AVRUPA BİRLİĞİ GENEL VERİ KORUMA TÜZÜĞÜ BAĞLAMINDA KİŞİSEL VERİLERİN KORUNMASI

Doç. Dr. Murat Volkan Dülger[161],[162]

ÖZET

Bireylerin temel hak ve hürriyetlerini ilgilendirilen kişisel veriler hakkında zaman içinde farkındalık oluşmuş ve bu çerçevede ulusal ve ulusüstü düzenlemeler yapılmıştır. Bu çerçevede kabul edilmiş en geniş kapsamlı ve en güncel düzenleme 2016/679 sayılı Avrupa Birliği Genel Veri Koruma Tüzüğüdür (Tüzük ya da GDPR). 95/46/EC sayılı Direktif bilişim teknolojilerinin günümüzdeki kadar gelişmiş olmadığı bir dönemde kabul edilmiş olup, amaçlarından biri olan AB ülkelerinde kişisel verilerin korunması hukukunda yeknesaklığı da sağlayamamıştır. Bu durum, AB veri koruma normlarının yeniden düzenlenmesi gereğini ortaya çıkarmıştır ve bu ihtiyaçtan hareketle Mayıs 2016'da Avrupa Birliği Genel Veri Koruma Tüzüğü kabul edilmiştir. İlk bakışta Tüzüğün genelinde fark edilebilen ve onu önceki düzenlemelerden ayıran en önemli farklılık, Tüzüğün AB'de kişisel verilerin korunması hukukunun yeknesaklaştırılması amacıyla oldukça ayrıntılı ve etkili bir sistem kurma çabasıdır. Tüzük, bu hedeften yola çıkarak hem tamamen yeni düzenlemelere yer vermiş, hem de daha önceden var olan düzenlemeleri daha somut ve detaylı olarak düzenlemiştir. Bu doğrultuda öncelikle Tüzüğün bölgesel kapsamı artırılmış ve belirli hallerde Tüzüğün AB dışındaki ülkelere de uygulanabilir olduğu öngörülmüştür. Kişisel verilerin korunması hukukunun gelişiminin ve ilgili düzenlemelerin analiz edilmesi ve Tüzüğün kabul edilmesinin arka planının anlaşılması, ayrıca Tüzüğün detaylıca incelenmesi amacıyla makale iki ana bölüme ayrılmıştır. Bu doğrultuda, 1. Bölüm'de kişisel verilerin korunması hakkının yer aldığı başlıca uluslararası düzenlemelere yer verilecektir. 2. Bölüm'de ise Tüzüğün kapsamı, getirdiği yenilikler, düzenlediği ilkeler, haklar ve yükümlülükler ile kurduğu sistem incelenecektir.

Anahtar Kelimeler: GDPR, kişisel veri, veri koruma hukuku, Avrupa Birliği, Genel Veri Koruma Tüzüğü, KVKK.

ABSTRACT

[161] İstanbul Aydın Üniversitesi Hukuk Fakültesi, Ceza Hukuku, Ceza Muhakemesi Hukuku ve Bilişim Hukuku öğretim üyesi.

[162] ORCID: https://orcid.org/0000-0003-4034-5436

The awareness on personal data which relates to basic rights and freedoms raised over time and national and international legal legislations have been adopted correspondingly. European Union General Data Protection Regulation numbered 2016/679 is the most broad in scope and most up-to-date legal text on the matter. The Directive numbered 95/6/EC, adopted in a context where information Technologies weren't as developed as today, failed its principal mission: ensuring uniformity and consistency between data protection laws of member states of European Union. This lead to the occurrence of the need for regulating European data protection law all over again. Based on this need, European General Data Protection Regulation was adopted on May 2016. The most outstanding novelty and difference on the general overview of The Regulation is that The Regulation aims to build a circumstantial and effective system in order to harmonize data protection law in the Europe. Based on this aim, The Regulation engage both creation of entirely new rules and remodeling of existing ones with a more circumstantial and comprehensive approach. In this direction, first the territorial scope of The Regulation was extended and it is provided that The Regulation can be applicable to the countries outside European Union within certain circumstances. This article was divided into two main parts in order to first analyze the development of personal data protection law, related legislations and background of the adoption of The Regulation and then examine the provision of The Regulation in detail. Accordingly, main international texts disposing right to personal data protection are presented in the First Part. The scope of The Regulation, the novelties brought by and the principles, rights and obligations disposed in The Regulation are examined in the Second Part.

Keywords: GDPR, personal data, data protection law, European Union, General Data Protection Regulation, KVKK.

GİRİŞ

Günümüzde en çok duyulan kavramlardan ikisi kişisel verilerin korunması ve yapay zekâ teknolojileridir. Teknolojinin hızla gelişerek her geçen gün hayatlarımıza yeni bir şey kattığı bu dönemde, neredeyse her bireyin kişisel verileri, bireylerin üzerlerinde çeşitli kontrol seviyelerine sahip olduğu işlemlere konu oluyor. İnsanlar kimi zaman kendi istekleri ile verilerini paylaşırlarken, kimi zaman "okudum, anladım" seçeneğine alel acele tıklayıp bunu gerçekleştiriyorlar; kimi zaman ise hiç haberleri olmadan verileri kendileri dışındaki kişilere ulaşıyor. Bu durum, kişisel verileri kullanarak nöral sinir ağları sistemiyle büyük bir hızla gelişen

yapay zekâ teknolojilerine kaynak sağlarken, bir yandan da gözetim toplumunun oluşmasına ve bireylerin sürekli kontrol altında tutulmasına yol açıyor.

Zamanla hakkında bilinçlenme oluşan bir konu olan kişisel veri, bireylerin temel hak ve özgürlükleri ile çok yakından ilgili olması sebebiyle pek çok riski de içinde barındırmakta. Bu nedenle bu alanın yasal düzeyde düzenlenmesi gerekliliği doğmuş ve kişisel verilerin korunması hususu ulusal ve uluslararası seviyede çeşitli belgelerde işlenmiştir. Bu çerçevede kabul edilmiş en geniş kapsamlı ve en güncel düzenleme 2016/679 sayılı Avrupa Birliği Genel Veri Koruma Tüzüğüdür (Tüzük ya da GDPR).

Kişisel verilerin korunması hukukunun gelişiminin ve ilgili düzenlemelerin analiz edilmesi ve Tüzüğün kabul edilmesinin arka planının anlaşılması, ayrıca Tüzüğün detaylıca incelenmesi amacıyla makale iki ana bölüme ayrılmıştır. Bu doğrultuda, 1. Bölüm'de kişisel verilerin korunması hakkının yer aldığı başlıca uluslararası düzenlemelere yer verilecektir. 2. Bölüm'de ise Tüzüğün kapsamı, getirdiği yenilikler, düzenlediği ilkeler, haklar ve yükümlülükler ile kurduğu sistem incelenecektir.

§ 1. Kişisel Verilerin Korunması Hakkı

Kişisel verilerin korunması hakkı aslında geçmişten beri var olan, fakat günümüzde çok hızlı değişen ve gelişen teknoloji ile birlikte daha görünür hale gelen, önemi artan ve kapsamı genişleyen bir haktır. Bu hak, başlı başına bağımsız bir hak veya diğer bazı hakların bir parçası olarak, yarım asır önce düzenlenmiş belgeler ile dahi korunmaya çalışılmıştır.

Makalenin I. Bölümünde, kişisel verilerin korunması hakkının farklı dönemlerde farklı uluslararası organizasyonlar tarafından nasıl değerlendirildiği, ardından da bu hakkın uluslararası mahkemelerce nasıl yorumlandığı incelenecektir.

I. Kişisel Verilerin Korunması Hakkının Gelişimi

Kişisel verilerin korunması hakkı, uzun bir süre "özel hayatın gizliliği" veya "özel ve aile hayatına saygı" başlıkları altında değerlendirilmiştir. Zamanla bu hakların kapsamlarının birbirinden farklılığı kabul edilmiş ve "kişisel verilerin korunması hakkı" temel haklar içerisinde, ayrı ve bağımsız bir hak olarak değerlendirilmeye başlanmıştır. Gerçekten de birbiriyle çok yakından ilgili olan bu iki hak, gerek içerikleri, gerek devletlere yükledikleri yükümlülükler düşünüldüğünde tam olarak örtüşmemektedir. Örneğin; özel hayatın gizliliği hakkı genel itibariyle devletlerin bireylerin özel hayatına müdahalesinin yasaklanması nosyonunu korurken, kişisel verilerin korunması hakkı ona kıyasla daha aktif, kişisel verilerin işlenmesi söz konusu olduğunda ilgili bireylerin menfaatlerini korumak amacıyla denetim ve denge sistemlerinin kurulmasını içeren

bir haktır.[163] Kişisel verilerin korunması hakkının gelişimi ve kapsamının tam olarak anlaşılabilmesi için, bu hakkı içeren uluslararası düzenlemelerin incelenmesi faydalı olacaktır.

A. OECD

Ekonomik İş Birliği ve Kalkınma Teşkilatı (OECD), 23.09.1980 tarihinde *Özel Yaşamın Gizliliğinin ve Sınır Ötesi Kişisel Veri Dolaşımının Korunmasına İlişkin Rehber İlkeler*'i (OECD Rehber İlkeleri) kabul etmiş ve böylelikle kişisel verilerin korunması ile ilgili uluslararası alanda adım adan ilk kuruluş olmuştur.[164] Söz konusu ilkeler bağlayıcılık taşımamaktadır ve tavsiye niteliğindedir.[165] Yumuşak hukuk kuralı (soft law) olarak nitelendirilen bu kuralların her ne kadar kâğıt üzerinde ve doğrudan bir bağlayıcılığı olmasa da, bunların ülkelerin çoğu tarafından benimsenmesi halinde, ilgili alanda temel başvuru kaynağı olmaktadır[166]. Nitekim OECD'nin Rehber ilkeleri de bu niteliğe ulaşmıştır.

Rehber ilkeler, sekiz temel prensipten oluşur: (1) *Veri toplamanın sınırlı olması ilkesi*, (2) *Veri niteliği ilkesi*, (3) *Amacın belirli olması gerektiği ilkesi*, (4) *Kullanımın sınırlanması ilkesi*, (5) *Veri güvenliği ilkesi*, (6) *Açıklık ilkesi*, (7) *Bireyin katılımı ilkesi*, (8) *Hesap verme zorunluluğu ilkesi*.

OECD ilkelerinin günümüzde yetersiz kalmasının sebebi, bu ilkelerin teknolojinin şimdiki kadar gelişmiş olmadığı, örneğin; bireylerin sosyal medya hesaplarından kendilerine dair pek çok bilgiyi ve görseli dünyanın her yerinde erişime açık olarak paylaşmadıkları bir dönemde kabul edilmiş olmasıdır. Gelişen teknoloji ve artan internet kullanımı, ilkelerin yayınlandığı zamanda öngörülemeyen yeni riskler ortaya çıkarmıştır.[167] Ayrıca, ilkelerin asıl düzenlenme amacının üye devletlerin ekonomik alanda geliştirilmesi amacından kaynaklanması da bireylerin kişisel verilerinin korunmasının tüm boyutlarıyla incelenmemesine sebep olmuştur.[168]

Bağlayıcı olmamasına rağmen üye devletler kişisel verilerin korunması hukuku alanındaki düzenlemelerinde OECD İlkeleri'ni göz önünde bulundurarak hareket etmiştir.[169]

---

163 **Christos Giakoumopoulos/Giovanni Buttarelli/Michael O'Flaherty**, Handbook on European Data Protection Law, Publications Office of the European Union, Luxembourg, 2018, s. 19.

164 **Murat Volkan Dülger**, Kişisel Verilerin Korunması Hukuku, Hukuk Akademisi, İstanbul, 2019, s. 30.

165 **Hüseyin Murat Develioğlu**, 6698 sayılı Kişisel Verilerin Korunması Kanunu ile Karşılaştırmalı Olarak Avrupa Birliği Genel Veri Koruma Tüzüğü Uyarınca Kişisel Verilerin Korunması Hukuku, On İki Levha Yayıncılık, İstanbul, 2017, s. 7.

166 Yumuşak hukuk kuralı hakkında ayrıntılı bilgi için bkz: **Andrew T. Guzman/Timothy L. Meyer**, International Soft Law, Journal of Legal Analysis, Volume 2, Issue 1, Spring 2010, s. 171–225.

167 **Develioğlu**, s. 7.

168 **Dülger**, s. 50.

169 **Dülger**, s. 51.

B. Birleşmiş Milletler

1. İnsan Hakları Evrensel Beyannamesi

10 Aralık 1948 tarihinde kabul edilen İnsan Hakları Evrensel Beyannamesinde kişisel verilerin korunması hakkı ayrı bir hak olarak düzenlenmemiştir. Fakat bu durum hakkın korunmasız bırakıldığı anlamına gelmemektedir. Beyannamenin 12. maddesinde hiç kimsenin özel hayatı, ailesi, meskeni veya yazışması konularında keyfi müdahaleye, şeref ve şöhretine karşı tecavüzlere maruz bırakılamayacağı ve herkesin bu karışma ve tecavüzlere karşı kanun yoluyla korunmaya hakkı olduğu[170] belirtilmiştir. Birleşmiş Milletler, kişisel verilerin korunmasını özel yaşamın gizliliği kapsamında değerlendirmiştir.

2. Birleşmiş Milletler Medeni ve Siyasi Haklara İlişkin Uluslarası Sözleşme

Kişisel verilerin korunması hakkı, 23 Mart 1976 tarihinde yürürlüğe giren *Medeni ve Siyasi Haklara İlişkin Uluslarası Sözleşme*'de; hiç kimsenin özel ve aile yaşamına, konutuna veya haberleşmesine keyfi veya hukuka aykırı olarak müdahale edilemeyeceği ve onuru veya itibarının hukuka aykırı saldırılara maruz bırakılamayacağı, ayrıca herkesin bu tür saldırılara veya müdahalelere karşı hukuk tarafından korunma hakkına sahip olduğunun düzenlendiği *"mahremiyet hakkı"* altında değerlendirilmiştir.[171] Örneğin, BM İnsan Hakları Komitesi mahremiyet hakkının incelendiği 16. genel yorumunda; kamu otoritelerinin, özel kişi veya kurumların bilgisayarlarda, veri bankalarında veya benzeri cihazlarda kişisel bilgi toplanması veya saklanmasının hukuki düzenlemeye tabii olması gerektiğini belirtmiştir.[172]

3. Bilgisayara Geçirilmiş Kişisel Veri Dosyalarının Düzenlenmesine İlişkin Rehber İlkeler

Yukarıda belirtildiği üzere, Birleşmiş Milletler, kişisel verilerin korunması hakkını özel hayatın gizliliği altında değerlendirmektedir. Bununla birlikte, gelişen teknoloji ve bilgisayar kullanımının yaygınlaşması, *Bilgisayara Geçirilmiş Kişisel Veri Dosyalarının Düzenlenmesine İlişkin Rehber İlkeler*'in (BM Rehber İlkeleri) yayınlanması gerekliliğini doğurmuştur.[173] Söz konusu ilkeler, doğrudan kişisel verilerin korunması hakkına ilişkin ilk Birleşmiş Milletler düzenlemesi olması sebebiyle büyük önem arz etmektedir.[174] İlgili kılavuzda aşağıdaki ilkeler

---

170 UN General Assembly, Universal Declaration of Human Rights, 10 Aralık 1948, 217 A (III), m. 12.

171 UN General Assembly, International Covenant on Civil and Political Rights, 16 Aralık 1966, United Nations, Treaty Series, vol. 999, p. 171, m. 17.

172 UN Human Rights Committee (HRC), CCPR General Comment No. 16: Article 17 (Right to Privacy), The Right to Respect of Privacy, Family, Home and Correspondence, and Protection of Honour and Reputation, 8 Nisan 1988, s. 10.

173 **Dülger**, s. 53.

174 **Dülger**, s. 53.

düzenlenmiştir: "*Hukuka uygunluk ve dürüstlük ilkesi*", *"doğruluk ilkesi"*, *"amacın belirliliği ilkesi"*, *"ilgili kişinin verilerine erişim hakkının bulunması ilkesi"*, *"verilerin güvenliği ilkesi"*, *"ayrımcılık yasağı ilkesi"*, *"denetim ve yaptırım ilkesi"*, *"sınır ötesi veri akışı ilkesi"*.

Söz konusu prensipleri düzenlemek suretiyle BM Rehber İlkeleri, üye ülke mevzuatlarında yer alması gereken asgari standartları belirlemeyi amaçlamıştır.[175]

C. Avrupa Konseyi

1. 108 No'lu Kişisel Verilerin Otomatik İşleme Tabii Tutulması Karşısında Bireylerin Korunması Sözleşmesi

1960'lı yıllarda bilişim teknolojilerinin ortaya çıkması ile birlikte bireylerin kişisel verilerinin korunmasını sağlamak için daha detaylı düzenlemelere ihtiyaç duyulmaya başlandı. Bu gereksinimi karşılamak amacıyla Avrupa Konseyi tarafından 28 Ocak 1981 tarihinde 108 No'lu Kişisel Verilerin Otomatik İşleme Tabii Tutulması Karşısında Bireylerin Korunması Sözleşmesi (108 No'lu Sözleşme)[176] imzalandı. Bu sözleşme, kişisel verilerin korunması alanında bağlayıcı nitelikteki ilk uluslararası sözleşme olması nedeniyle büyük önem arz eder. Sözleşme, bireyleri kişisel verilerinin işlenmesine bağlı olarak ortaya çıkabilecek zararlardan korumanın yanı sıra, sınırlararası veri akışlarını düzenlemeyi hedefler.[177]

108 No'lu Sözleşme, kamu sektöründe ve özel sektörde gerçekleştirilen her türlü veri işleme faaliyetine uygulanır. Buna yargı ve emniyet teşkilatının veri işlemesi de dahildir[178]. İleride bahsedileceği üzere, bu yönüyle Avrupa Birliği Genel Veri Koruma Tüzüğü'nden farklılaşmaktadır. Çünkü Tüzük, yargı ve emniyet teşkilatı tarafından gerçekleştirilen veri işleme faaliyetlerini kapsam dışı bırakmıştır.

