2008

[Veri Koruma Direktifi madde 9 kapsamında "gazetecilik faaliyetleri" kavramı]

C-524/06, *Heinz Huber/Bundesrepublik Deutschland* [BD], 16 Aralık 2008

[Bir istatistik kaydında yabancılar hakkında veri bulundurmanın meşruiyeti]

C-275/06, *Productores de Música de España (Promusicae)/Telefónica de España SAU* [BD], 29 Ocak 2008

["Kişisel veri" kavramı; internet erişim sağlayıcılarının, KaZaA dosya değişimi programlarının kullanıcılarının kimliklerini fikri mülkiyet koruma birliğine açıklamaları yükümlülüğü]

C-101/01, *Bodil Lindqvist'e yönelik cezai işlemler*, 6 Kasım 2003

[Özel kişisel veri kategorileri]

Birleştirilmiş davalar C-465/00, C-138/01 ve C-139/01, *Rechnungshof/Österreichischer Rundfunk ve Diğerleri ve Christa Neukomm ve Jospeh Lauermann/Österreichischer Rundfunk*, 20 Mayıs 2003

[Kamu sektörü ile ilgili kurumların belirli kategorilerindeki çalışanların maaşlarına ilişkin kişisel verileri yayınlama konusundaki yasal zorunluluğun orantılılığı]

C434/16, *Peter Nowak/Data Protection Commissioner, Opinion of the Advocate General Kokott*, 20 Temmuz 2017

[Kişisel veri kavramı; birinin kendi denetim belgesine erişimi; denetleyenin düzeltmeleri]

C-291/12, *Michael Schwarz/Stadt Bochum*, 17 Ekim 2013

[Bir ön karar için referans; özgürlük, güvenlik ve adalet alanı; biyometrik pasaport; parmak izleri; yasal dayanak; orantılılık]

2016/681 sayılı Direktif'e ilişkin içtihat

Opinion 1/15 of the Court (Büyük Daire), 26 Temmuz 2017

[Hukuki dayanak; Yolcu Adı Kaydı verilerinin aktarılması ve işlenmesi hakkında Kanada ve Avrupa Birliği arasında anlaşma taslağı; taslak anlaşmanın Avrupa Temel Haklar Şartı'nın 7, 8 ve 52(1) maddeleriyle ve AB'nin İşleyişine Hakkında Anlaşma'nın 16. maddesine uygunluğu]

AB Kurumları Veri Koruma Regülasyonu ile ilgili içtihat

C-615/13 P, *ClientEarth, Pesticide Action Network Europe (PAN Europe)/European Food Safety Authority (EFSA), European Commission*, 16 Temmuz 2015

[Belgelere erişim]

C-28/08 P, *Avrupa Komisyonu/The Bavarian Lager Co. Ltd.* [BD], 29 Haziran 2010

[Belgelere erişim]

2002/58/EC sayılı Direktif'e ilişkin içtihat

C-536/15, *Tele2 (Hollanda) BV ve Diğerleri/Autoriteit Consument en Markt (AMC)*, 15 Mart 2017

[Ayrımcılık yasağı prensibi; kamuya açık rehber sorgulama hizmetleri ve rehberlerin sunulması amacıyla abonelere ilişkin kişisel verilerin sağlanması; abonenin rızası; halka açık olan rehber sorgulama hizmetleri ve rehberlerin sağlandığı Üye Devlet temelinde ayrım yapılması]

Birleştirilmiş davalar C-203/15 and C-698/15, *Tele2 Sverige AB/Post- och telestryrelsen ve Secretary of State for the Home Department/Tom Watson ve Diğerleri* [BD], 21 Aralık 2016

[Elektronik haberleşmenin gizliliği; elektronik haberleşme hizmetleri sağlayıcıları; trafik ve

konum verilerinin genel ve ayrım gözetmeksizin saklanmasına ilişkin yükümlülük; mahkeme veya bağımsız idari makam tarafından önceden inceleme yapılmaması; Avrupa Birliği Temel Haklar Şartı; AB hukukuna uygunluk]

C-70/10, *Scarlet Extended SA/Société belge des auteurs, compositeurs et éditeurs SCRL (SABAM)*, 24 Kasım 2011

[Bilgi toplumu; telif hakkı; internet; 'eş düzeyde' yazılım; İnternet hizmet sağlayıcıları; telif hakkını ihlal eden dosya paylaşımını önleme amacıyla elektronik haberleşmeyi filtrelemek için bir sistem kurulması; iletilen bilgileri izlemek için genel bir yükümlülük olmaması]