Bu sözleşme ile birlikte, otomatik işlemeye konu olan kişisel verilerin *"adil bir biçimde ve yasal yoldan elde edilip işlenmesi"*, *"belirli ve meşru amaçlar için kaydedilmesi ve bu amaçlara aykırı kullanılmaması"*, *"kaydedilmelerinin amaçlara uygun ve yerinde olması ve aşırı olmaması"*, *"doğru olmaları ve gerektiğinde güncellenmeleri gerektiği"*, *"ilgili kişilerin kimliklerini belirlemeye, kaydedilme amaçlarını gerçekleştirmek için gerekli olan süreyi aşmayacak şekilde imkan verecek bir biçimde saklanması"* prensipleri düzenlenmiştir.[179] Ek olarak, iç hukukta uygun

---

175 **Develioğlu**, s. 10.
176 Council of Europe, Convention for the Protection of Individuals with Regard to the Automatic Processing of Individual Data, 28 Ocak 1981, ETS 108 (Convention 108).
177 **Giakoumopoulos/Buttarelli/O'Flaherty**, s. 24.
178 **Giakoumopoulos/Buttarelli/O'Flaherty**, s. 24.
179 Convention 108, m. 5.

güvenceler sağlanmadıkça özel veri kategorilerinin, yani bireylerin ırksal kökenlerini, siyasi düşüncelerini, dinlerini veya diğer inançlarını ortaya koyan kişisel veriler ile sağlık veya cinsel hayatları ve ceza mahkumiyetleriyle ilgili kişisel verilerin, otomatik işleme tabi tutulamayacağı açıkça belirtilmiştir.[180]

108 No'lu Sözleşmede ele alınmış bir diğer husus ise, bireylerin kendileri ile ilgili olarak saklanan kişisel verileri öğrenme ve gerektiğinde bunları düzelttirme, eğer veriler sözleşmede belirtilmiş ilkelere vücut veren iç hukuk hükümlerinin ihlali suretiyle işlenmiş ise bunları sildirtme hakkıdır.[181]

Sözleşmede belirlenmiş haklar, 9. madde uyarınca, yalnızca (a) taraf devletin kanunlarında öngörülmüş olması ve (b) demokratik bir toplumda (i) devlet güvenliğinin korunması, kamu güvenliği, devletin mali menfaatleri veya suçların önlenmesi veya (ii) ilgili kişinin veya başkasının hak ve özgürlüklerinin korunması için gerekli bir önlem oluşturması hallerinde sınırlanabilecektir.[182] Ayrıca, sözleşme, taraf devletler arasında kişisel verilerin serbest aktarımını öngörürken, yasal düzenlemelerin bu sözleşme ile getirilen seviyede bir koruma sağlamadığı devletlere veri aktarılmasına bazı sınırlamalar getirmektedir.[183]

Bir diğer önemli nokta ise, 108 No'lu Sözleşme AİHM'in yargı yetkisi altında olmasa da, AİHS'in 8. maddesi (özel ve aile hayatına saygı hakkı) kapsamında inceleme yaparken, mahkeme, bu sözleşmeyi dikkate almış ve sözleşmede belirlenmiş prensipler ışığında bu hakka bir müdahale olup olmadığına karar vermiştir.[184]

2001 yılında, 108 No'lu Sözleşme'deki eksiklikleri gidermek için bir adım atılarak, bu sözleşmeye ek niteliğindeki *Kişisel Verilerin Otomatik İşleme Tabi Tutulması Karşısında Bireylerin Korunması Sözleşmesine Ek Denetleyici Makamlar ve Sınıraşan Veri Akışına İlişkin Protokol* kabul edilmiştir.[185] Bu kapsamda Ek Protokol, taraf olmayan devletlere sınıraşan veri akışı ve yerel denetleyici makamlarının kurulmasının zorunluluğu konularını düzenlemiştir.[186]

2. 108 +

18 Mayıs 2018 tarihinde kabul edilen *Kişisel Verilerin İşlenmesine İlişkin Bireylerin Korunmasına İlişkin Sözleşmede Değişiklik Yapılmasına Daire Protokol*'ün *(108+)* imzalanması

180 Convention 108, m. 6.
181 Convention 108, m. 8.
182 Convention 108, m.9.
183 **Giakoumopoulos/Buttarelli/O'Flaherty**, s. 25.
184 **Giakoumopoulos/Buttarelli/O'Flaherty**, s. 25.
185 **Dülger**, s. 56.
186 **Giakoumopoulos/Buttarelli/O'Flaherty**, s. 26;

ile 108 No'lu Sözleşme modernize edilmiş ve bilişim teknolojilerinin getirdiği yeniliklere uyum sağlanması, dijital alanda gizliliğin korunmasının pekiştirilmesi ve sözleşmenin takip mekanizmalarının güçlendirilmesi hedeflenmiştir.[187] Ek Protokol, 108 No'lu Sözleşmenin önemli prensiplerini tekrar teyit ederek sabitleştirmiş, ayrıca veri işleyen kişilerin sorumluluklarını ve hesap verebilirliklerini artırmış ve bireylere yeni haklar tanımıştır.[188] Fakat 108+ henüz Türkiye tarafından onaylanarak iç hukukumuza dahil edilmemiştir.

3. Avrupa İnsan Hakları Sözleşmesi

II. Dünya Savaşı'nın ardından Avrupa'daki devletleri bir araya getirmek, hukuku, demokrasiyi, insan haklarını ve sosyal gelişimi teşvik etmek amacıyla, Avrupa Konseyi, 4 Kasım 1950 tarihinde *Avrupa İnsan Hakları Sözleşmesi*'ni *(AİHS)* kabul etmiştir. AİHS'in 8. maddesinde "özel ve aile hayatına saygı hakkı" düzenlenmiş olup[189] bu hak uyarınca "herkes özel ve aile hayatına, konutuna ve yazışmasına saygı gösterilmesi hakkına sahiptir". Kişisel verilerin korunması hakkı da, bu hak ile korunan kavramlardan biridir. Nitekim, Avrupa İnsan Hakları Mahkemesi (AİHM) birçok kararında devletin gözetim faaliyetlerinin kişilerin özel hayatlarına bir müdahale olduğunu belirtmiştir.[190] Fakat belirtmek gerekir ki, özel hayata saygı hakkı mutlak, dokunulmaz bir hak değildir. Yukarıda bahsedilen maddenin 2. fıkrasında bu hakka müdahaleyi meşru hale getirebilecek amaçlara yer verilmiştir.[191]

Ayrıca, AİHM, özel hayata saygı hakkının yalnızca pasif bir hak olmadığını ve hakkın içeriğinin yerine getirebilmesi için bazı durumlarda devletlere aktif yükümlülükler de yüklediğini pek çok kararında dile getirmiştir.[192]

---

187 **Dülger**, s. 55; **Giakoumopoulos/Buttarelli/O'Flaherty**, s. 26.

188 **Giakoumopoulos/Buttarelli/O'Flaherty**, s. 26.

189 **Giakoumopoulos/Buttarelli/O'Flaherty**, s. 22.

190 **Giakoumopoulos/Buttarelli/O'Flaherty**, s. 23; AİHM, Klass ve Diğerleri v. Almanya, No. 5029/71, 6 Eylül 1978; AİHM, Rotaru v. Romanya [GC], No. 28341/95, 4 Mayıs 2000; AİHM, Szabó and Vissy v. Hungary, No. 37138/14, 12 Ocak 2016.

191 AİHS m. 8(2): "Bu hakkın kullanılmasına bir kamu makamının müdahalesi, ancak müdahalenin yasayla öngörülmüş ve demokratik bir toplumda ulusal güvenlik, kamu güvenliği, ülkenin ekonomik refahı, düzenin korunması, suç işlenmesinin önlenmesi, sağlığın veya ahlakın veya başkalarının hak ve özgürlüklerinin korunması için gerekli bir tedbir olması durumunda söz konusu olabilir."

192 **Giakoumopoulos/Buttarelli/O'Flaherty**, s. 23. Örneğin; AİHM, I v. Finlandiya, No. 20511/03, 17 Temmuz 2008; AİHM, K.U. v. Finlandiya, No. 2872/02, 2 Aralık 2008.

D. Avrupa Birliği

1. 95/46/EC Sayılı Kişisel Verilerin İşlenmesi ve Serbest Dolaşımı Bakımından Bireylerin Korunmasına İlişkin Avrupa Parlamentosu ve Avrupa Konseyi Direktifi

95/46/EC sayılı *Kişisel Verilerin İşlenmesi ve Serbest Dolaşımı Bakımından Bireylerin Korunmasına İlişkin Avrupa Parlamentosu ve Avrupa Konseyi Direktif*'i *(Direktif),* 24 Ekim 1995 tarihinde yayınlanmış ve Avrupa Birliği Genel Veri Koruma Tüzüğüyle yürürlükten kaldırılana kadar AB'de veri korumasına ilişkin başlıca yasal düzenleme olmuştur.

Direktif, pek çok Üye Devletin iç hukuklarında daha önceden veri koruması ile ilgili hukuki düzenleme yaptığı bir zamanda, kişisel verilere daha güçlü bir koruma sağlanması ve Üye Devletlerin iç hukuklarını uyumlaştırma ve kişisel verilerin serbest dolaşımını sağlama gereksinimleri sebebiyle ortaya çıkmıştır.[193] Fakat, AB Direktifleri tüm AB ülkelerine doğrudan uygulanmaz; Direktif'te yer alan kurallar, ayrıca bu devletlerin ulusal hukuklarına aktarılmalıdır. Bu aktarım gerçekleşirken, Üye Devletlerin takdir hakkı (ve dolayısıyla marjı) söz konusudur.[194] Bu nedenle, Direktif, farklı ülkelerde farklı şekillerde yorumlanmış ve iç hukuklara yeknesak olarak aktarılamamıştır. Dolayısıyla, Direktif, AB'de kişisel verilerin korunmasına ilişkin yeknesaklığın sağlanmasında başarısız olmuştur.[195]

Genel olarak Direktif, 108 No'lu Sözleşme ve ulusal hukuklarda yer alan ilkeleri yansıtmakta ve çoğunlukla bu ilkeleri detaylandırmaktadır. Direktif'te temel olarak benimsenmiş prensipler *meşruluk ve adilllik*; *kişisel verilerin açık, belirli ve meşru amaçlar için toplanması*; *şeffaflık*; *orantılılık*; *güvenlik* ve *veri işlemenin denetime tabi olmasıdır*.[196] Ayrıca, Direktif ve 108 No'lu Sözleşme arasında bir etkileşim mevcuttur. Bu etkileşim, her iki belgeyi de kişisel verilerin korunmasına ilişkin olarak olumlu yönde etkilemektedir.[197]

Son olarak belirtmek gerekir ki 6698 sayılı Kişisel Verilerin Korunması Kanunu'nun hazırlanmasında Direktif önemli ölçüde yol gösterici olmuştur.

2. Avrupa Birliği Temel Haklar Şartı

7 Aralık 2000 tarihinde imzalanan ve 1 Aralık 2009 tarihli Lizbon Anlaşması'nın kabul edilmesiyle bağlayıcılık kazanan *Avrupa Birliği Temel Haklar Şartı (AB Şartı)*, kişisel verilerin korunması hakkını ayrı ve bağımsız bir hak olarak düzenlemiştir. AB Şartı'nın *"kişisel verilerin*

193 **Giakoumopoulos/Buttarelli/O'Flaherty**, s. 29.
194 **Giakoumopoulos/Buttarelli/O'Flaherty**, s. 50.
195 **Dülger**, s. 59.
196 **Dülger**, s. 58.
197 **Giakoumopoulos/Buttarelli/O'Flaherty**, s. 29.

korunması" başlıklı 8. maddesinin 1. fıkrasına göre *"herkes, kendisine ilişkin kişisel bilgilerinin korunmasını isteme hakkına sahiptir."* Aynı maddenin 2. fıkrasında ise kişisel verilerin *"belirtilen amaçlar için ve ilgili kişinin muvafakatine veya yasada öngörülen başka meşru temele dayalı olarak adil şekilde"* kullanılması gerektiği ve *"herkesin kendisi hakkında toplanmış olan bilgilere erişme ve bunlarda düzeltme yaptırma hakkına"* sahip olduğu hususları düzenlenmiştir. Bunlara ek olarak AB Şartı, söz konusu ilkelerin uygulanması için *"bağımsız bir makam tarafından denetim"* yapılmasını öngörmüştür.[198]

Bu düzenleme ile kişisel verilerin korunması hakkı insan hakları ile temel hak ve özgürlükler kapsamında değerlendirilmiş, ayrıca özel hayatın gizliliğinden de ayrılmıştır; böylece, kişisel verilerin korunması hakkının önemi ortaya konmuştur.[199]

3. Adli ve Kolluk Teşkilatında Kişisel Verilerin Korunmasına İlişkin 2016/680 Sayılı Direktif

96/46/EC sayılı Direktif adli ve kolluk teşkilatının faaliyetleri için uygulama alanı bulmamaktaydı. Bu nedenle, verilerin korunması ile diğer meşru menfaatler arasında bir dengenin kurulabilmesi için başka birtakım belgelerin düzenlenmesi gerekliydi. Emniyet teşkilatının kişisel veri işlemesi ile ilgili olarak AB kapsamında gerçekleştirilen ilk yasal düzenleme, AB Konseyinin polis ve cezai konularda adli iş birliği hakkında yayınladığı 2008/977/JHA sayılı Çerçeve Kararı'dır. Bu kararın kuralları yalnızca Üye devletler arasındaki polis ve yargı verisi değişimine uygulanmakta, emniyet teşkilatı tarafından ulusal düzeydeki kişisel veri işlemelerini ise kapsam dışı bırakmaktaydı. AB Parlamentosu ve Konseyi'nin 27 Nisan 2016 tarihli ve 2016/680 sayılı *"Yetkili Makamlar Tarafından Suçun Önlenmesi, Soruşturulması, Tespiti veya Kovuşturulması veya Cezai Süreçlerin Yürütülmesi Amacıyla İşlenen Kişisel Verilere İlişkin Gerçek Kişilerin Korunmasına ve Bu Tür Verilerin Serbest Dolaşımına Dair Direktifi"* 2008/977/JHA sayılı Çerçeve Kararı yürürlükten kaldırmış ve yukarıda bahsedilen eksikliği gidermiştir. Avrupa Birliği Genel Veri Koruma Tüzüğüne paralel olarak düzenlenen 2016/680 sayılı bu Direktif, emniyet teşkilatı bağlamında kişisel verilerin korunması ile ilgili olarak ayrıntılı bir sistem kurmakla birlikte, kamu güvenliğini ilgilendiren veri işlemenin özelliklerini de dikkate almıştır.[200]

Bu Direktif, ceza yargılamalarına dahil olan çeşitli kategorilerdeki bireylerin kişisel verilerinin korunmasını sağlamaktadır. Polis ve ceza yargılaması yetkilileri suçun önlenmesi,

198 European Union, Charter of Fundamental Rights of the European Union, 26 Ekim 2012, 2012/C 326/02, m. 8.
199 **Dülger**, s. 63.
200 **Giakoumopoulos/Buttarelli/O'Flaherty**, s. 31, 32.

soruşturulması, tespiti veya kovuşturulması ve cezai süreçlerin yürütülmesi amaçlarıyla kişisel veri işlerken, bu direktifin hükümlerine uygun davranmak yükümlülüğü altındadır.[201]

Genel olarak bu Direktif, Avrupa Birliği Genel Veri Koruma Tüzüğündeki ilke ve tanımlara dayanmakta olsa da, polis ve ceza yargılaması alanlarının doğasını dikkate almaktadır.[202]

4. Avrupa Parlamentosu ve Konseyinin 2002/58/EC Sayılı Elektronik Haberleşme Sektöründe Özel Alanın Korunması ve Kişisel Bilgilerin İşlenmesi Direktifi

12 Temmuz 2012 tarihinde kabul edilen 2002/58/EC sayılı *Elektronik Haberleşme Sektöründe Özel Alanın Korunması ve Kişisel Bilgilerin İşlenmesi Direktifi (E-Gizlilik Direktifi)*[203], kişisel verilerin telekomünikasyon ve iletişim hizmetleri alanındaki güvenliği, kişisel veri ihlallerinin bildirimi ve bu iletişimlerin gizliliği ile ilgili kuralları düzenlemektedir.[204]

E-Gizlilik Direktifinde sıkça 95/46/EC sayılı Direktife atıf yapılmış olup, esas itibariyle söz konusu Direktifi tamamlayıcı niteliktedir. Ek olarak, bu direktif üye devletlere söz konusu kuralları iç hukuklarına aktarmaları yönünde yükümlülük getirmiştir.[205]

5. 2006/24/EC Sayılı İletişim Trafik Verilerinin Saklanması Direktifi

15 Mart 2006 tarihinde, Londra Metrosunda yaşanan 7 Temmuz 2005 tarihli bombalı saldırıyı takiben ve onun etkisiyle 2006/24/EC sayılı *İletişim Trafik Verilerinin Saklanması Direktifi* kabul edilmiştir. Bu direktif, iletişim trafik bilgileri ve yer bilgileri ile ilgili hususları düzenlemektedir. Söz konusu direktif uyarınca iletişim hizmetleri kullanan kişilerin iletişim içeriği haricindeki bilgileri yalnızca ciddi suç şüphesi halinde saklanabilecektir.[206]

6. 45/2001 ve 2018/1725 Sayılı Avrupa Birliği Kurumları Veri Koruma Tüzükleri

95/46/EC sayılı Direktif sadece üye devletler için uygulanabilir olduğundan, AB kurum ve organlarının gerçekleştirdiği veri işleme faaliyetlerini düzenleyecek hukuki bir düzenleme ihtiyacıyla 45/2001 sayılı *Avrupa Birliği Kurumları Veri Koruma Tüzüğü* kabul edilmiştir. 45/2001 sayılı Tüzükte genel itibariyle AB veri koruma rejiminin ilkeleri benimsenmiştir. Tüzüğün uygulama alanı Birlik organ ve kurumlarınca işlenen kişisel verilerdir. Ayrıca, bu tüzük hükümlerinin uygulanmasının takip edilmesi amacıyla bağımsız bir denetim makamı olan Avrupa

---

201 **Giakoumopoulos/Buttarelli/O'Flaherty**, s. 282.
202 **Giakoumopoulos/Buttarelli/O'Flaherty**, 283.
203 European Parliament and Council of Europe, Directive 2002/58/EC Concerning the Processing of Personal Data and the Protection of Privacy in the Electronic Communications Sector, 12 Temmuz 2012 (E-Privacy Regulation).
204 **Giakoumopoulos/Buttarelli/O'Flaherty**, s. 33; E-Privacy Regulation, m. 4.
205 **Dülger**, s. 63.
206 **Dülger**, s. 63.