C-461/10, *Bonnier Audio AB, Earbooks AB, Norstedts Förlagsgrupp AB, Piratförlaget AB, Storyside AB/Perfect Communication Sweden AB*, 19 Nisan 2012

[Telif hakkı ve ilgili haklar; verilerin internet üzerinden işlenmesi; münhasır bir hak ihlali; bir internet hizmet sağlayıcı tarafından sağlanan IP adresi ile internet üzerinden bir FTP sunucusu aracılığıyla temin edilen sesli kitaplar; internet hizmet sağlayıcısına, IP adresinin kullanıcısının adını ve adresini vermesi için verilen talimat]

Dizin

Avrupa Birliği Adalet Divanı'nın içtihatları

Avrupa Komisyonu/The Bavarian Lager Co. Ltd. [BD], C-28/08 P, 29 Haziran 2010

František Ryneš/Úřad pro ochranu osobních údajů, C-212/13, 11 Aralık 2014

Google Inc./Agencia Española de Protección de Datos (AEPD), Mario Costeja González [BD], C-131/12, Google Spain SL, 13 Mayıs 2014

Heinz Huber/Bundesrepublik Deutschland [BD], C-524/06, 16 Aralık 2008

Institut professionnel des agents immobiliers (IPI)/Geoffrey Englebert ve Diğerleri, C-473/12, 7 Kasım 2013

International Transport Workers' Federation, Finnish Seamen's Union/Viking Line ABP, OÜ Viking Line Eesti [BD], C-438/05, 11 Aralık 2007

Maximilian Schrems/Data Protection Commissioner [BD], C-362/14, 6 Ekim 2015

Michael Schwarz/Stadt Bochum, C-291/12, 17 Ekim 2013

Opinion 1/15 of the Court (Grand Chamber), 26 Temmuz 2017

Pasquale Foglia v. Mariella Novello (No. 2), C-244/80, 16 Aralık 1981

Patrick Breyer/Bundesrepublik Deutschland, C-582/14, 19 Ekim 2016

Peter Nowak/Data Protection Commissioner, Opinion of the Advocate General Kokott, C434/16, 20 Temmuz 2017

Pilkington Group Ltd/European Commission, Order of the President of the General Court, T-462/12 R, 11 Mart 2013

Productores de Música de España (Promusicae)/Telefónica de España SAU [BD], C-275/06, 29 Ocak 2008

Rechnungshof/Österreichischer Rundfunk ve Diğerleri ve Christa Neukomm ve Jospeh Lauermann/Österreichischer Rundfunk, Birleştirilmiş davalar C-465/00, C-138/01 ve C-139/01, 20 Mayıs 2003

Scarlet Extended SA/Société belge des auteurs, compositeurs et éditeurs SCRL (SABAM), C-70/10, 24 Kasım 2011

Smaranda Bara ve Diğerleri/Casa Naţională de Asigurări de Sănătate ve Diğerleri, C-201/14, 1 Ekim 2015

Tele2 (Hollanda) BV ve Diğerleri/Autoriteit Consument en Markt (AMC), C-536/15, 15 Mart 2017

Tele2 Sverige AB/Post- och telestryrelsen ve Secretary of State for the Home Department/Tom Watson ve Diğerleri [BD], Birleştirilmiş davalar C-203/15 and C-698/15, 21 Aralık 2016

Tietosuojavaltuutettu/Satakunnan Markkinapörssi Oy ve Satamedia Oy [BD], C-73/07, 16 Aralık 2008

Volker und Markus Schecke GbR ve Hartmut Eifert/Land Hessen [BD], Birleştirilmiş davalar C-92/09 ve C-93/09, 9 Kasım 2010

Weltimmo s. r. o. v. Nemzeti Adatvédelmi és Információszabadság Hatóság, C-230/14, 1 Ekim 2015

Worten – Equipamentos para o Lar SA/Autoridade para as Condições de Trabalho (ACT), C-342/12, 30 Mayıs 2013

YS/Minister voor Immigratie, Integratie en Asiel ve Minister voor Immigratie, Integratie en Asiel/M ve S, Birleştirilmiş davalar C-141/12 ve C-372/12, 17 Temmuz 2014