Veri Koruma Denetçisi (European Data Protection Supervisor) tesis etmiştir.[207] Avrupa Veri Koruma Denetçisi, veri koruma hukukuna ilişkin düzenlemelerde Birliğe danışmanlık vermek, Birlik kurumlarında veri koruma hukukunun uygulanmasını sağlamak, kurumları denetlemek ve koordinasyonu sağlamakla görevlidir.

GDPR'ın yürürlüğe girmesinden sonra 23 Ekim 2018'de 45/2001 sayılı Tüzüğü ilga eden ve yerine GDPR'la uyumlu düzenlemeler getiren 2018/1725 sayılı Tüzük kabul edilmiştir. Bu yeni Tüzük GDPR ilke ve esaslarını, kamu sektörünün veri işleme konusundaki özelliklerini dikkate alarak AB kurum, kuruluş ve yetkililerinin işlediği veriler bakımından uyarlamıştır. Tüzükte GDPR hükümleri büyük ölçüde benimsenmekle birlikte Birlik bünyesinde kurum ve kuruluşların işleyeceği veriler bakımından bazı istisna halleri düzenlenmiştir. 2018/1725 sayılı Tüzükle AB veri koruma reformunun önemli bir ayağının daha tamamlandığı ve Birlik veri koruma hukukunun daha tutarlı ve modern bir yapıya kavuşturulmuş olduğu söylenebilir[208].

7. 206/679 Sayılı Avrupa Birliği Genel Veri Koruma Tüzüğü

Yukarıda bahsedildiği üzere, 95/46/EC sayılı Direktif bilişim teknolojilerinin günümüzdeki kadar gelişmiş olmadığı bir dönemde kabul edilmiş olup, amaçlarından biri olan AB ülkelerinde kişisel verilerin korunması hukukunda yeknesaklığı da sağlayamamıştır. Bu durum, AB veri koruma yasalarının yeniden düzenlenmesi gereğini ortaya çıkarmıştır ve bu ihtiyaçtan hareketle Mayıs 2016'da Avrupa Birliği Genel Veri Koruma Tüzüğü kabul edilmiştir.[209]

II. Kişisel Verilerin Korunması Hakkının Sınırlandırılması

Kişisel verilerin korunması hakkı ne bağımsız olarak ne de özel yaşamın gizliliği hakkı altında düşünüldüğünde mutlak bir haktır. Dolayısıyla bu hak belirli şartların varlığı halinde meşru olarak sınırlanabilir. Bir hakkın meşru olarak sınırlanmasından bahsedilebilmek için üç aşamalı bir test uygulanır:

(1) Söz konusu müdahale hukuki düzenlemeler tarafından öngörülmüş olmalı ve müdahaleyi düzenleyen mevzuat keyfilikten korumayı sağlayacak nitelikte olup, sonuçları açısından öngörülebilir olmalıdır.

(2) Söz konusu müdahale meşru bir amaç gütmelidir.

---

207 **Giakoumopoulos/Buttarelli/O'Flaherty**, s. 34, 35.

208 2018/1725 sayılı Tüzük kabul edilmeden önce kabul edilmiş olan GDPR'ın gerekçesinin 17. maddesinde 45/2001 sayılı Tüzüğün güncellenerek GDPR'la uyumlu hale getirilmesi gerektiği hususu açıkça belirtilmiştir.

209 **Giakoumopoulos/Buttarelli/O'Flaherty**, s. 30.

(3) Söz konusu müdahale demokratik bir toplumda gerekli olmalıdır. Bunun sağlanması için bu müdahale; (a) gerekli ve zararı önlemek açısından ölçülü olmalı ve (b) hakkın özüne zarar vermemelidir.

Bu noktada AİHS'te özel hayata saygı hakkının sınırlandırılması hususunda hangi amaçların meşru amaç kabul edildiği, 8. maddenin 2. fıkrasında belirtilmiştir. Buna göre; "*Bu hakkın kullanılmasına bir kamu makamının müdahalesi, ancak müdahalenin yasayla öngörülmüş ve demokratik bir toplumda ulusal güvenlik, kamu güvenliği, ülkenin ekonomik refahı, düzenin korunması, suç işlenmesinin önlenmesi, sağlığın veya ahlakın veya başkalarının hak ve özgürlüklerinin korunması için gerekli bir tedbir olması durumunda söz konusu olabilir.*"

§ 2. Avrupa Genel Veri Koruma Tüzüğünün Ortaya Çıkışı, Uygulama Alanı ve Temel İlkeleri

Makalenin 1. Bölümünde detaylıca anlatıldığı üzere, değişen ve gelişen teknolojinin getirdiği yenilikler ve doğurduğu riskler ile AB ülkelerinde kişisel verilerin korunması hukukunun yekneksaklaştırılması gerekliliği Avrupa Birliği Genel Veri Koruma Tüzüğü'nün (Tüzük) düzenlenmesi ihtiyacını ortaya çıkarmıştır.

Makalenin 2. Bölümünde, belirli eksiklikleri tamamlamak ve kişisel verilerin korunması hukukunu daha detaylı bir şekilde düzenlemek amacıyla düzenlenen Tüzüğün kapsamı, getirdiği yenilikler, düzenlediği ilkeler, yüklediği sorumluluklar, kurduğu sistem ve bu sistemin nasıl uygulamaya konulacağı bir bütün olarak incelenecektir.

I. Tüzüğün Ortaya Çıkma Süreci

Tüzük, kişisel verilerin korunması hakkının öneminin zamanla daha iyi anlaşılması ve bu hakka ilişkin olarak kendisinden önce var olan düzenlemelerin değişen ve gelişen teknolojiler ile birlikte bu hakkın etkin bir şekilde korunması hususunda yetersiz kalması sebepleriyle ortaya çıkmıştır[210].

Avrupa Birliği Komisyonu, bu ihtiyaçları göz önünde bulundurarak 95/46/EC sayılı Direktif'te kapsamlı değişiklikler yapılmasını içeren bir Öneri hazırlamış ve 25 Ocak 2012 tarihinde yayımlamıştır.[211] Söz konusu Öneri'yi Avrupa Komisyonu adına Başkan Yardımcısı

---

210 **Jan Philipp Albrecht**, "How The GDPR Will Change The World", Eur. Data Prot. L. Rev. 287, 2016, s. 289.

211 Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation), Sec (2012), Brussels, 25 January 2012, C-7-0025/12, http://www.europarl.europa.eu/RegData/docs_autres_institutions/commission_europeenne/com/2012/0011/COM_COM(2012)0011_EN.pdf

Viviane Reding aynı gün kamuoyuna açıklamıştır. Reding, açıklamasında 17 yıl önce Avrupa'da internet kullananların oranının yalnızca % 1 olduğunu bugün ise büyük miktarda verinin saniyeler içinde kıtalar arasında aktarıldığını, Öneri'nin sektörün sağlıklı büyümesini temin ederken, bireylerin dijital ortamda kişisel verilerinin korunmasını da güçlendireceğini vurgulamıştır.[212]

Söz konusu yetersizliğin önemli görünümlerinden biri de, kişisel verilerin korunmasının daha önce hiçbir düzenlemede Tüzükte olduğu kadar kapsamlı ele alınmamış olmasının yanı sıra, Tüzüğün yürürlükten kaldırdığı ve 1995'ten Mayıs 2018'e kadar Avrupa Birliği'nin kişisel verilerin korunması ile ilgili başlıca belgesi olan 95/46/EC sayılı Direktif'in bağlayıcı olmamasıdır.[213]

Avrupa Birliği'nde kişisel veri alanında ilk önemli düzenleme, 1995 yılında 95/46/EC sayılı Direktif ile yapılmıştır.[214] Bu Direktif 20 yıl yürürlükte kaldıktan sonra, 2016 yılında kabul edilen Genel Veri Koruma Tüzüğü (GDPR), 25 Mayıs 2018 tarihinden itibaren uygulanmaya başlamıştır. Avrupa Birliği müktesebatında, kurucu antlaşmalar, katılım antlaşmaları ve bu antlaşmaların ekleri olan protokoller birincil hukuk kaynaklarını oluştururken; tüzükler, direktifler, kararlar ise ikincil hukuk kaynaklarını oluşturmaktadır. Tüzükler (regulations) ile yönergeler (directives)[215] etkileri itibariyle birbirinden farklıdır.[216] AB Direktifleri, AB üyesi ülkelerin mevzuatlarını belirli bir konuda, somut ilke ve amaçlar doğrultusunda yaklaştırmak ve uyumlu hale getirmek amacıyla AB Bakanlar Konseyi ve AB Komisyonu tarafından çıkarılan yasal metinleri ifade eder. Direktif'e muhatap üye devletler, belirlenen süreler çerçevesinde kendi ulusal mevzuatları ile gerekli düzenlemeleri yapmakla yükümlüdürler. Ancak Direktif hükümleri üye ülkelerde doğrudan uygulama kabiliyetine sahip değildir. Buna karşılık AB Bakanlar Konseyi tarafından çıkarılan Tüzükler, genel kapsama sahiptir ve tüm AB üyesi ülkelerde doğrudan doğruya uygulanırlar. Tüzükler, Topluluk Resmi Gazetesi'nde yayımlandıktan sonra, yürürlük tarihinde tüm üye ülkeler için bağlayıcı metin halini alır.[217] Üye ülkeler bu metinleri doğrudan uygularlar. GDPR, 95/46/EC sayılı Direktif'ten farklı olarak "Tüzük (Regulation)" olarak düzenlenmiştir ve bu yönüyle tüm üye ülkeler için doğrudan bağlayıcı bir yasal metin niteliğindedir.

---

212 Commission proposes a comprehensive reform of data protection rules to increase users' control of their data and to cut costs for businesses, 25 January 2012, http://europa.eu/rapid/press-release_IP-12-46_en.htm

213 **Albrecht,** s. 289.

214 Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protectionof individuals with regard to the processing of personal data andon the free movement of such data, Official Journal, L 281, 23/11/1995, p. 31-50. (Data Protection Directive)

215 Türkçe ifadesi 'yönerge' olarak tercüme edilebilecek olan 'directives' anlaşılabilirliği ve artık Türkçe'de de bu şekilde kullanılması nedeni ile 'Direktif' olarak ifade edilecektir.

216 **Mehmet Nuri Tapan**, "Avrupa Birliği (AB) Hukukunun Kaynakları ve Ulusal Hukuka Etkileri: Avrupa Adalet Divanı", Türkiye Barolar Birliği Dergisi, S. 3, Y. 1998 (s. 971-1020), s. 993 vd.

217 **Tapan**, s. 994.

AB'nin yürürlüğe koyduğu yeni Genel Veri Koruma Tüzüğü, 95/46/EC sayılı Direktif ile kıyaslandığında bireyi daha merkeze alan anlayışı, kırtasiyecilik ve bürokrasiyi devre dışı bırakıp doğrudan uygulamaya ve sonuç almaya yönelik düzenlemeleri ve coğrafi olarak geniş uygulama alanı nedeni ile veri koruma alanında Kopernik devrimi benzeri bir etki yaratacağı ifade edilmiştir.[218] 16. yüzyılda Prusyalı matematikçi ve astronomi bilimcisi Nikolas Kopernik'in ortaya koyduğu yeni evren görüşünde[219] "dünya" değil; "güneş" merkezdedir ve gezegenler sabit bir yörünge üzerinde güneşin etrafında dönerler. Kopernik Devrimi (Copernican revolution) olarak bilinen bu anlayış, 18. yüzyılda Immanuel Kant tarafından felsefe ve düşünce dünyasında yapılmıştır.[220] Buna göre nasıl astronomide Güneş merkez konumuna gelmiş ise, bilme süreçlerinde de özne merkezde olmalı ve bilgi nesnelere değil, nesneler bilgiye uymalıdır. Yeni Tüzüğün bu çerçevede birey haklarını öne çıkaran yeni bir anlayış getirdiği vurgulanmaktadır.[221]

Yaşanan teknolojik gelişmeler ile birlikte bireylerin verilerinin korunmasına her zamankinden daha çok ihtiyaç duyulması karşısında daha 2011 yılının Haziran ayında 95/46/EC sayılı Direktif'in yenilenmesi ihtiyacından bahsedilmiştir.[222] 2012 yılı başında AB Komisyonu, bu

---

218 **Christopher Kuner**, The European Commission's Proposed Data Protection Regulation: A Copernican Revolution in European Data Protection Law, Privacy and Security Law Report, June 2012, http://robertgrzeszczak.bio.wpia.uw.edu.pl/files/2012/12/Kuner_A-Copernican-Revolution-in-European-Data-Protection-Law.pdf (Son Erişim Tarihi: 10.02.2019)

219 Nicolaus Copernicus (1473-1543). Kopernik'in teoremini açıkladığı "De revolutionibus orbium caelestium (Göksel Kürelerin Devinimleri Üzerine)" eseri 1543 yılında basılmıştır. Bununla birlikte Kopernik'in ortaya koyduğu yeni evren görüşünün, İran'ın Merage şehrinde Nasiruddin Tusi (1201-1274) tarafından kurulan Maragha Okulu çalışmaları ile ondan 200 yıl önce ortaya konulduğu artık iddiadan öte ortaya konulmuş bir gerçek halini almıştır. Nasiruddin Tusi, Batlamyus'un evren anlayışını eleştirmiş ve samanyolunun yıldızlardan oluştuğunu belirtmiş ve yeni matematik yöntemlerle "çifte bağı teorisini" oluşturmuştur. Bu teoremin Kopernik tarafından aynen kullanıldığını 1906 yılında J.L.E. Dreyer açıklamıştır. Tusi'den sonra aynı okuldan İbnü'ş Şatir (Ibn al-Shatiral) (1304-1375) güneş ve gezegen sistemini ortaya koymuştur. Kopernik'in İbnü'ş Şatır'ın "Nihâyat el-Sûl ve Ta'lîk el-Ersâd (Nihayat alsul of c Ala' al-Din)" eserlerindeki görüş ve hesaplamaları kullandığı ise ilk kez 1950 yılında Beyrut Amerikan Üniversitesi'nden E.S. Kennedy tarafından açıklanmıştır. Kopernik İbnü'ş Şatır'ın "merkür modeli" ve "ay modeli" hesaplamalarını birebir kullanmıştır. Kopernik'in bu bilim adamlarının eserlerine atıf yapmaması ve onlardan hiç bahsetmemesi, ayrıca hesaplamaları dahi aynen kendi eserine aktarması karşısında, Kopernik'in eserinin iktibasın ötesinde bir intihal olduğu akla gelmektedir. Bkz. **F. Jamil Ragep**, "Copernicus and His Islamic Predecessors: Some Historical Remarks", Mc. Gill University, History of Science Journal, N. XLV, 2007 s. 65-81.

220 What is the Copernican Revolution in Kant, https://www.the-philosophy.com/copernican-revolution-kant (Son Erişim Tarihi: 10.03.2019)

221 **Dave Elliman**, GDPR: It is time to rethink your approach to privacy, August 11, 2017, https://www.thoughtworks.com/insights/blog/gdpr-it-s-time-rethink-your-approach-privacy

222 Comprehensive Approach on Personal Data Protection in the European Union, June 2011, https://edps.europa.eu/data-protection/our-work/publications/opinions/comprehensive-approach-personal-data-protection_en

konuda değişiklik teklifi hazırlamıştır. Ardından Madde 29 Çalışma Grubu,[223] veri koruma alanında yapılacak reforma ihtiyaç duyulduğunu belirtmiştir.[224] 12 Mart 2014 tarihinde GDPR Taslağı, AB Parlamentosu tarafından kabul edilmiştir.[225] AB Konseyi, 15 Haziran 2015 tarihinde Taslak ile ilgili görüşlerini açıklamış, sonraki süreçte müzakereler devam etmiş ve süreç sonunda 27 Nisan 2016 tarihinde GDPR kabul edilerek 4 Mayıs 2016 tarihinde AB Resmi Gazetesi'nde yayımlanmıştır.[226] Tüzüğün yürürlük tarihi olarak ise GDPR'ın 99/2 maddesi ile 25 Mayıs 2018 tarihi belirlenmiştir. Tüzük, bu tarihte yürürlüğe girmiştir.

AB Komisyonu tarafından 95/46/EC sayılı Direktif'in yerini almak üzere açıklanan Genel Veri Koruma Tüzüğü 11 bölüm, 99 madde ve 173 gerekçeden (recitals)[227] oluşmaktadır.

Direktif, kişisel verilerin korunması kapsamında belirli hedefler ortaya koymuş, fakat bu hedeflerin gerçekleştirilme yöntemlerini ülkelerin kendi iç hukuk düzenlemelerine ve Direktifin belirlediği sınırlar dahilinde üye ülkelerin takdirine bırakmıştır.[228] Söz konusu Direktif doğrultusunda, ülkeler ulusal hukuklarında birbirinden farklı düzenlemelere yer vermiş olup, iç hukuktaki bu farklılıklar kişisel verilerin etkin olarak korunabilmesini önünde bir engel oluşturmuştur.[229] Tüzük, bahsi geçen problemleri aşmak düşüncesiyle tamamen bağlayıcı

---

223 Article 29 Working Group (WP 29). 1998 yılında yürürlüğe giren 95/46/EC sayılı Direktif'in 29 uncu maddesi uyarınca AB üyesi ülkelerin veri koruma otoriteleri, Avrupa Veri Koruma Denetçiliği (European Data Protection Supervisor) ve Avrupa Komisyonu (European Commission) temsilcilerinden oluşan çalışma grubunu ifade eder. Bu Çalışma Grubu karar verici olmamakla birlikte çalışmalarında bağımsızdır ve veri koruma alanında ortaya çıkan sorunların çözümü, güncel konularda görüş hazırlamak gibi yönlendirici bir etkiye sahiptir. GDPR'ın yürürlüğe girmesiyle birlikte Madde 29 Çalışma Grubu sona ermiş ve yerine Avrupa Veri Koruma Kurulu (The European Data Protection Board-EDPB) kurulmuştur. GDPR'ın 68 inci maddesiyle oluşturulan yeni Kurul, AB üyesi ülkelerin veri koruma otorite başkanları ve temsilcileri ile Avrupa Veri Koruma Denetçiliği temsilcilerinden oluşmaktadır. Bkz. European Data Protection Board, https://edpb.europa.eu/about-edpb/about-edpb_en

224 EDPS, The History of the General Data Protection Regulation, https://edps.europa.eu/data-protection/data-protection/legislation/history-general-data-protection-regulation_en (Son Erişim Tarihi: 10.03.2019)

225 Progress on EU Data protection reform now irreversible following European Parliament vote, Strasbourg, 12 March 2014, http://europa.eu/rapid/press-release_MEMO-14-186_en.htm

226 Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), Official Journal of the European Union, L 119/1, 4 May, 2016, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2016.119.01.0001.01.ENG (Son Erişim Tarihi: 10.03.2019)

227 Recitals, bir yasal metin ile ilgili beyan, açıklama ve gerekçeleri içerebilmektedir. AB müktesabatında 'recitals' politik düşünceler ile normatif dil olmaksızın, yasal metnin gerekçelerini içeren kısmı ifade etmektedir. Genellikle 'Whereas (iken, dığından anlamı verir)' ile başlarlar. Bkz. Tadas Klimas; Jurate Vaiciukaite, The Law of Recitals in European Community Legislation, ILSA Journal of International & Comparative Law, V. 15, 2008, https://www.researchgate.net/publication/228152770_The_Law_of_Recitals_in_European_Community_Legislation

228 **Dülger**, s. 66.