Avrupa İnsan Hakları Mahkemesi içtihatları

Allan/Birleşik Krallık, No. 48539/99, 5 Kasım 2002

Amann/İsviçre [BD], No. 27798/95, 16 Şubat 2000

Association for European Integration and Human Rights ve Ekimdzhiev/Bulgaristan, No. 62540/00, 28 Haziran 2007

Avilkina ve Diğerleri/Rusya, No. 1585/09, 6 Haziran 2013

Axel Springer AG/Almanya [BD], No. 39954/08, 7 Şubat 2012

Aycaguer/Fransa, No. 8806/12, 22 Haziran 2017

B.B./Fransa, No. 5335/06, 17 Aralık 2009

Bărbulescu/Romanya [BD], No. 61496/08, 5 Eylül 2017

Bernh Larsen Holding AS ve Diğerleri/Norveç, No. 24117/08, 14 Mart 2013

Biriuk/Litvanya, No. 23373/03, 25 Kasım 2008

Bohlen/Almanya, No. 53495/09, 19 Şubat 2015

Brito Ferrinho Bexiga Villa-Nova/Portekiz, No. 69436/10, 1 Aralık 2015

Brunet/Fransa, No. 21010/10, 18 Eylül 2014

Cemalettin Canli/Türkiye, No. 22427/04, 18 Kasım 2008

Ciubotaru/Moldova, No. 27138/04, 27 Nisan 2010

Copland/Birleşik Krallık, No. 62617/00, 3 Nisan 2007

Coudec ve Hachette Filipacchi Associés/Fransa [BD], No. 40454/07, 10 Kasım 2015

D.L./Bulgaristan, No. 7472/14, 19 Mayıs 2016

Dalea/Fransa, No. 964/07, 2 Şubat 2010

Dragojević/Hırvatistan, No. 68955/11, 15 Ocak 2015

Elberte/Letonya, No. 61243/08, 13 Ocak 2015

G.S.B./İsviçre, No. 28601/11, 22 Aralık 2015

Gaskin/Birleşik Krallık, No. 10454/83, 7 Temmuz 1989

Godelli/İtalya, No. 33783/09, 25 Eylül 2012

Halford/Birleşik Krallık, No. 20605/92, 25 Haziran 1997

Haralambie/Romanya, No. 21737/03, 27 Ekim 2009

I/Finlandiya, No. 20511/03, 17 Temmuz 2008

Iordachi ve Diğerleri/Moldova, No. 25198/02, 10 Şubat 2009

K.H. ve Diğerleri/Slovakya, No. 32881/04, 28 Nisan 2009

K.U./Finlandiya, No. 2872/02, 2 Aralık 2008

Karabeyoğlu/Türkiye No. 30083/10, 7 Haziran 2016

Khelili/İsviçre, No. 16188/07, 18 Ekim 2011

Klass ve Diğerleri/Almanya, No. 5029/71, 6 Eylül 1978

Köpke/Almanya, No. 420/07, 5 Ekim 2010

Kopp/İsviçre, No. 23224/94, 25 Mart 1998

L.H./Letonya, No. 52019/07, 29 Nisan 2014

L.L./Fransa, No. 7508/02, 10 Ekim 2006

Leander/İsveç, No. 9248/81, 26 Mart 1987

Liberty ve Diğerleri/Birleşik, No. 58243/00, 1 Temmuz 2008

M.K./Fransa, No. 19522/09, 18 Nisan 2013

M.M./Birleşik Krallık, No. 24029/07, 13 Kasım 2012

M.N. ve Diğerleri/San Marino, No. 28005/12, 7 Temmuz 2015

M.S./İsveç, No. 20837/92, 27 Ağustos 1997

Magyar Helsinki Bizottság/Macaristan [BD], No. 18030/11, 8 Kasım 2016

Malone/Birleşik Krallık, No. 8691/79, 2 Ağustos 1984

Michaud/Fransa, No. 12323/11, 6 Aralık 2012

Mosley/Birleşik Krallık, No. 48009/08, 10 Mayıs 2011

Müller ve Diğerleri/İsviçre, No. 10737/84, 24 Mayıs 1988

Mustafa Sezgin Tanrıkulu/Türkiye, No. 27473/06, 18 Temmuz 2017

Niemietz/Almanya, No. 13710/88, 16 Aralık 1992

Odièvre/Fransa [BD], No. 42326/98, 13 Şubat 2003

P.G. ve J.H./Birleşik Krallık, No. 44787/98, 25 Eylül 2001