229 **Giakoumopoulos/Buttarelli/O'Flaherty**, s. 29.

niteliktedir ve veri korumaya ilişkin kuralların tüm üye devletlerde yeknesak şekilde uygulanmasını amaçlamaktadır.[230]

II. Temel Kavramlar

Tüzük ile ilgili detaylı açıklamalardan önce, Tüzüğün uygulama alanın, düzenlediği ilkelerin, hakların ve sorumluluklarının anlamının tam anlamıyla kavranabilmesi için, kişisel verilerin koruması hukukunun temel kavramlarının Tüzük çerçevesindeki tanımlarına değinmek gerekir.

A. Kişisel Veri

Tüzük uyarınca, "kişisel veri"; *belirli veya belirlenebilir bir gerçek kişiye ilişkin her türlü bilgidir*.[231] Yani, bir kişinin kimliğini açıkça ortaya koyan veya ek bilgiler ile ortaya konulabilir kılan bilgilerdir.[232] Bu bağlamda "belirlenmiş bir gerçek kişi" özellikle isim, kimlik numarası, konum verileri, çevrim içi tanımlayıcı ya da söz konusu gerçek kişinin fiziksel, fizyolojik, genetik, ruhsal, ekonomik, kültürel veya toplumsal kimliğine özgü bir ya da daha fazla sayıda faktöre atıfta bulunularak doğrudan veya dolaylı olarak tanımlanabilen bir kişidir.[233] Bir kişinin belirlenebilir olup olmadığı değerlendirilirken; o bireyin belirlenmesi için direkt veya dolaylı olarak kullanılabilecek ve o bireye diğerlerinden farklı bir muamelede bulunulmasını mümkün kılabilecek makul her türlü araç dikkate alınmalıdır.

Tüzükte kişisel veri kavramı genel olarak 95/46/EC sayılı Direktifle paralel olarak düzenlenmiştir. Ancak kişiyi belirlenebilir kılan her türlü verinin kişisel veri sayılmasını garanti etmek adına Tüzüğün bazı özel vurguları olduğunu belirtmek gerekir. Özellikle Gerekçe m. 30'da IP adresleri, site çerezleri gibi kişiyi belirlenebilir kılabilen çevrimiçi verilerin kişisel veri olduğunun vurgulanması Tüzüğün öne çıkan yönlerindendir[234].

B. Veri Sahibi

Bir bireyin kişisel verilerinin işlenmesi söz konusu ise, kişisel verileri işlenen bu kişi "veri sahibi"dir. Bu anlamda yalnızca gerçek kişiler veri sahibi sıfatına sahip olabilir, dolayısıyla veri

---

230 **Dülger**, s. 66.
231 General Data Protection Regulation (GDPR), m. 4(1).
232 **Giakoumopoulos/Buttarelli/O'Flaherty**, s. 83.
233 GDPR, m. 4(1).
234 **Mário Fernandes/Alberto Rodrigues da Silva/António Gonçalves**, "Specification of Personal Data Protection Requirements: Analysis of Legal Requirements based on the GDPR Regulation", https://www.researchgate.net/profile/Mario_Fernandes14/publication/324054218_Specification_of_Personal_Data_Protection_Requirements_-_Analysis_of_Legal_Requirements_from_the_GDPR_Regulation/links/5ad7b07baca272fdaf8029d1/Specification-of-Personal-Data-Protection-Requirements-Analysis-of-Legal-Requirements-from-the-GDPR-Regulation.pdf (Son erişim tarihi: 19.07.2019).

koruma kurallarından faydalanabilir.[235] Bu durum, tüzel kişilerin hiçbir şekilde yasal koruma altında olmadıkları anlamına gelmez. Makalenin 1. Bölümünde açıklandığı üzere, AİHS'te özel ve aile hayatına saygı hakkı düzenlenmiş olup, bu hak çerçevesinde kişiler özel ve aile hayatlarına saygı gösterilmesi hakkının yanı sıra, konutlarına ve yazışmalarına saygı gösterilmesi hakkına da sahiptir. AİHM, tüzel kişilere ilişkin verilerin korunmasını, özellikle konut ve yazışmalara saygı hakkı altında ele almaktadır.[236] Bu anlamda veri sahibi kavramı Tüzükte, 108 No'lu Sözleşmeye kıyasla daraltılmıştır: 108 No'lu Sözleşme uyarınca, veri korumasının asıl muhatabı gerçek kişiler olmakta birlikte, bu sözleşmede Taraf Devletler'in veri korumasını ulusal hukukları ile tüzel kişileri de kapsayacak şekilde genişletebileceğini düzenlenmiştir.[237]

Tüzükte ise kişisel verinin tanımı yapılırken açıkça "gerçek kişi" vurgusu yapılmış (m. 4), ayrıca Gerekçe m. 14'te Tüzüğün tüzel kişilerin verileri bakımından uygulanmayacağı açık bir şekilde belirtilmiştir. Bu itibarla Tüzük çerçevesinde veri sahibi tartışmasız bir şekilde sadece gerçek kişiler olabilir.

C. Kişisel Verilerin Anonim Hale Getirilmesi

Saklama süresinin sınırlandırılması ilkesi uyarınca, kişisel veriler, veri sahiplerinin yalnızca kişisel verilerin işlenme amaçlarının gerektirdiği sürece teşhis edilmesini sağlayan şekilde tutulur.[238] Dolayısıyla, kişisel verilerin işleme amacı için artık gerekli olmadığı fakat bir süre daha saklanması uygun görüldüğü noktada, ilgili veriler silinmeli veya anonimleştirilmelidir.[239]

Kişisel verilerin anonim hale getirilmesi, bir dizi kişisel veriden, bir kişiyi belirlenebilir kılan unsurların çıkarılması, takiben veri sahibinin belirlenemez hale getirilmesidir.[240] Diğer bir deyişle, kişisel verilerin başka verilerle eşleştirilse dahi hiçbir surette kimliği belirli veya belirlenebilir bir gerçek kişiyle ilişkilendirilemeyecek hale getirilmesidir.[241] Anonimleştirme işlemi sonrasında, kişinin belirlenebilir kılınması artık hiçbir şekilde mümkün olmamalıdır.[242]

D. Takma Ad Kullanımı

Takma ad kullanımı (psödonimleştirme), kişisel verilerin belirli veya belirlenebilir bir gerçek kişiyle ilişkilendirilmemesinin sağlanması amacı ile, ek bilgilerin ayrı tutulması ve teknik

---

235 GDPR, m. 4(1).
236 **Giakoumopoulos/Buttarelli/O'Flaherty**, s. 84.
237 **Giakoumopoulos/Buttarelli/O'Flaherty**, s. 85.
238 GDPR, m. 5(1)(e).
239 **Giakoumopoulos/Buttarelli/O'Flaherty**, s. 93.
240 GDPR, Gerekçe 26; **Giakoumopoulos/Buttarelli/O'Flaherty**, s. 93.
241 30224 sayılı Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi Hakkında Yönetmelik, m. 10(1).
242 GDPR, Gerekçe 26;

ve düzenlemeye ilişkin tedbirlere tabi olması koşuluyla, kişisel verilerin söz konusu ek bilgiler kullanılmaksızın spesifik bir veri sahibiyle artık ilişkilendirilemeyecek şekilde işlenmesidir.[243]

Anonim hale getirilmiş verilerin aksine, psödonimleştirilmiş veriler, kişisel veri olma niteliklerini korurlar, bu nedenle Tüzüğün uygulama alanı içerisinde kalmaya devam ederler.[244]

Kişisel veri tanımı GDPR'da, 95/46/EC sayılı Direktif'e göre daha geniş şekilde düzenlenmiştir. GDPR'da kişisel veri tanımlanmış veya tanımlanabilir bir gerçek kişiye ilişkin her türlü bilgi şeklinde tanımlanmışken; 95/46/EC sayılı Direktif'te kişisel veri ilgilisi kişi ve kişilik özellikleri ile sınırlı şekilde tanımlanmıştı (95/46/EC, m. 2/1-a). GDPR kapsamında kişiye ait isim, kimlik numarası, konum verileri, çevrimiçi tanımlayıcı ya da söz konusu gerçek kişinin fiziksel, fizyolojik, genetik, ruhsal, ekonomik, kültürel veya toplumsal kimliğine özgü bir ya da daha fazla sayıda faktörü de bu kapsamda belirtmiştir (GDPR, m. 4/1). Takma ad şeklinde kullanılan veriler de korunabilir kişisel veriler kapsamına dahil edilmiştir.

GDPR'in 4/5 maddesiyle takma ad kullanımı (pseudonymisation), kişisel verilerin tanımlanmış veya tanımlanabilir bir gerçek kişiyle ilişkilendirilmemesinin sağlanması amacı ile ek bilgilerin ayrı şekilde tutulması ile teknik/organizasyonel tedbirlere tabi tutulması koşuluyla, kişisel verilerin söz konusu ek bilgiler kullanılmaksızın spesifik bir veri sahibiyle artık ilişkilendirilemeyecek şekilde işlenmesi olarak tanımlanmıştır. Takma ad kullanımı ile oluşturulan veriler de GDPR kapsamında kişisel veriye dahil kabul edilmiştir (GDPR, rec. 26). Çünkü bu veriler ek bilgiler ile yeniden tanımlanabilir ve kişiye atfedilebilir niteliktedir. Bu açıdan anonimleştirme, takma ad kullanımından farklıdır. Anonimleştirilmiş veriler, veri konusu tanımlanamayacak hale getirilmiş verileri ifade eder. Bu nedenle GDPR veri koruma ilkeleri istatiksel ve araştırma amaçları dahil olmak üzere, anonimleştirilmiş veriler için geçerli bir koruma sistemi getirmez (GDPR, rec. 26).[245]

E. Veri İşleme

Veri işleme faaliyeti, otomatik yöntemlerle olsun veya olmasın, kişisel veri veya kişisel veri setleri üzerinde gerçekleştirilen toplama, kaydetme, düzenleme, yapılandırma, saklama, uyarlama veya değiştirme, elde etme, danışma, kullanma, iletim yoluyla açıklama, yayma veya kullanıma sunma, uyumlaştırma ya da birleştirme, kısıtlama, silme veya imha gibi herhangi bir işlem veya

243 GDPR, m. 4(5).
244 **Giakoumopoulos/Buttarelli/O'Flaherty**, s. 94.
245 Handbook on European Data Protection, s. 94.

işlem dizisidir. Diğer bir deyişle, kişisel veri üzerinde ve ona ilişkin gerçekleştiren her faaliyet veri işlemedir.[246]

F. Veri Sorumlusu ve Veri İşleyen

Veri sorumlusu, yalnız başına veya başkalarıyla birlikte kişisel verilerin işlenmesine ilişkin amaçları ve yöntemleri belirleyen gerçek veya tüzel kişi, kamu kuruluşu, kurumu veya diğer herhangi bir organdır.

Veri işleyen ise, veri sorumlusu adına kişisel verileri işleyen bir gerçek ya da tüzel kişi, kamu kuruluşu, kurumu veya diğer herhangi bir organdır.[247]

İki ya da daha fazla sayıda veri sorumlusunun işleme amaçları ve yöntemlerini ortak bir şekilde belirlediği hallerde ise bu veri sorumluları "ortak veri sorumluları"dır.[248]

Sorumlulukların belirlenmesi açısından kimin veri sorumlusu, kimin veri işleyen olduğunun belirlenmesi çok önemlidir. Veri sorumlusu ve veri işleyen arasındaki ayrım; veri sorumlusunun veri işlemenin amaçlarını ve yöntemlerini belirleyen tüzel veya gerçek kişi, veri işleyenin ise veri sorumlusu adına ve onun talimatları uyarınca veri işlemeyi gerçekleştiren kişi olmasıdır.[249]

Belirtildiği üzere, veri sorumlusu bir gerçek veya tüzel kişi, kamu kuruluşu, kurumu veya diğer herhangi bir organ olabilir. Bununla ilgili olarak Madde 29 Çalışma Grubu, bireylerin haklarını kullanabilmeleri amacı ile, veri işlemenin tüzel kişi, kamu kuruluşu, kurumu veya diğer herhangi bir organ tarafından gerçekleştirilmesi halinde, bu tüzel kişi, kuruluş, kurum veya organın içerisindeki belirli bir insanın veri sorumlusu olarak değerlendirilmesindense, ilgili tüzel kişi, kuruluş, kurum veya organın veri sorumlusu olarak düşünülmesi gerektiğini belirtmektedir.[250]

Veri işleyen, Birlik ya da Üye Devlet hukuku çerçevesinde bu yönde hareket etmesinin gerekmemesi durumunda, veri sorumlusundan aldığı talimatlar haricinde veri işleme faaliyeti gerçekleştiremez.[251] Nitekim, veri sorumlusu ve işleyen arasındaki sözleşme, bu ilişkinin kurulabilmesi için yasal bir zorunluluktur. Bu sözleşme, veri sorumlusu ile ilgili olarak işleyen açısından bağlayıcıdır ve işleme faaliyetinin konusu ve süresi, işleme faaliyetinin mahiyeti ve

246 GDPR, m. 4(2).
247 GDPR, m. 4(7), 4(8).
248 GDPR, m. 26(1).
249 **Giakoumopoulos/Buttarelli/O'Flaherty**, s. 101.
250 Article 29 Working Party (2010), Opinion 1/2010 on the concepts of "controller" and "processor", WP 169, Brussels, 16 Şubat 2010.
251 GDPR, m. 29.

amacı, kişisel verilerin türü ve veri sahiplerinin kategorileri ile veri sorumlusunun yükümlülükleri ve haklarını ortaya koyar.[252]

Veri işleyenin işleme faaliyetini veri sorumlusunun talimatlarına aykırı olarak gerçekleştirirse, veri işleyen, talimatlardan ayrıldığı ölçüde veri sorumlusu olarak değerlendirilir.[253] Böyle bir durumda, Madde 29 Çalışma Grubu ortak veri sorumluluğunun olduğunu varsaymaktadır.[254]

Değinilmesi gereken diğer bir nokta, veri işleyenin, veri sorumlusunun önceden verdiği spesifik veya genel yazılı onay olmaksızın başka bir işleyenle çalışmasının yasaklanmış olmasıdır.[255]

Veri sorumlusu, tek başına veya başkalarıyla birlikte kişisel verilerin işlenmesine ilişkin amaçları ve yöntemleri belirleyen kişi/topluluktur (GDPR, m. 4/7). İşleyici (processor) ise veri sorumlusu adına kişisel verileri işleyen kişi/topluluk olarak ifade edilmiştir (GDPR, m. 4/8).[256] 95/46/EC sayılı Direktif'te de yer alan bu farklılık, GDPR'da da korunmakla birlikte 95/46/EC sayılı Direktif'te sorumluluk sadece veri sorumluları açısından getirilmişken, GDPR ile her ikisine de belirli ölçüde sorumluluk getirilmiştir. Veri ilgilileri, GDPR'ın 79. maddesi uyarınca hem veri sorumlusu hem işleyenle karşı dava açma hakkına sahiptir. GDPR'ın 82. maddesi uyarınca veri sahibinin her ikisine karşı tazminat davası açma hakkı da bulunmaktadır. Ayrıca örneğin denetim makamına veri ihlalinin gecikmeksizin (without undue delay) bildirilmesi yükümlülüğü hem veri veri sorumluları, hem veri işleyenler için getirilmiştir (GDPR, m. 33/1-2). Bu şekilde veri işleyenler açısından da genişleyen bir sorumluluk rejimi kabul edilmiştir.

f. Ortak Veri Sorumluluğu (Joint Controllers)

Ortak veri sorumluluğu (joint controllers) terimi GDPR ile getirilen önemli yeniliklerden bir tanesidir. Bununla birlikte 95/46/EC sayılı Direktif'te yer alan veri sorumlusu tanımında da

252 GDPR, m. 28(3).

253 **Giakoumopoulos/Buttarelli/O'Flaherty**, s. 108, 109.

254 Article 29 Working Party (2010), Opinion 1/2010 on the concepts of "controller" and "processor", WP 169, Brussels, 16 Şubat 2010), s. 25.

255 GDPR, m. 28(2).

256 Bu tanımlar 95/46/EC sayılı Direktif'in 2. maddesindeki tanımlarla benzerdir. 95/46/EC sayılı Direktif'te yer alan veri sorumlusu tanımı da Avrupa Konseyi'nin veri koruması alanındaki ilk önemli sözleşme kabul edilen 108 sayılı Sözleşmesi'nin 2/d maddesinde yer alan "dosya konrolörü (controller of the file)" tanımından alınmıştır. Bkz. European Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, 28 January 1981, ETS No. 108, https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/108 Sözleşme'nin 223 sayılı Sözleşme ile güncellenen versiyonunda ise veri sorumlusu, tek başına veya diğerleriyle birlikte veri işleme konusunda karar verme yetkisine sahip olan gerçek veya tüzel kişi, kamu otoritesi, hizmeti, ajansı veya diğer herhangi bir yapı şeklinde tanımlanmıştır. Bkz. Güncellenen 108 sayılı Sözleşme, https://rm.coe.int/16808ade9d, m. 2/d).

"kişisel verilerin işlenme araçlarını ve amaçlarını tek başına veya diğerleriyle ortaklaşa belirleyen" ifadesi ile birden fazla veri sorumlusu olması halinden bahsedildiği görülmektedir.

GDPR'ın 26. maddesi "ortak veri sorumluları (joint controllers)" başlığı ile düzenlenmiştir. Maddeye göre iki ya da daha fazla sayıda veri sorumlusu şayet verilerin işleme amaçlarını ve yöntemlerini birlikte belirlemişlerse, bu halde ortak veri sorumlusu olarak nitelendirileceklerdir. Eğer bir şirket, kişisel verilerin hangi araçlarla (how) ve hangi amaçlar için (why) işleneceğini belirliyor ise o takdirde, veri sorumlusu olarak kabul edilmektedir. Eğer birden fazla şirket, bu süreci birlikte yerine getiriyor ise, şirketler "ortak veri sorumluları (joint controllers)" olarak nitelendirilecektir (GDPR, m. 26). Bu anlamda örneğin bir şirket faaliyet alanı ile ilgili bir alt şirkete çalışanlarının muhasebe işlerini yaptırıyor ise, bu alt muhasebe şirketi verileri işleyen (processor), asıl şirket ise veri sorumlusu (controller) olarak çalışanların kişisel verilerinden sorumlu olacaktır. Bir başka örnek olarak online ortamda bebek bakıcılığı hizmetleri sunan bir şirket, bir başka şirket ile de bebek için gerekli olan oyun, DVD gibi araçların kiralanması için sözleşme yapmış olabilir. Her iki şirket de, hizmetlerin sunulduğu web sitesinin teknik kurulumunda yer almaktaysalar, her iki şirket "ortak veri sorumlusu (joint controller)" sıfatı ile müşterilerinin kişisel verilerinin korunmasından sorumlu olacaklardır.[257]

Veri sorumlularının sorumlulukları AB hukuku veya üye devlet hukukunca belirlenmediği takdirde, ortak veri sorumlularının sorumlulukları ve GDPR kapsamındaki yükümlülüklere uygunlukları, aralarında yapacakları anlaşmayla şeffaf bir şekilde belirlenecektir. Bununla birlikte, veri sahibi GDPR kapsamındaki haklarını her veri sorumlusu açısından ve her birine karşı kullanabilir. Bu belirlemenin sorumluluğun açık bir şekilde tayinine imkân verecek şekilde yapılması gerekir (GDPR, rec. 79). Bu nedenle aralarındaki sorumluluk belirleme anlaşmasının yazılı yapılması 26. madde ile şart koşulmamakla birlikte, şeffaflık, açıklık, sorumluluğun tayini ve ispat açısından yazılı yapılmasında fayda bulunmaktadır.

Gerçek kişinin kişisel verilerinin ihlalinden doğan zararlardan hem veri işleyenler hem veri sorumluları birlikte sorumlu olacaklardır. Ortak veri sorumluların bulunduğu aynı işlemlerden doğan zararlardan, her veri sorumlusu veya işleyen tüm zarardan sorumlu olacaktır (GDPR, rec. 146 ve m. 82/4). Bununla birlikte ortak veri sorumluları aynı adli sürece katılmışlar ise, iç düzenlemelerindeki sorumluluklarına göre zararın tazmin edilmesine karar verilebilecektir (GDPR,

257 Örnekler için bkz. What is a Data Controller or a Data Processor, https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/obligations/controller-processor/what-data-controller-or-data-processor_en#references

rec. 146 ve m. 82/5).

ABAD (Avrupa Birliği Adalet Divanı) nezdinde karara bağlanan bir uyuşmazlıkta hem Facebook hem de Facebook üzerinde fan sayfasını yöneten şirket "ortak veri sorumlusu" olarak veri işlenmesinden sorumlu tutulmuşlardır.[258] Karara konu olayda Alman şirketi Wirtscharft akademie Schleswig-Holstein Şirketi, Facebook'ta yer alan fan sayfaları aracılığıyla eğitim hizmetleri sunmaktadır. Facebook Insights uygulaması ile fan sayfasını ziyaret eden kullanıcıların bilgisayarlarına çerez/cookies yerleştirilmekte ve bu sayede Alman şirket ve Facebook kullanıcılara ait kişisel bilgileri toplanmaktadır. Bu ihlal nedeniyle Almanya'nın Schleswig-Holstein eyaleti Veri Koruma Otoritesi'ne (Unabhängiges Landeszentrum für Datenschutz-ULD) başvuru yapılır ve 2011 yılında ULD, Şirketin, Facebook fan sayfasının kullanımını durdurmasını çünkü kullanıcıların rızası alınmaksızın Facebook ve şirket tarafından kişisel verilerin kayıt edildiğini belirtir. Şirket, olayda kişisel verileri işleyenin kendisi değil Facebook olduğunu belirterek yargı yoluna başvurur ve mahkeme olayı ABAD önüne taşır. ABAD, 5 Haziran 2018 tarihinde verdiği Karar'da hem Wirtscharftakademie Şirketi'nin hem de Facebook'un "ortak veri sorumlusu (joint controller)" niteliği taşıdığını ve sorumlusu olduğuna karar vermiştir. Wirtscharftakademie Şirketi, Facebook'ta fan sayfasının parametrelerini tanımlayarak ve bu fan sayfasını yönetmek ve kullanıcılara tanıtmak sureti ile ortak sorumlu olmuştur. Facebook Insights uygulaması ile toplanan kişisel verilere ilişkin ne Facebook tarafından ne de Wirtschaftsakademie şirketi tarafından kullanıcılar bilgilendirilmemiştir. Burada toplanan kişisel veriler, fan sayfasının ne zaman ziyaret edildiği, hangi ülkeden ziyaret edildiği, yaş grupları, kişilere ilişkin diğer kişisel verilerden oluşmaktadır. ABAD, Wirtscharftakademie Şirketinin, kişisel verileri kendisi toplamasa dahi Facebook Insights uygulaması sayesinde kişisel verilerin işlenmesini talep edebileceğini ayrıca toplanan bu verilerden kendi faaliyetlerinde faydalanabileceğini belirlemiştir. Bu nedenle hem Facebook İrlanda, hem de Wirtscharftakademie Şirketinin veri ihlalinden dolayı ortaklaşa sorumlu olduğuna karar verilmiştir. Eylemin oluş zamanı itibariyle 95/46/EC sayılı Direktif'in ortak sorumluluk esası uygulanmış ve GDPR'ın 26. maddesi uygulanmamıştır. Ancak ABAD'ın GDPR 26. maddesine yaklaşımının da bu tür durumlarda birlikte sorumluluk şeklinde değerlendirilebileceği anlaşılmaktadır. Bununla birlikte ABAD, sorumluluğun eşit derecede olmayacağının da altını çizmiştir.[259]

---

258 Judgment of the Court (Grand Chamber), C-210/16, 5 June 2018, Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein v. Wirtschaftsakademie Schleswig-Holstein GmbH, Interveners: Facebook Ireland Ltd., Vertreter des Bundesinteresses beim Bundesverwaltungsgericht.

259 ABAD, C-210/16, paragraf 43.

III. Tüzüğün Uygulama Alanı

A. Genel Olarak

Tüzüğün maddi kapsamı 2. maddede belirtilmiştir. Buna göre *"Tüzük, kişisel verilerin tamamen ya da kısmen otomatik araçlarla işlenmesine ve kişisel verilerin otomatik araçlar haricinde bir dosyalama sisteminin parçasını oluşturan veya bir dosyalama sisteminin parçasını oluşturması amaçlanan araçlarla işlenmesine uygulanır."*[260]

Fakat, Tüzükte açıkça belirtildiği üzere, Tüzük, kamu güvenliğine yönelik tehditlere karşı güvence sağlanması ve bu tehditlerin önlenmesi de dâhil olmak üzere suçların önlenmesi, soruşturulması, tespiti veya kovuşturulması ya da cezaların infaz edilmesiyle ilgili olarak yetkin makamlar tarafından kişisel verilerin işlenmesine uygulanmaz.[261] Böyle bir durumda Adli ve Kolluk Teşkilatında Verilerin Korunmasına İlişkin 2016/680 Sayılı Direktif uygulama alanı bulacaktır.

B. Tüzüğün Kişi Bakımından Uygulama Alanı

Tüzük düzenlemeleri veri sorumlusu ve veri işleyenler bakımından yükümlülük ve sorumluk doğuracak, veri sahipleri de Tüzük uyarınca korunacaktır. Bu nedenle kimin veri sorumlusu, kimin veri işleyen ve kimin veri sahibi olduğunun tespit edilmesi büyük önem arz etmektedir.[262]

Tüzüğün kişi bakımından uygulamasında veri sorumluları ve veri işleyenler açısından bir sınırlama öngörülmüştür. Konu bakımından sınırlamayla iç içe olan bu sınırlamaya göre; Tüzüğün tamamen kişisel veya ev faaliyeti esnasında bir gerçek kişi tarafından gerçekleştirilen veri işlemelere uygulanmayacağı açıkça düzenlenmiştir.[263]

Veri sahipleri yönüyle kişi bakımından tek sınırlama gerçek kişi olma koşuludur. Tüzükte kişisel verinin tanımı yapılırken açıkça "gerçek kişi" vurgusu yapılmış (m. 4), ayrıca Gerekçe m. 14'te Tüzüğün tüzel kişilerin verileri bakımından uygulanmayacağı açık bir şekilde belirtilmiştir. Bu itibarla Tüzük sadece kişisel verisi işlenen gerçek kişiler bakımından uygulanacaktır.

C. Tüzüğün Yer Bakımından Uygulama Alanı

Tüzük, Avrupa Birliği temelli bir düzenleme olmasına rağmen, coğrafi olarak uygulama alanı Avrupa Birliği sınırlarından daha geniştir.[264] Öncelikle, 3. maddenin 1. fıkrası uyarınca

---

260 GDPR, m. 2.
261 GDPR, m. 2(2)(d).
262 **Paul Voigt/Axel von dem Bussche**, The EU GDPR: A Practical Guide, Springer, Heidelberg, 2017, s. 17.
263 GDPR, m. 2(2)(c).
264 **Voigt/von dem Bussche**, s. 22.

"Tüzük, işleme faaliyeti Birlik içerisinde gerçekleşip gerçekleşmediğine bakılmaksızın, Birlik içerisindeki bir veri sorumlusu veya veri işleyenin işletmesinin faaliyetleri bağlamında kişisel verilerin işlenmesine uygulanır." Bunun yanı sıra, aynı maddenin 2. fıkrası, Tüzüğün, Avrupa Birliği ile içerisindeki işlemeler ile sınırlı olmadığını ve Tüzüğün, işleme faaliyetlerinin belirli hususlarla alakalı olması durumunda, Birlik içerisinde bulunan veri sahiplerinin kişisel verilerinin Birlik içerisinde kurulu olmayan bir veri sorumlusu veya veri işleyen tarafından işlenmesine uygulanacağını düzenlemektedir. Buna göre Tüzük *"veri sahibine bir ödeme yapılmasına gerek olup olmadığına bakılmaksızın, Birlik içerisindeki söz konusu veri sahiplerine mal ya da hizmetlerin sunulması"* veya *"veri sorumlusu veya işleyenin davranışları birlik içerisinde gerçekleştiği ölçüde, davranışlarının izlenmesi"* hallerinde uygulama alanı bulacaktır. Bunlar dışında Tüzük ayrıca, *"Birlik içerisinde olmamasına rağmen uluslararası kamu hukukuna istinaden bir üye devletin hukukunun uygulandığı bir yerde kurulu bulunan bir veri sorumlusu tarafından kişisel verilerin işlenmesine uygulanır."*

GDPR'ın önemli yeniliklerinden bir tanesi de uygulama alanının (territorial scope) genişletilmiş olmasıdır (extraterritorial scope)[265].

Avrupa Konseyi'nin 10 Ocak 1985 tarihinde yürürlüğe giren 108 sayılı Sözleşmesi'nin 1. maddesiyle uygulama alanı açısından üye ülke toprakları esas alınmıştır. Buna göre uyruğu ve ikameti ne olursa olsun, "her bir Taraf ülkedeki gerçek kişinin hakları" güvence altına alınmaktadır. Bununla birlikte 108 sayılı Sözleşme'nin değişen koşullara uyarlanması amacıyla oluşturulan 2014 tarihli Taslak'ta "ülkesel (territorial)" yaklaşım yerine, veri işleme öznelerinin yargılama yetkileri (jurisdiction) esas alınmıştır. Bu yeni ifade, Sözleşme'nin 10 Ekim 2018 tarihinde güncellenen 223 sayılı Sözleşme'de kabul edilmiştir.[266] Bu ifade tanımlanmamakla birlikte, Sözleşme'nin ilk haline göre uygulama alanını her üye ülkenin yargılama yetkilerinin yorumuna göre genişleteceği muhakkaktır.[267]

95/46/EC sayılı Direktif'te uygulama alanını düzenleyen 4/a bendi ile veri sorumlusunun yerleşik olduğu yer, 4/c bendi ile ise veri işlemede kullanılan otomatik cihazların bulunduğu yer

---

265 Guidelines 3/2018 on the territorial scope of the GDPR (Article 3) - Version for public consultation Adopted on 16 November 2018, s. 3. https://edpb.europa.eu/sites/edpb/files/consultation/edpb_guidelines_3_2018_territorial_scope_en.pdf (Son erişim: 19.07.2019)

266 Protocol amending the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, ETS No. 223, Strasbourg, 10.X. 2018, https://www.coe.int/en/web/conventions/full-list/

267 **Paul de Hert/Michal Czerniawski**, "Expanding the European Data Protection Scope beyond Territory: Article 3 of the General Data Protection Regulation in its Wider Context", International Data Privacy Law, V. 6, No. 3, 2016 (s. 230-243), s. 232.

esas alınmıştır. 95/46/EC sayılı Direktif'in 4/a bendinin uygulanması için ilk olarak veri sorumlusunun AB üyesi ülkelerde bulunması hali, ikinci aşamada ise veri işleme faaliyetinin bu veri sorumlusunun faaliyetlerinden kaynaklanmış olması hali dikkate alınmıştır.[268]

GDPR'da konunun düzenlendiği 3. Maddenin1. fıkrasında öncelikle AB topraklarındaki bir veri sorumlusu/işleyenin faaliyetleri esas alınmıştır. Bu düzenleme 95/46/EC sayılı Direktif'in 4/1 maddesi ile uyumludur. Ancak bentte yer alan "işleme faaliyetinin Birlik içerisinde gerçekleşip gerçekleşmediğine bakılmaksızın" ifadesi de uygulama alanını genişletici etki doğurabilecektir. Çünkü AB topraklarında yer alan bir veri sorumlusunun AB toprakları dışındaki veri işleme faaliyetleri esas alındığında da uygulanacaktır.[269]

GDPR'ın 3/2 maddesi ise veri sorumluları ve işleyenlerin AB dışında faaliyet göstermesi durumunda da GDPR'ın uygulama alanı bulmasını sağlamaktadır. Buna göre veri veri sorumlusu/işleyen şirketin merkezi ve faaliyet alanı AB dışında olsa dahi, şayet AB topraklarında bir mal ve hizmet sunumunda bulunuyor ise bu şirketin olası kişisel veri ihlali durumunda GDPR hükümleri uygulanabilecektir. Bu ihtimalde, veri sahibine herhangi bir ödemede bulunulması şartı da aranmamaktadır (GDPR, m. 3/2-a). Bu durum, internetin söz konusu olduğu günümüzde GDPR uygulamasını aşırı genişletici bir etki doğurmaktadır.[270] Çünkü herhangi bir web sitesine dünyanın her yerinden girilebilmektedir. Örneğin ABD'de faaliyet gösteren bir seyahat şirketinin web sitesini kullanan bir AB vatandaşı, bu site aracılığıyla ABD'de bir otele rezervasyon yapmış olsa, bu takdirde ABD şirketi bu kişi açısından GDPR uygulaması ile karşılaşabilecektir. Aynı şekilde Türkiye'de faaliyet gösteren şirketler de, bu olasılıkları dikkate alarak GDPR uyumluluğunu sağlamakla yükümlü olabileceklerdir. Bu geniş uygulama alanı hem ülkeler ve bu ülkelerde faaliyet gösteren şirketler açısından hem de hakları ihlal edilen bireyler bakımından belirsizlik oluşturabilecek niteliktedir. Çünkü ne zaman hangi ülke hukuku ile karşılaşılacağı birey açısından da net değildir. Bu gibi durumlarda, GDPR'nın uygulama alanının belirlenmiş olması diğer ulusal kanunları devre dışı bırakmayacaktır ve kanunlar ihtilafı kurallarının uygulanması kaçınılmaz olacaktır. GDPR'da bu uygulama gerçek kişilerin GDPR'ın koruma haklarından mahrum olmamaları için konulduğu belirtilmekte ve bu tür bir veri sorumlusu/işleyenin AB içindeki veri sahiplerine mal/hizmet sunup sunmadığının belirlenmesi için bunun öngörülüp öngörülmediğinin (envisages) öncelikle belirlenmesi gerektiği ifade edilmektedir (GDPR, rec. 23). Veri

268 **Hert/Czerniawski**, s. 233.
269 Guidelines 3/2018 on the territorial scope of the GDPR (Article 3) - Version for public consultation Adopted on 16 November 2018, s. 12.
270 **Hert/Czerniawski**, s. 237.

sorumlusu/işleyenin sadece web sitesinin AB içinden erişilebilir olması durumunda, şirketin e-posta adresi, diğer iletişim ayrıntıları, kullanılan dil, kullanılan para birimi ve AB içindeki müşterilerin yorumları gibi değerlendirmeler dikkate alınabilecektir. Şirketin nerede kurulmuş olduğu bu belirlemeleri yapmak için yeterli olmayacaktır (GDPR, rec. 23). Bununla birlikte, GDPR'ın 3/2-a maddesiyle getirilen AB vatandaşlarının korunmasına yönelik bu yetki düzenlemesinin, GDPR'ın 23. gerekçesiyle yumuşatıldığı ve internet şirketlerine GDPR dışına çıkma şansı verdiği ifade edilmektedir. Buna örnek olarak AB dışından örneğin bir Çin şirketi, global ölçekte oluşturduğu internet sitesinde ürün kataloglarını sergiler. Bu kataloglara dünyanın her yerinden erişim sağlanabilir. Bu aşamada kullanıcılar herhangi bir kişisel verisini kayıt ettirmeksizin, bu katalogları inceleyebilmektedir. Dolayısıyla bir AB vatandaşı bu kataloglardan bir ürün beğense, bu aşamada henüz GDPR uygulanması mümkün olmaz. Ne zamanki kullanıcı ürünü seçip almak için bağlantıyı tıklar. Bu halde kullanıcının önüne üçüncü kişiye ait yeni bir web sitesi açılır. Bu sitede 23. gerekçeye uygun araçlar bulunmaz. Örneğin para birimi Euro değil, ABD dolarıdır. Kullanıcı kişisel verilerini bu yeni web sitesinde kayıt ettirir. Bu üçüncü kişiye ait web sitesi, GDPR kapsamında olmadığını iddia edebilir çünkü AB üyesi ülkelere mal ve hizmet sunumu yapan bu site değil, Çin menşeili şirkete ait ilk web sitesidir. Dolayısıyla bu siteden bir mal ve hizmet sunumu gerçekleşmemiştir. Dolayısıyla GDPR yetkisini doğuran olayın sadece mal ve hizmet sunumuna indirgenmesi eleştirilmiştir. Oysa bu ifade "pazarlama (marketing) ile bağlantılı (related to marketing)" veya "mal/hizmet tedariki (supply of goods or services)" şeklinde ifade edilse yahut daha basit şekilde "AB içindeki veri sahibi ile bağlantılı" şeklinde ifade edilse, GDPR uygulama alanının daha net ve kesin olacağı ifade edilmiştir.[271]

GDPR'ın 3/2-b maddesiyle AB dışında merkezi olan sosyal medya şirketlerinin hedef alındığı açık olan bir düzenleme yer almaktadır. Buna göre davranışların AB içinde gerçekleştiği ölçüde, AB içindeki tüketicilerin (veri sahiplerinin) davranışlarının izlenmesi durumunda GDPR uygulama alanı bulacaktır[272]. Dolayısıyla AB içinde müşteri tabanı bulunan ve online davranışsal reklamcılık faaliyetinden faydalanan tüm sosyal ağ şirketleri, arama motoru şirketleri veya diğer şirketler bu madde düzenlemesi nedeniyle GDPR uygulamasına muhatap olabileceklerdir. Bu düzenlemede yer alan "davranışların AB içinde gerçekleştiği ölçüde (as far as their behaviour takes place within the Union)" ifadesi, veri sorumlusu ile veri sahibi arasında tek bağlantının veri

[271] **Robert Madge**, Five Loopholes in the GDPR, August 27, 2017, https://medium.com/mydata/five-loopholes-in-the-gdpr-367443c4248b (Son Erişim Tarihi: 20.03.2019).