Peck/Birleşik Krallık, No. 44647/98, 28 Ocak 2003

Pruteanu/Romanya, No. 30181/05, 3 Şubat 2015

Roman Zakharov/Rusya [BD], No. 47143/06, 4 Aralık 2015

Rotaru/Romanya [BD], No. 28341/95, 4 Mayıs 2000

S. ve Marper/Birleşik Krallık [BD], Nos. 30562/04 ve 30566/04, 4 Aralık 2008

Satakunnan Markkinapörssi Oy ve Satamedia Oy/Finlandiya, No. 931/13, 27 Haziran 2017

Sciacca/İtalya, No. 50774/99, 11 Ocak 2005

Segerstedt-Wiberg ve Diğerleri/İsveç, No. 62332/00, 6 Haziran 2006

Shimovolos/Russia, No. 30194/09, 21 Haziran 2011

Silver ve Diğerleri/Birleşik Krallık, Nos. 5947/72, 6205/73, 7052/75, 7061/75, 7107/75, 7113/75, 25 Mart 1983

Sinan Işık/Türkiye, No. 21924/05, 2 Şubat 2010

Szabó ve Vissy/Macaristan, No. 37138/14, 12 Ocak 2016

Szuluk/Birleşik Krallık, No. 36936/05, 2 Haziran 2009

Taylor-Sabori/Birleşik Krallık, No. 47114/99, 22 Ekim 2002

The Sunday Times/Birleşik Krallık, No. 6538/74, 26 Nisan 1979

Uzun/Almanya, No. 35623/05, 2 Eylül 2010

Vereinigung bildender Künstler/Avusturya, No. 68345/01, 25 Ocak 2007

Versini-Campinchi ve Crasnianski/Fransa, No. 49176/11, 16 Haziran 2016

Vetter/Fransa, No. 59842/00, 31 Mayıs 2005

Von Hannover/Almanya, No. 59320/00, 24 Haziran 2004

Von Hannover/Germany (No. 2) [BD], Nos. 40660/08 ve 60641/08, 7 Şubat 2012

Vukota-Bojić/İsviçre, No. 61838/10, 18 Ekim 2016

Wisse/Fransa, No. 71611/01, 20 Aralık 2005

Y/Türkiye, No. 648/10, 17 Şubat 2015

Z/Finlandiya, No. 22009/93, 25 Şubat 1997

Ulusal mahkemelerin içtihadı

Almanya, Federal Anayasa Mahkemesi (*Bundesverfassungsgericht*), 1 BvR 209/83, 1 BvR 484/83, 1 BvR 420/83, 1 BvR 362/83, 1 BvR 269/83, 1 BvR 440/83 (*Volkszählungsurteil*), 15 Aralık 1983

Almanya, Federal Anayasa Mahkemesi (*Bundesverfassungsgericht*), 1 BvR 256/08, 2 Mart 2010

Romanya, Federal Anayasa Mahkemesi (*Curtea Constituþionalã a României*), No. 1258, 8 Ekim 2009

Çekya, Anayasa Mahkemesi (*Ústavní soud České republiky*), 94/2011 Coll., 22 Mart 2011

Avrupa Birliği Temel Haklar Ajansı hakkında internette pek çok bilgi mevcuttur.

fra.europa.eu'daki FRA websitesinden erişilebilmektedir.

Avrupa İnsan Hakları Mahkemesi'nin içtihadı hakkında daha fazla bilgiyi Mahkeme'nin internet sitesinde bulabilirsiniz: echr.coe.int. HUDOC arama portalı İngilizce ve/veya Fransızca dillerinde karar ve ilamlara, ek dillere çevirilere, hukuki özetlere, basın açıklamalarına ve Mahkeme'nin çalışmaları hakkında diğer bilgilere erişimi sağlamaktadır.

Avrupa Konseyi yayınları nasıl edinilir?

Avrupa Konseyi Yayınları, insan hakları, hukuk bilimi, sağlık, etik, sosyal ilişkiler, çevre, eğitim, kültür, spor, gençlik ve mimari miras dahil olmak üzere Konsey'in tüm başvuru alanlarında eserler üretmektedir. Kapsamlı katalogtan kitaplar ve elektronik yayınlar online olarak sipariş edilebilir: http://book.coe.int/.

Sanal okuma odası, kullanıcıların yeni yayınlanan esas çalışmaların seçme parçalarından veya belirli resmi belgelerin tam metinlerinden ücretsiz olarak faydalanmalarını sağlamaktadır.

Avrupa Konseyi Sözleşmeleri hakkında bilginin yanı sıra sözleşmelerin tam metnine Antlaşma Ofisi'nin websitesinden de erişilebilir: http://conventions.coe.int/.

AB ile temasa geçme

Şahsen

Avrupa Birliği'nin her tarafında yüzlerce Doğrudan Avrupa bilgi merkezi bulunmaktadır. Size en yakın merkezin adresini şurada bulabilirsiniz: https://europa.eu/european-union/contact_en

Telefon veya e-postayla

Doğrudan Avrupa, Avrupa Birliği hakkında sorularınızı cevaplayan bir hizmettir. Bu servise,

- ücretsiz telefonla: 00 800 6 7 8 9 10 11 (bazı operatörler bu aramalar için ücret alabilir),
- şu standart numaradan: +32 22999696 veya
- şu e-posta yoluyla: https://europa.eu/european-union/contact_en

başvurabilirsiniz.

AB hakkında bilgi

Online

Avrupa Birliği hakkında AB'nin tüm resmi dillerindeki bilgiyi Europa websitesinde bulabilirsiniz: https://europa.eu/european-union/index_en

AB yayınları

Ücretsiz ve ücretli AB yayınlarını şu adresten indirebilir veya sipariş edebilirsiniz: https://publications.europa.eu/en/publications. Doğrudan Avrupa'ya veya yerel bilgi merkezinize başvurarak birden fazla ücretsiz yayın kopyası alabilirsiniz (bkz. https://europa.eu/european-union/contact_en).

AB hukuku ve ilgili belgeler

1952'den beri tüm AB hukuku dahil olmak üzere AB'den tüm resmi dil sürümlerinde hukuki bilgiye erişim için EUR-Lex'e gidiniz: http://eur-lex.europa.eu.

AB'den açık kaynak

AB Açık Veri Portalı (http://data.europa.eu/euodp/en) AB'den gelen veri kümelerine erişimi sağlar. Veriler hem ticari hem de ticari olmayan amaçlarla ücretsiz olarak indirilebilir ve yeniden kullanılabilir.

Bilgi teknolojisinin hızlı bir şekilde gelişmesi, hem Avrupa Birliği (AB) hem de Avrupa Konseyi (CoE) araçlarınca korunan bir hak olan güçlü kişisel veri korumasına duyulan ihtiyacı daha da artırdı. Teknolojik gelişmeler, gözetim, iletişimin dinlenmesi ve veri saklama gibi alanların sınırlarını genişlettiğinden, bu önemli hakkın korunmasında yeni ve önemli zorluklarla karşılaşılmaktadır. Bu el kitabı veri korumasında uzman olmayan hukuk uygulamacılarına hukukun bu yeni alanını tanıtmak için tasarlanmıştır. AB'nin ve CoE'nin uygulanabilir hukuki çerçevelerine genel bir bakış sunmaktadır. Aynı zamanda, hem Avrupa Birliği Adalet Divanı hem de Avrupa İnsan Hakları Mahkemesi'nin ana kararlarını özetleyerek önemli içtihatlarını da açıklamaktadır. Ek olarak, sürekli gelişen bu alanda karşılaşılan farklı konuların pratik gösterimleri olarak iş gören varsayımsal senaryolar sunmaktadır.

AVRUPA BİRLİĞİ TEMEL HAKLAR AJANSI Schwarzenbergplatz 11 - 1040 Viyana - Avusturya Tel. +43 (1) 580 30-60 - Fax +43 (1) 580 30-699 fra.europa.eu – info@fra.europa.eu – @EURightsAgency

AVRUPA İNSAN HAKLARI MAHKEMESİ AVRUPA KONSEYİ 67075 Strazburg Cedex - Fransa Tel. +33 (0) 3 88 41 20 18 - Fax +33 (0) 3 88 41 27 30 echr.coe.int - publishing@echr.coe.int – @ECHRPublication

AVRUPA VERİ KORUMA DENETÇİSİ Rue Wiertz 60 – 1047 Brüksel – Belçika Tel. +32 2 283 19 00 www.edps.europa.eu – edps@edps.europa.eu – logo@EU_EDPS