[272] Guidelines 3/2018 on the territorial scope of the GDPR (Article 3) - Version for public consultation Adopted on 16 November 2018, s. 12.

sahibinin AB üyesi ülkelerde ikamet etmesi olduğu, gevşek bağlantılı durumlarda GDPR'ın uygulanmasının önüne geçecektir.

Veri işleme faaliyetinin "veri sahiplerinin davranışlarının izlenmesi" olarak nitelendirilebilmesi için, başta veri sahibinin kişisel tercihleri, davranışları ve tutumlarını analiz etmek veya tahmin etmek veya o kişiyle ilgili kararlar almak için bir gerçek kişinin profilinin çıkarılması gibi, kişisel veri işleme tekniklerinin kullanımını içeren internette gerçek kişilerin izlenmesi olup olmadığı tespit edilmelidir (GDPR, rec. 24). Bu kapsamda Facebook, Google, Twitter gibi şirketlerin GDPR uygulama alanına dahil olduğu açıktır.

D. Tüzüğün Konu Bakımından Uygulama Alanı

Tüzük, AB hukuku kapsamına girmeyen faaliyetler ile AB üyesi devletler tarafından AB Antlaşması'nın Beşinci Başlığının İkinci Bölümü[273] kapsamına giren faaliyetlere ilişkin olarak kişisel verilerin işlenmesi halinde uygulanmayacaktır. Ayrıca tamamen kişisel veya ev faaliyetleri esnasında bir gerçek kişi tarafından kişisel verilerin işlenmesi ile kamu güvenliğine yönelik tehditlere karşı güvence sağlanması ve bu tehditlerin önlenmesi de dahil olmak üzere suçların önlenmesi, soruşturulması, tespiti veya kovuşturulması ya da cezaların infaz edilmesiyle ilgili olarak yetkili makamlar tarafından kişisel verilerin işlenmesi halinde de Tüzük uygulanmayacaktır (GDPR, m. 2/2).

IV. Temel İlkeler

A. Hukuka Uygunluk, Adillik ve Şeffaflık

1. Hukuka Uygunluk

Kişisel verilerin hukuka uygun olarak işlenmesi ilkesi; veri işlemenin, veri sahibinin rızası veya Tüzükte düzenlenmiş diğer bir hukuka uygunluk sebebine dayanılarak gerçekleştirilmesi gerekliliğini ifade eder. Veri işlemenin hukuka uygunluğu, Tüzüğün 6. maddesinin 1. fıkrasında düzenlenmiştir. Buna göre veri sahibinin rızası olmamasına rağmen veri işlemenin hukuka uygun olması için işleme faaliyetinin,

(i) veri sahibinin taraf olduğu bir sözleşmenin uygulanması veya bir sözleşme yapılmadan önce veri sahibinin talebiyle adımlar atılması için,

(ii) veri sorumlusunun tabi olduğu bir yasal yükümlülüğe uygunluk sağlanması amacı ile,

(iii) veri sahibinin veya başka bir gerçek kişinin hayati menfaatlerinin korunması amacı ile,

[273] Avrupa Birliği Andlaşması, Beşinci Başlık, İkinci Bölümü, AB ortak dış ve güvenlik politikasına ilişkin özel hükümleri içerir. Bkz. Consolidated Version of The Treaty on European Union, Official Journal of the European Union, C 326/13, 26.10.2012.

(iv) kamu yararına gerçekleştirilen bir görevin yerine getirilmesi veya veri sorumlusuna verilen resmi bir yetkinin uygulanması hususunda,

(v) özellikle veri sahibinin çocuk olması halinde veri sahibinin kişisel verilerin korunmasını gerektiren menfaatleri veya temel hakları ve özgürlüklerinin bir veri sorumlusu veya üçüncü bir kişi tarafından gözetilen meşru menfaatlere ağır basması haricinde, söz konusu menfaatler doğrultusunda,

gerekli olması aranmaktadır.[274]

2. Adillik

Veri işlemenin Tüzükte yer alan ilkelere uygun olması için adil olması gerekir. Bu anlamda, işleme faaliyetine dayanak yapılan hukuk normları adalete uygun olarak düzenlenmiş olmalıdır.[275] Ayrıca veri sorumluları; veri sahiplerini ve kamuyu, verileri hukuka uygun ve şeffaf bir şekilde işleyecekleri konusunda haberdar etmelidir. Bunun yanında, veri sorumluları veri işleme faaliyetlerinin Tüzüğe uygun olarak gerçekleştirildiğini gösterebilecek durumda olmalıdır. Ek olarak, veri sorumluları, özellikle veri sahibinin rızasının işleme faaliyeti için hukuki dayanak oluşturduğu durumlarda, mümkün olduğunca veri sahibinin taleplerine uygun hareket etmelidir.[276] Tüm bunlar düşünüldüğünde, adil olma ilkesi, şeffaflık yükümlülüğünün ötesinde olup kişisel verilerin etiğe uygun bir şekilde işlenmesi ile ilgilidir.[277]

Bu ilkeye örnek olarak AİHM'in *K.H. ve Diğerleri v. Slovakya* kararı[278] gösterilebilir. Bu davada başvurucular, Roman etnik kökenli, hamilelikleri ve doğumları sırasında Slovakya'da bulunan iki hastanede tedavi görmüş kadınlardır. Doğumlarından sonra bu kadınlardan hiçbiri, çok kez denemelerine rağmen, hamile kalamamışlardır. Bunun üzerine yerel mahkemeler, hastanelere, hastaneye danışmaları ve tıbbi kayıtlarından el yazıları ile bilgi almaları için başvurucu ve temsilcilerine izin vermelerine karar vermiş, fakat suistimalin önlenmesi gerekçesiyle bu belgelerin fotokopilerinin alınması talebini reddetmiştir. Oysa, AİHS'in 8. maddesi uyarınca, devletlerin, veri sahiplerinin dosyalarının bir kopyasını veri sahiplerine erişilir kılmak yönünde bir yükümlülükleri vardır. Bu davada ise yerel mahkeme, başvurucuların kendi sağlıklarına ilişkin bilgilere etkili bir erişim elde etme taleplerini reddetmiş ve reddederken geçerli bir sebep ileri sürememiştir. Mahkeme ilgili bilgilerin suistimalden korunması için bu talebi reddettiğini belirtse de, kişisel

274 GDPR, m. 6(1); **Develioğlu**, s. 58.
275 **Dülger**, s. 116.
276 **Giakoumopoulos/Buttarelli/O'Flaherty**, s. 118.
277 **Giakoumopoulos/Buttarelli/O'Flaherty**, s. 119.
278 AİHM, K.H. ve Diğerleri v. Slovakya, No. 32881/04, 28 Nisan 2009.

verilerine ilişkin dosyalarına zaten erişim elde eden bireylerin ayrıca bu dosyaların bir kopyasını alarak kendilerine ilişkin bilgileri nasıl suistimal edebileceğini düşündüğünü açıklayamamıştır. AİHM bu davada AİHS'in 8. maddesinin ihlal edildiğine karar vermiştir.[279]

3. Şeffaflık

95/46/EC sayılı Direktifteki ilkelere ek olarak düzenlenmiş şeffaflık ilkesi; veri sorumlularına, veri sahiplerini, verilerinin nasıl kullanıldığı ile ilgili bilgilendirme yükümlülüğü yüklemektedir.[280] Bu kapsamdaki her türlü bildirim *"öz, şeffaf, anlaşılır ve kolayca erişilebilir bir biçimde, açık ve sade bir dil kullanarak"* veri sahibine sağlanmalıdır. Veri sorumlusu söz konusu bilgileri yazılı olarak veya uygun olduğu hallerde, elektronik yollar da dahil olmak üzere diğer yollarla sağlayacaktır. Veri sahibi tarafından talep edilmesi durumunda, veri sahibinin kimliğinin diğer yollarla doğrulanması koşuluyla, bilgiler sözlü olarak sağlanabilir.[281]

Şeffaflık ilkesi; henüz işleme faaliyetleri başlamadan önce kişiye yapılan bilgilendirme için uygulama alanı bulduğu gibi, işleme sırasında veri sahiplerinin erişimine hazır bulunan bilgiler ve veri sahibine kendi verilerine erişim talep etmeleri üzerine verilen bilgiler de bu kapsamdadır.[282]

Bu ilke uyarınca, kişisel verilerinin işlenmesinin riskleri, kuralları, koruyucuları ve işlemeye ilişkin veri sahiplerinin hakları, ilgili kişiler için açık ve net olmalıdır. [283] Aynı zamanda kişisel verilerin işlenmesinin sınırlı ve belirli amacı da, verilerin toplanması sırasında, veri sahipleri tarafından biliniyor olmalıdır.[284]

Şeffaflık ilkesinin nasıl yorumlandığına örnek olarak AİHM'in *Haralambie v. Romanya*[285] kararı incelenebilir. Bu davada, başvurucu, gizli servis teşkilatı bünyesinde tutulan kendisine ilişkin bilgilere erişim talep etmiştir. Başvurucuya bu bilgilere erişim ancak talebinden beş sene sonra sağlanmıştır. AİHM, bireylerin, kamu makamları tarafından tutulan şahsi dosyalarına erişebilmekte çok ciddi çıkarları olduğunu belirtmiştir. AİHM, ayrıca, yetkililerin, bu bağlamda söz konusu bilgilere ulaşımın sağlanması için efektif bir prosedür öngörülmesi gerektiğini ifade etmiştir. Bu davada AİHM, ne dosyaların sayısının çokluğunun ne de arşivleme sistemlerindeki yetersizliğin, başvurucunun dosyalarına erişim talebinin yerine getirilmesinde beş senelik bir gecikmeyi meşru kıldığını belirtmiştir. Yetkililerin, başvurucuya, şahsi dosyalarına erişim sağlayabilmesi için etkili

279 **Giakoumopoulos/Buttarelli/O'Flaherty**, s. 118, 199.
280 **Giakoumopoulos/Buttarelli/O'Flaherty**, s. 120.
281 GDPR, m. 12(1).
282 **Giakoumopoulos/Buttarelli/O'Flaherty**, s. 120.
283 GDPR, Gerekçe 39.
284 GDPR, Gerekçe 39.
285 AİHM, Haralambie v. Romanya, No. 21737/03, 27 Ekim 2009.

ve erişilebilir bir yol sağlamaması nedeniyle, AİHM, AİHS'in 8. maddesinin ihlal edildiğine karar vermiştir.[286]

B. Belirli, Açık ve Meşru Amaçlara Yönelik İşleme (Amacın Sınırlandırılması İlkesi)

Amacın sınırlandırılması ilkesi uyarınca, *kişisel veriler belirtilen, açık ve meşru amaçlara yönelik olarak toplanır ve yalnızca bu amaçlara uygun bir şekilde işlenebilir*.[287] Şeffaflık, öngörülebilirlik ve kişilerin verileri üzerindeki kontrolü nosyonları ile yakından ilgili olan bu ilke, veri sahiplerinin haklarını kullanabilmeleri açısından oldukça önemlidir.[288]

Yani, kişisel verilerin işlenmesini faaliyetlerinin meşruiyeti, işlemenin belirli, açık ve meşru bir amaç doğrultusunda gerçekleştirilmesine bağlıdır.[289] İlk amaç ile bağdaşan başka bir amaçla veri işleme faaliyetinin gerçekleştirilebilmesi için, bu işleme için veri sahibinin tekrar rızası alınmalı veya işleme faaliyeti başka bir hukuki dayanağa sahip olmalıdır.[290] Örneğin; bir havayolu şirketi, bir uçuşun düzgün bir şekilde idaresinin sağlanabilmesi için, rezervasyon yaptıkları sırada yolcularında bazı verileri toplar. Bu çerçevede, söz konusu havayolu, yolcuların koltuk numaralarına, özel besin gereksinimlerine, özel fiziksel ihtiyaçlarına ilişkin bilgileri alır. Fakat, bu havayolu şirketi aldığı bu bilgileri varış yerindeki göç makamlarına sağlayacak olursa, veri sahiplerinden uçuşun düzgün bir şekilde işletilmesi amacı ile toplanan ilgili verilerin toplanma sırasındaki amaçtan farklı bir amaç için kullanılması söz konusu olacaktır[291]. Bu nedenle, bu bilgilerin bir göç makamına aktarımının gerçekleştirilmesi için farklı ve yeni bir yasal dayanak bulunması gerekir.[292]

Burada vurgulanması gereken nokta, belirlenen amaçtan farklı bir amaçla işlemenin söz konusu olması için farklı bir amacın yeterli olup, mutlaka önceki ile bağdaşmayan bir amaç olmasının gerekmemesidir.[293] Bu çerçevede, ilave olarak gerçekleştirilmesi planlanan işlemenin orijinal amaç ile uyumlu olup olmadığı değerlendirilirken kişisel verinin toplanması amacı ve ilave işleme amaçları arasındaki ilişki, kişisel verilerin toplandığı bağlam ve veri sahiplerinin ilerideki kullanımlarına ilişkin makul beklentileri, kişisel verilerin niteliği, planlanan ilave işlemenin veri sahipleri açısından sonuçları, orijinal ve ilave işleme faaliyetleri için uygun korumaların varlığı

286 **Giakoumopoulos/Buttarelli/O'Flaherty**, s. 120.
287 GDPR, m. 5(1)(b).
288 **Giakoumopoulos/Buttarelli/O'Flaherty**, s. 122.
289 **Giakoumopoulos/Buttarelli/O'Flaherty**, s. 122.
290 **Giakoumopoulos/Buttarelli/O'Flaherty**, s. 123.
291 Guide to General Data Protection Regulatin.
292 **Giakoumopoulos/Buttarelli/O'Flaherty**, s. 123.
293 **Dülger**, s. 121.

gibi faktörler dikkate alınmalıdır.[294] Ayrıca belirtilmelidir ki, kamu yararına arşivleme amaçları, bilimsel veya tarihi araştırma amaçlarıyla veya istatistiki amaçlarla işleme faaliyetlerinin baştaki amaçlara *a priori* uygunluğu Tüzükte açıkça düzenlenmiştir[295]. Her koşulda, ilave olarak veri işlemesi geçekleştirilirken anonimleştirme, şifreleme veya takma ad kullanımı da dahil olmak üzere uygun güvencelerin bulunması gerekir.[296] Örneğin; A Şirketinin, müşterileri ile ilgili olarak müşteri ilişkileri yönetimine dair verileri topladığını ve sakladığını varsayalım. Bu verilerin, A Şirketi tarafından, müşterilerinin satın almaya yönelik davranışlarını istatistiki olarak analiz etmek için kullanılması Tüzüğün belirlediği ilkelere bir aykırılık teşkil etmeyecektir. Yine de, A Şirketinin istatistiki amaçlarla ilave işleme yapmasının hukuka uygun olması için, A Şirketi veri sahibinin hak ve özgürlüklerini korumak için gerekli güvenceleri sağlamalıdır.[297] Son olarak, ilave veri işlemenin, veri sahibinin rızasına dayanması veya Birlik veya Üye Devlet hukukunca kamu yararı gibi önemli hedeflerin güvence altına alınması için gerekli ve ölçülü bir tedbir niteliğinde olması durumunda, veri sorumlusu, amaçların uyumluluğuna bakılmaksızın söz konusu ilave işlemeyi gerçekleştirebilmelidir.[298]

C. Verilerin İşlendikleri Amaçla Bağlantılı, Sınırlı ve Ölçülü Olması (Veri Minimizasyonu)

Veri minimizasyonu ilkesi uyarınca, *kişisel veriler, işlendikleri amaçlarla ilgili olarak yeterli, yerinde ve gerekli olanla sınırlı olmalıdır*.[299] Bu kapsamda Tüzüğün lafzı 95/46/EC sayılı Direktif ve 108 No'lu Sözleşme'den farklılık göstermektedir: Bu belgelerde verilerin toplanmasının *"gerekli olanla sınırlı olması"* yerine *"aşırı olmaması"* gerektiği düzenlenmiştir.

Veri minimizasyonu ilkesine göre veri sorumlusunun yükümlülüğü veri işlemesini minimumda tutmaktan ziyade, veri toplanmasını işleme amaçlarını göz önüne alarak yeterli olan ölçüde sınırlandırmaktır.[300] Yani, veri sorumlusunun işleme için seçtiği veri kategorileri, işlemenin açıkça belirtilmiş amacına ulaşmak için gerekli olmalıdır ve veri sorumlusu, veri toplanmasını veri işleme ile güdülen spesifik amaç ile doğrudan ilgisi olan bilgiler ile sınırlandırmalıdır.[301]

---

294 GDPR, m. 6(4); **Giakoumopoulos/Buttarelli/O'Flaherty**, s. 124.
295 GDPR, m. 5(1)(b).
296 **Giakoumopoulos/Buttarelli/O'Flaherty**, s. 124.
297 **Giakoumopoulos/Buttarelli/O'Flaherty**, s. 125.
298 GDPR, Gerekçe 50.
299 GDPR, m. 5(1)(c).
300 **Voigt/von dem Bussche**, s. 90.
301 **Giakoumopoulos/Buttarelli/O'Flaherty**, s. 125.

Örneğin; *Digital Rights Ireland* davasında[302] ABAD, organize suç ve terör gibi ciddi bir suçla mücadele amacıyla ilgili verilerin yetkili makamlara olası aktarımları için kamuya açık elektronik haberleşme servisleri ve ağları tarafından oluşturulan veya işlenen kişisel verilerin saklanmasına ilişkin yerel hukuklarda yer alan hükümlerin yeknesaklaştırılmasını amaçlayan Veri Saklama Direktifinin geçerliliğini incelemiştir. Genel olarak ciddi bir suçla mücadele meşru bir menfaat olarak düşünülse de bu direktifin *"bir fark, sınır veya istisna gözetmeksizin tüm bireyleri ve her tür elektronik haberleşme ile trafik verisini"* kapsaması, sorunlu bulunmuştur.[303]

GDPR'ın 5/1-c maddesinde düzenlenen verilerin asgari ölçüde işlenmesi ilkesi nedeniyle kişisel veriler ancak gerekli olan ile sınırlı şekilde toplanabilecektir. Dolayısıyla bu ilke, kullanıcılarına ait doğum tarihi, yaşadığı yer, çalıştığı yer, meslek, arkadaşları, ilgi alanları, ailesinden uzaklığı gibi pek çok kişisel veriyi toplayan Facebook gibi sosyal medya şirketleri açısından önemli bir aşamayı içermektedir. Veri sorumlusu niteliği taşıyan sosyal medya şirketlerinin veri sahibinin haklarını kullanabilmesini teminen şeffaf bir şekilde kullanıcıyı, topladığı verilere ilişkin bilgilendirmesi, işlenen verilere ilişkin veri tabanını sunması zorunludur (GDPR, m. 12). Facebook'un kullanıcılara ilişkin tuttuğu kabul edilen bu verilerin, olayların gerçekleşme tarihlerinin, saklanan sayısız fotoğrafın ve kullanıcıların kontak listelerine ilişkin verilerin GDPR'ın 4/1 maddesi uyarınca kişisel veri olduğunda şüphe bulunmamaktadır. Dolayısıyla Facebook kullanıcıları, bu verilerin Facebook tarafından işlenmesinin ve saklanmasının GDPR'ın 5/1-c ve 5/1-e maddelerinde düzenlenen ilkeler çerçevesinde unutulma hakkının düzenlendiği 17. maddeye göre "artık gerekli olmadığını" belirterek silinmelerini talep edebileceklerdir. Bu tür taleplerde, Facebook'un bir veri sorumlusu olarak GDPR'ın 17. maddesinin gecikmeksizin uygulanmasından sorumlu olduğu, aksi takdirde 83. maddede düzenlenen müeyyidelerle karşılaşabileceği söylenebilecektir.

D. Doğru ve Gerektiğinde Güncel Tutulma

Doğruluk ve güncellik ilkesi uyarınca, *kişisel veriler doğru ve gerektiğinde güncel tutulur*; işlendikleri amaçlar göz önünde tutularak, doğru olmayan kişisel verilerin gecikmeye mahal verilmeksizin silinmesi veya düzeltilmesinin sağlanmasıyla ilgili makul tüm adımlar atılmalıdır.[304]

Bu ilke kapsamında, kişisel bir bilgiye sahip olan bir veri sorumlusu, öncelikle, verinin gerçeği yansıttığına ve güncel olduğuna dair makul bir kesinliğe ulaşmak için çaba göstermeden

---

302 Kararın tam metni için bakınız: http://curia.europa.eu/juris/document/document.jsf?text=&docid=150642&pageIndex=0&doclang=EN&mode=req&dir=&occ=first&part=1&cid=612496.

303 **Giakoumopoulos/Buttarelli/O'Flaherty**, s. 126.

304 GDPR, m. 5(1)(d).

bu bilgiyi kullanmamalıdır.[305] Ayrıca, verilerin ilk defa elde edilmesi aşamasında, veri doğrudan ilgili kişiden ve onun bilgisi dahilinde alınıyorsa, mevzubahis veri bu kişi tarafından doğru bir şekilde verilmelidir.[306]

Tüzüğün lafzından da anlaşıldığı üzere, kişisel verilerin güncel tutulması *"gerektiğinde"* sağlanmalıyken, kişisel verilerin doğruluğu için böyle bir parantez açılmamıştır. Bu doğrultuda, bazı verilerin mutlaka düzenli olarak kontrol edilerek güncellenmesi gerekirken, bazı kaydedilmiş verilerin güncellenmesi ise hukuken yasaklanmıştır. Örneğin; bir medikal kayıttaki bulgular daha sonra yanlış oldukları anlaşılsa bile güncellenerek değiştirilmemelidir. Böyle durumlarda, yalnızca daha sonraki bir aşamada ekleme yapıldığının açık bir şekilde belirtilmesi suretiyle yeni bulgular kaydedilebilecektir. Diğer bir örnek ise sürekli güncellemenin gerekli olduğu durumlarla ilgilidir; bir kişi bir bankaya kredi çekmek için başvurduğunda, banka, bu iş için oluşturulmuş veri tabanlarından kişinin kredi verilebilir durumda olup olmadığını inceler. Böyle bir veri tabanının güncel olmayan veriler içermesi durumunda ilgili kişinin olumsuz sonuçlarla karşılaşması mümkündür. Bu nedenle böyle veri tabanlarını kontrol edenler verileri güncel tutmalıdır.[307]

Verilerin doğru ve gerektiğinde güncel tutulması ilkesi, bireylerin kişisel verilerine erişim hakkı, verilerinin düzeltilmesini veya silinmesini talep etme haklarıyla oldukça yakından ilgilidir.[308]

Nitekim, *Rijkeboer*[309] davasında ABAD, gizlilik hakkının, veri sahiplerinin kişisel verilerinin doğru ve hukuka uygun bir şekilde işlendiğinden emin olmasını da içerdiğini ifade etmiştir.[310]

E. Verilerin Amaç İçin Gereken Süre Kadar Muhafaza Edilmesi (Sınırlı Süre Saklama İlkesi)

Sınırlı süre saklama prensibi, *veri sahiplerinin yalnızca kişisel verilerin işlenme amaçlarının gerektirdiği sürece teşhis edilmesini sağlayan bir şekilde tutulması gerektiğ*ini ifade etmektedir.[311] Daha basit ve açık bir anlatımla kişisel veriler ancak ilgili amacın gerektirdiği süre boyunca işlenmeli, bu sürenin sonunda verinin işlenmesine son verilmeli, veri ya yok edilmeli ya da ilgili kişiyi teşhis edemeyecek şekilde anonimleştirilmelidir. Dolayısıyla bu ilke uyarınca, işleme

305 **Giakoumopoulos/Buttarelli/O'Flaherty**, s. 127.
306 **Dülger**, s. 133.
307 **Giakoumopoulos/Buttarelli/O'Flaherty**, s. 128.
308 **Voigt/von dem Bussche**, s. 91, 92.
309 ABAD, C-553/07, College van burgemeester en wethouders van Rotterdam v. M. E. E. Rijkeboer, 7 Mayıs 2009.
310 **Giakoumopoulos/Buttarelli/O'Flaherty**, s. 128.
311 GDPR, m. 5(1)(e).

amacı gerçekleştirildikten sonra ilgili kişisel veriler silinmeli, yok edilmeli veya anonimleştirilmelidir. Bu kapsamda belirtilmesi gereken bir nokta, sınırlı süre saklama ilkesinin, yalnızca kişilerin kimliklerinin belirlenmesine olanak verecek şekilde tutulan veriler için uygulama alanı bulacağıdır.[312]

Bu ilke uyarınca, kişisel verilerin gerektiğinden uzun süre tutulmaması için, veri sorumlusu tarafından verilerin silinmesi veya periyodik kontrolü için bazı zaman aralıkları belirlenmesi gerekir.[313] Verilerin işleme amacı için gereken süre kadar muhafaza edilmesi gerekliliği, unutulma hakkı ile doğrudan ilgilidir.[314]

Değinilmesi gereken bir diğer nokta ise, kişisel verilerin kamu yararı için, bilimsel veya tarihi araştırma amaçlarıyla veya istatistiki amaçlarla arşivlenmesi durumunda, ilgili verilerin yalnızca yukarıda belirtilen amaçlarla kullanılması ve Tüzük uyarınca gereken uygun teknik ve düzenlemeye ilişkin tedbirlerin uygulanması şartı ile, bu arşivlenmiş verilerin daha uzun süre saklanabileceğidir.[315]

Örneğin; *S. and Marper*[316] davasında, AİHM, haklarındaki ceza davaları beraat ve davanın düşmesi ile sona ermiş başvuruculara parmak izlerinin, hücre örneklerinin ve DNA örneklerinin sınırsız bir süre boyunca saklanmasının ölçüsüz olduğuna ve demokratik bir toplumda gerekli olarak nitelendirilemeyeceğine karar vermiştir.[317] Diğer bir örnek ise, *Digital Rights Ireland*[318] davasıdır. Bu davada ABAD, yukarıda da açıklandığı üzere, Veri Saklama Direktifinin geçerliliğini incelemiştir. Bu direktif verilerin herhangi bir ayrım yapılmadan en az altı ay en çok yirmi dört ay boyunca saklanmasını öngörmüştür, ABAD bu çerçevede Veri Saklama Direktifinin altı ay ile yirmi dört ay arasında değişebilecek saklamanın süresinin belirlenmesi ile ilgili objektif kriterler öngörmemiş olmasını bir sorun olarak dile getirmiştir.[319]

Amaç için gereken sürenin sonunda kural olarak verilerin kalıcı olarak imha edilmesi gerekir. Kalıcı olarak imha etmenin hemen mümkün olmaması durumunda ilgili veri eldeki olanaklarla silinmeli, yani veri sorumlusunun olağan erişim ve kullanım alanlarından

312 **Giakoumopoulos/Buttarelli/O'Flaherty**, s. 129.
313 GDPR, Gerekçe 39.
314 **Voigt/von dem Bussche**, s. 92.
315 GDPR, m. 5(1)(e); **Giakoumopoulos/Buttarelli/O'Flaherty**, s. 129, 130.
316 AİHM, S. and Marper v. Birleşik Kırallık [GC], Nos. 30562/04 and 30566/04, 4 Aralık 2008.
317 **Giakoumopoulos/Buttarelli/O'Flaherty**, s. 129.
318 ABAD, Joined cases C-293/12 and C-594/12, Digital Rights Ireland Ltd v. Minister for Communications, Marine and Natural Resources ve Diğerleri and Kärntner Landesregierung ve Diğerleri [GC], 8 Nisan 2014.
319 **Giakoumopoulos/Buttarelli/O'Flaherty**, s. 130.

çıkarılmalıdır. Bunun yanı sıra verinin anonimleştirme gibi işlemlerden geçirilerek ilgili kişileri teşhis edemeyecek bir niteliğe getirilip saklanması da mümkündür[320].

F. Veri Güvenliği İlkesi

Veri güvenliği ilkesine göre, veri sorumlusu, son teknoloji, uygulama maliyeti ve işleme faaliyetinin mahiyeti, kapsamı, bağlamı ve amaçlarının yanı sıra işleme faaliyetinin gerçek kişilerin hakları ve özgürlükleri açısından teşkil ettiği çeşitli olasılıklar ve ciddiyetlere sahip riskleri dikkate alarak, hem işleme yönteminin belirlenmesi esnasında hem de işleme faaliyeti esnasında, *veri koruma ilkelerinin etkili bir şekilde uygulanması ve bu Tüzüğün gerekliliklerinin yerine getirilmesine yönelik olarak,* yetkisiz veya yasa dışı işlemeye karşı ve kazara kayba, imhaya veya tahribe karşı koruma da dahil olmak üzere, *gerekli güvencelerin entegre edilmesi amacı ile tasarlanan, uygun teknik ve düzenlemeye ilişkin tedbirler uygulamalı ve veri sahiplerinin haklarını korumalıdır.*[321] Tüzük, takma ad kullanılmasını, açıkça veri güvenliği için uygun tedbirlerden biri olarak kabul etmiştir.

Örneğin; *"Melodi Ertekin, 9 Ocak 1992 tarihinde doğmuştur ve iki erkek kardeşi ile birlikte üç çocuklu bir ailenin tek kız çocuğudur"* cümlesi şu şekillerde psödonimleştirilebilir:

(i) "M.E. 1992 iki erkek kardeşi ile birlikte üç çocuklu bir ailenin tek kız çocuğudur"; veya (ii) 1701 iki erkek kardeşi ile birlikte üç çocuklu bir ailenin tek kız çocuğudur". (i) şeklinde gerçekleştirilen psödonimleştirme, (ii) biçiminde gerçekleştirilene göre daha az güvenlidir.[322] Buradan anlaşılması gereken, psödonimleştirme yönteminin veri korumanın verimliliğini etkileyebileceğidir.[323]

G. Hesap Verebilme Zorunluluğu

Veri sorumlusu, Tüzükte düzenlenmiş ilkelere uygun davranmaktan sorumludur ve buna uygun davrandığını gösterebilmek yükümlülüğü altındadır.[324] Bu maksatla, veri sorumlusu, uygun teknik ve düzenlemeye ilişkin tedbirleri almalıdır. Tüzükte lafzen veri sorumlusunun hesap verebilirliğinden bahsedilmiş olsa da, belirli yükümlülükler altında olan veri işleyenin de bu ilkelere uygun davrandığına ilişkin hesap verebilir durumda olması gerekir.[325]

---

320 GDPR uyarınca anonimleştirme ve benzer tekniklerin şartları, avantajları ve karşılaştırması için bkz. **Mike Hintze/Khaled El Emam**, "Comparing the benefits of pseudonymisation and anonymisation under the GDPR", Journal of Data Protection & Privacy, Volume 2, Number 2, Autumn 2018, s. 145-158.

321 GDPR, m. 5(1)(f).

322 **Giakoumopoulos/Buttarelli/O'Flaherty**, s. 131, 132.

323 **Giakoumopoulos/Buttarelli/O'Flaherty**, s. 132.

324 GDPR, m. 5(2), 25.

325 **Giakoumopoulos/Buttarelli/O'Flaherty**, s. 134, 135.

Bu kapsamda izlenecek prosedürler ve kurulacaklar sistemler, veri işlemenin yarattığı risk ve verinin niteliğine bağlı olarak değişiklik gösterecektir[326]. Bu ilkeye uygun hareket etmek için veri sorumluları ve veri işleyenler, örneğin; işleme faaliyetlerine ilişkin kayıt tutabilir ve gerektiğinde bu kayıtları denetim makamına sunabilir[327], belirli durumlarda kişisel verilerin korunması ile ilgili konularda görev yapacak bir veri koruma görevlisi atanabilir[328], bir işleme türünün gerçek kişilerin hakları ve özgürlükleri açısından yüksek bir riske sebebiyet vermesinin muhtemel olduğu hallerde, işleme faaliyetinden önce, veri koruma etki değerlendirmesi yapabilir[329], özel ve olağan durumlarda veri korunmasını temin edebilir[330], veri sahiplerinin haklarını kullanabilmeleri için yöntem ve prosedürler yürürlüğe koyabilir[331], onaylanmış davranış kuralları veya sertifikasyon mekanizmalarına bağlı kalabilir[332].

Madde 29 Çalışma Grubu hesap verme zorunluluğunu; veri sorumlusunun, işleme faaliyetleri bağlamında ve olağan şartlarda veri koruma kurallarına bağlılığı sağlayacak tedbirler alması ve veri koruma kurallarına uygun hareket edildiğini veri sahipleri ve denetim makamlarına gösterecek gerekli belgeleri hazır bulundurması yükümlülüğü olarak özetlemiştir.[333]

§ 3. Veri İşlemenin Kuralları

I. Veri Sorumlusunun Genel Yükümlülükleri

A. Temsilci Atama Yükümlülüğü

Yukarıda açıklandığı üzere, Tüzüğün uygulama alanı AB üyesi ülkelerden daha geniş tutulmuştur. Tüzükte AB'deki kişilerin verilerinin işlenmesi halinde, veri sorumlusu veya veri işleyen AB'de bulunmasa dahi Tüzüğün uygulanacağının öngörülmesine paralel olarak, veri sorumlusu veya işleyenin yazılı olarak Birlik içerisinde bir temsilci ataması gerektiği düzenlenmiştir.[334] Atanacak temsilci, kişisel verileri kendilerine mal veya hizmetlerin sağlanması ile ilgili olarak işlenen veya davranışı izlenen veri sahiplerinin bulunduğu üye devletlerin birinde bulunmalıdır.[335]

326 Guide to General Data Protection Regulatin.
327 GDPR, m. 30.
328 GDPR, m. 37-39.
329 GDPR, m. 35.
330 GDPR, m. 25.
331 GDPR, m. 12, 24.
332 GDPR, m. 40, 42.
333 Article 29 Working Party, Opinion 3/2010 on the principle of accountability, WP 173, Brussels, 13 July 2010.
334 GDPR m. 27(1); **Develioğlu**, s. 98, 99.
335 GDPR m. 27(3).

AB dışındaki veri sorumlusunun birden fazla AB ülkesinde bulunan veri sahiplerinin verilerini işliyor olması durumunda temsilcinin bu ülkelerden hangisinde bulunması ve dolayısıyla hangi ülkenin veri koruma otoritesi nezdinde tescil edilmesi gerektiği konusunda seçim hakkı veri sorumlusuna bırakılmıştır.[336] Veri sorumlusu ilgili ülkelerden kendisi için en uygun olanında temsilci atayabilir. Ancak temsilci hangi ülkede olursa olsun, tüm AB vatandaşlarına yönelik aydınlatma metinlerinde temsilcinin kimlik ve iletişim bilgileri yer almalıdır.[337]

İşlemenin nadir olarak gerçekleştiği ve özel nitelikli kişisel verilerin büyük ölçekli olarak işlenmesinin söz konusu olmadığı hallerde, işleme faaliyetinin mahiyeti, bağlamı, kapsamı ve amaçları dikkate alındığında söz konusu işlemenin gerçek kişilerin hakları ve özgürlükleri açısından bir riske sebep olmasının muhtemel olmadığı sonucuna ulaşılıyorsa temsilci atanmasına gerek yoktur.[338] Ayrıca ilgili işleme bir kamu kuruluşu veya organı tarafından gerçekleştiriliyorsa, bu kuruluş veya organın Birlik içerisinde bir temsilci ataması aranmaz.[339]

95/46/EC sayılı Direktif'in 4/2. maddesine göre, veri sorumlusunun AB topraklarında yerleşik olmaması ve işleme amaçları için AB topraklarındaki otomatik cihazlar kullanılmış ise, veri sorumlusu kendisine karşı açılacak davalara zarar vermeksizin, o üye ülke topraklarında yerleşik bir temsilci atamakla yükümlü kılınmıştı.

GDPR'ın 4/17. maddesine göre temsilci AB içerisinde kurulu bulunan, 27. madde uyarınca veri sorumlusu veya işleyen tarafından yazılı olarak belirlenen, GDPR kapsamındaki yükümlülükleri ile ilgili olarak veri sorumlusu veya işleyeni temsil eden gerçek veya tüzel kişi şeklinde tanımlanmıştır. Dolayısıyla temsilci ataması yazılı olarak yapılmalıdır. Ayrıca temsilci olarak gerçek kişiler gibi tüzel kişiler de atanabilecektir (GDPR, rec. 80).

Kişisel verileri kendilerine mal veya hizmetlerin sağlanması ile ilgili olarak işlenen veya davranışı izlenen (GDPR, m. 3/2) veri sahiplerinin bulunduğu üye devletlerde faaliyet gösteren veri sorumlusu/işleyenler temsilci atamakla yükümlüdür (GDPR, rec. 80, m. 27/3).

Temsilci, işleme faaliyeti ile ilgili tüm hususlarda, GDPR'a uygunluk sağlanması amacıyla özellikle denetim makamları ve veri ilgilileri tarafından veri sorumlusu veya işleyene ek olarak veya bunlar yerine muhatap kabul edilmek üzere yetkilendirilir (GDPR, m. 27/4).

---

336 Guidelines 3/2018 on the territorial scope of the GDPR (Article 3) - Version for public consultation Adopted on 16 November 2018, s. 21.

337 Guidelines 3/2018 on the territorial scope of the GDPR (Article 3) - Version for public consultation Adopted on 16 November 2018, s. 12.

338 GDPR m. 27(2)(a).

339 GDPR m. 27(2)(b).

B. Ortak Veri Sorumlularının İş Bölümü Anlaşması Yapma Yükümlülüğü

Yukarıda açıklandığı üzere, iki ya da daha fazla sayıda veri sorumlusunun işleme amaçları ve yöntemlerini ortak bir şekilde belirlediği hallerde, bu veri sorumluları ortak veri sorumlularıdır. Birlik veya Üye Devlet hukuku tarafından belirlenmiş olmadıkça, ortak veri sorumlularının Tüzükte yer alan yükümlülüklerinin gerçekleştirilecek bir anlaşma ile şeffaf bir şekilde belirlemesi gerekmektedir.[340]

Ortak veri sorumluları her iki veri sorumlusu nezdindeki veri işleme faaliyetlerinin hukuka uygunluğundan birlikte mesul oldukları gibi, herhangi bir ihlal durumunda da birlikte müteselsil sorumlu olmaktadır.[341] Diğer ortak veri sorumlusu nezdindeki ihlallerden sorumlu olmak istemeyen veri sorumlusu, hangi yükümlülüklerin hangi veri sorumlusu bakımından yerine getirileceğini açıkça düzenlemelidir[342]. Bu kapsamda tarafların sorumluluk ve sorumsuzluk alanları somut ve ayrıntılı olarak belirlenmelidir.[343] Bu noktada tarafların sorumlulukların veri sahiplerinin mağduriyetine yol açacak şekilde sorumsuzluk alanları oluşturacak şekilde düzenlenemeyeceği aşikârdır. Böyle bir düzenleme hükümsüz olacak ve her ir veri sorumlusu ayrı ayrı ve müteselsil olarak sorumlu olmaya devam edecektir. Veri sahiplerinin haklarının kullandırılmasına yönelik yükümlülükler ise ortak veri sorumlularından birine devredilemez[344]. Her bir veri sorumlusunun veri sahiplerinin haklarını kullanabilmeleri için gerekli başvuru ve cevap mekanizmalarını GDPR'a uygun şekilde tesis etmesi gerekir.

Sonuç olarak her bir veri sorumlusunun sorumluluk ve sorumsuzluk alanları açık ve net bir anlaşmayla belirlenmelidir. Aksi halde hangi veri sorumlusu nezdinde gerçekleştiğine bakılmaksızın her bir yükümlülük için her bir veri sorumlusu müteselsil sorumlu olacaktır[345].

C. Veri İşleyenlerin Seçimi İle İlgili Yükümlülükler

Tüzüğün 28. maddesi uyarınca, veri sorumlusunun, işleme faaliyeti esnasında Tüzüğün gerekliliklerinin yerine getirilmesini ve veri sahibinin haklarının korunmasını sağlayacak biçimde

---

340 GDPR m. 26(1); **Develioğlu**, s. 102.

341 Guide to General Data Protection Regulatin- Information Commissioner's Office, https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/controllers-and-processors/what-does-it-mean-if-you-are-joint-controllers/ (Son erişim: 19.07.2019)

342 Guide to General Data Protection Regulatin.

343 **Gernot Fritz/Nadja Paulus**, "CJEU rules on joint controllership – what does this mean for companies?", Freshfields Bruckhaus Deringer LLP, https://digital.freshfields.com/post/102f0aw/cjeu-rules-on-joint-controllership-what-does-this-mean-for-companies, (Son erişim: 19.07.2019).

344 **Fritz/Paulus.**

345 Guide to General Data Protection Regulatin.

uygun teknik ve düzenlemeye ilişkin tedbirler uygulama hususunda yeterli güvenceler sağlayan veri işleyenleri kullanması gerekmektedir.[346]

D. Kayıtlar ile ilgili Yükümlülükler (Documentation Requirements)

i. Veri Koruma Politikaları Oluşturulması

Veri sorumlusu, veri işleme faaliyetinin GDPR hükümlerine uygun olarak gerçekleştirilmesini sağlamak ve bu şekilde gerçekleştirildiğini gösterebilmek için uygun teknik ve organizasyonel tedbirleri almalı ve uygulamalıdır (GDPR, m. 24/1). Bu amaçla uygun veri koruma politikalarını uygulayacaktır (GDPR, m. 24/2). Şirketlerin uygun veri koruma politika kuralları amaçlar, anahtar terimlerin tanımları, temel ilkeler ve kişisel veri işlemesinin amaçları, sorumluluklar ve bu konulardaki ana denetleyici otoriteyi içermelidir.[347]

ii. Mahremiyet Bildirimi (Privacy Notice)

Veri sorumlusu kişisel verilerin işlenmesine ilişkin her türlü bildirimi kısa, öz, şeffaf, anlaşılır ve kolay erişilebilir bir biçimde veri sahibine yazılı/elektronik/sözlü olarak sunabilmelidir (GDPR, m. 12/1). Aynı şekilde veri sahibinin kişisel verilerinin toplanması durumunda, veri sorumlusu kendi kimlik ve irtibat bilgileri, veri koruma görevlisinin irtibat bilgileri, veri işlemesinin yasal dayanağı, buna ilişkin varsa meşru menfaatler, kişisel verilerin alıcıları, kişisel verilerin üçüncü bir ülke/uluslararası kuruluşa aktarılıp aktarılmayacağı ile buna ilişkin güvenceleri veri sahibine sunmalıdır (GDPR, m. 13/1, 14/1). Yine verilerin kişisel verilerin saklanacağı süre, bu sürenin net olmaması halinde buna ilişkin kullanılan kriterler, verilerin taşınabilirliğine, düzeltilmesine, kısıtlanmasına ve silinmesine ilişkin açıklamalar, veri işlenmesine ilişkin rızanın geri çekilme hakkı, bir denetim makamına şikâyet hakkı gibi hususlar da veri sahibine sunulmalıdır (GDPR, m. 13/2). Bu bilgiler genel olarak veri sorumlusu şirketlerin verilerini işlediği müşterilere ilişkin açıklayıcı ve anlaşılır nitelikte olmalıdır. Şirketler bu açıklamaları web sitelerinde de sunabilecektir.

iii. Veri Saklama ve İşleme Kayıtları (Data Retention/Records of processing activities)

Veri sorumlusu işlenen kişisel verilere ilişkin yazılı (elektronik dahil) bir kayıt tutmakla yükümlü kılınmıştır (GDPR, m. 30/1). Bu kayıtlarda veri sorumlusu, veri koruma görevlisi, veri işleme amaçları, veri sahibi ve kişisel veri kategorileri, alıcılar, veri aktarımları, verilerin silinmesine ilişkin süre sınırları gibi açıklamalar yer alacaktır (GDPR, m. 30/1-2).

---

346 GDPR m. 28(1).

347 **Punit Bhatia**, Contents of Data Protection Policy according to GDPR, https://advisera.com/eugdpracademy/knowledgebase/contents-of-the-data-protection-policy-according-to-gdpr/ (Son Erişim Tarihi: 18.03.2019).

iv. Veri Sahibi Rıza Formu

Veri işlemesinin rızaya dayalı olduğu hallerde, rıza talebi açık bir şekilde ayırt edilebilir, anlaşılır ve kolay erişilebilir bir biçimde açık ve sade bir dil kullanılmak suretiyle sunulmalıdır (GDPR, m. 7/2). Rıza, yazılı form dışında elektronik veya sözlü olarak da sunulabilecektir (GDPR, rec. 32). Rıza, bir internet sitesini ziyaret esnasında kutuyu işaretleme şeklinde olabilecek, buna karşılık sessizlik (silence), önceden işaretlenen kutucuklar (pre-ticked boxes) veya hareketsizlik (inactivity) rıza olarak yorumlanamayacaktır. İşlenen her bir veri için ayrı rıza gereklidir. Rızanın verildiği durumlarda, veri sorumlusu veri sahibinin rızası bulunduğunu ispatlayabilmelidir (GDPR, rec. 42).

Veri sahibinin çocuk olduğu durumlarda rızanın geçerli olabilmesi için çocuğun en az 16 yaşında olması gerekir (GDPR, m. 8/1). Veri sahibinin 16 yaşından küçük olduğu durumlarda, rızanın velayet hakkı sahibi tarafından verilmesi veya çocuk tarafından verilip velayet hakkı sahibi tarafından onaylanması şarttır (GDPR, m. 8/1).

Önceden işaretlenen kutucukların geçerli bir rıza olup olmamasına ilişkin ABAD önünde bir uyuşmazlık bulunmaktadır. Buna göre "dein-macbook.de" internet sitesi online ortamda promosyon amaçlı çekilişler yaparak alışveriş yapan kullanıcılara hediyeler dağıtmaktadır. Bunun için kullanıcıların isim, adres bilgileri gibi kişisel verileri kayıt edilmektedir. Kullanıcılar, bu bilgileri sponsorluk yapan kuruluşlara da önlerine çıkan kutucuğu işaretlemek suretiyle (pre-ticked boxes) vermeyi kabul etmektedirler. Çekilişe katılım Planet49 isimli şirketin, tüketicilerin davranışlarını takip etmesi ve hedefli reklamlarını kullanabilmesi için çerezlere izin verilmesine ilişkin kutucuk işaretleme ile mümkün olmaktadır. Olayın, GDPR'ın yürürlüğe girdiği dönem öncesi olması nedeniyle davanın Hukuk Sözcüsü (Advocate General), 95/46/EC sayılı Direktif'e göre de bir değerlendirme yapmıştır. Hukuk Sözcüsüne göre 95/46/EC sayılı Direktif'in 2/h maddesine göre rızanın "özgürce ve bilgilendirilme sonrası" verilmesinin gerekmesi, 7/a maddesine göre rızanın "açık, net ve kesin" biçimde yapılmasının gerekmesi nedeni ile bu tür önceden işaretlenmiş kutucuklar yolu ile kişisel verilerin işlenmesine rıza gösterilmesi geçersizdir. Madde 29 Çalışma Grubu'nun da rızaya ilişkin görüşü bu doğrultudadır. Ayrıca GDPR ile rıza hususu çok daha açık ve kesinlik gerektiren şekilde düzenlenmiştir. Uyuşmazlıkta, kullanıcı çekilişe katılmak için kutucuğu işaretlemek zorunda bırakılmıştır. Bu işaretleme ile de, kullanıcı çerez (cookies) kullanımına izin vermektedir. GDPR'ın 7/4. maddesiyle kullanıcıyı asıl hizmetten yararlanmak için bu tür aceleye getiren rıza alma şekilleri (bundling) yasaklanmıştır. Dolayısıyla Sözcü'ye göre kullanıcılar önceden işaretlenen bu kutucukların sonuçları hakkında yeteri kadar

bilgilendirilmemiştir ve bu tür alınmış bir rıza geçerli bir rıza olarak değerlendirilmemelidir.[348] ABAD'ın kararının da bu yönde olacağını düşünüyoruz. Çünkü yeterli bilgilendirme yapılmaksızın bilhassa hizmetten yararlanmayla eşzamanda yapılan işaretlenen kutucuklar hem 95/46/EC sayılı Direktif hem de GDPR'ın 7 ve 42. Gerekçesi uyarınca geçerli bir rıza olarak yorumlanamaz.

v. Veri İşleme Antlaşması

Veri sorumlusu kendi adına veri işleme faaliyetinin gerçekleştirilmesini istemesi durumunda, işleyene spesifik ve yazılı onay vermelidir. Bu onayın verildiği durumlarda veri sorumlusu, veri işleyenlerden GDPR gereksinimleri olan teknik ve organizasyonel tedbirleri uygulamak için gerekli olan uzman bilgisi, güvenilirlik ve kaynaklar gibi konularda yeterli güvenceleri sağlamasını bekleyecektir. Bu tür durumlarda veri sorumlusu ve işleyen, veri işleme konusu, süresi, amacı, işlenen kişisel verinin çeşidi, veri sahiplerinin kategorileri gibi konularda Sözleşme ve AB mevzuatı/AB üyesi ulusal mevzuatına uymakla yükümlü olacaklardır. Veri sorumlusu adına işlemenin tamamlanmasından sonra, veri işleyen, işlenen verinin AB mevzuatı veya üye ülke mevzuatı uyarınca saklanması gerekmediği sürece, silmekle veya temin ettiği yere iade ile yükümlü olacaktır (GDPR, rec. 81).[349]

vi. Veri İhlali Açıklaması ve Bildirimi

Kişisel veri ihlalinin gerçek kişilerin hakları ve özgürlükleri açısından yüksek bir riske sebebiyet vermesinin muhtemel olduğu hallerde, veri sorumlusu kişisel veri ihlalini gereksiz bir gecikmeye mahal vermeden veri sahibine iletmekle yükümlüdür (GDPR, m. 34/1). Bir kişisel veri ihlali olması durumunda, veri sorumlusu ihlalden haberdar olduğu andan itibaren en geç 72 saat içinde, kişisel veri ihlalini denetim makamına bildirmekle yükümlüdür (GDPR, m. 33/1). Yapılan veri ihlali bildiriminde şu hususlara dikkat edilmelidir (GDPR, m. 33/3):

- İlgili veri sahibi ve veri kaydı kategorileri ve sayısına ilişkin açıklamaların yer aldığı veri ihlalinin niteliği açıklanmalıdır.

- Veri koruma görevlisi veya daha fazla bilginin elde edilebileceği diğer irtibat noktasına ilişkin isim ve gerekli bilgiler sağlanmalıdır.

- Kişisel veri ihlalinin olası sonuçları açıklanmalıdır.

---

348 Opinion of Advocate General Szpunar, delivered on 21 March 2019 (1), Case C-673/17, Planet 49 GmbH v. Bundesverband der Verbraucherzentralen und Verbraucherverbande-Verbraucherzentrale Bundesverband e.V., http://curia.europa.eu/juris/document/document.jsf?text=&docid=212023&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=5537788 (Son Erişim Tarihi: 22.03.2019)

349 Veri sorumlusunun, GDPR 28/2 maddesine göre işleyen ile yapabileceği Veri İşleme Antlaşması örneği için bkz. http://www.fastviewer.com/demo/FV-ADV_Kunden_EN.pdf (Son Erişim Tarihi: 19.03.2019)

- Veri ihlalinin olası olumsuz etkilerinin azaltılmasına yönelik alınan/önerilen tedbirler açıklanmalıdır.

Bu bilgilerin aynı zamanda sağlanmasının mümkün olmadığı durumlarda, bilgiler gereksiz ek bir gecikmeye mahal vermeksizin, aşamalı olarak da sağlanabilecektir (GDPR, m. 33/4).

II. Veri İşlemede Hukuka Uygunluk Nedenleri

A. Kişisel Verilerin İşlenmesinde Hukuka Uygunluk Nedenleri

Yukarıda açıklandığı üzere, kişisel verilerin hukuka uygun, adil ve şeffaf bir şekilde işlenmesi Tüzükte yer alan ilkelerden birisidir. Bu ilke uyarınca kişisel verilerin işlenmesi hukuka uygun olmalıdır ve işleme faaliyeti, ancak aşağıdaki hususlardan en az biri geçerli olduğunda ve olduğu ölçüde hukuka uygundur:

(a) Veri sahibinin bir ya da daha fazla sayıda belirli bir amaca yönelik olarak kişisel verilerinin işlenmesine onay vermesi,

(b) Veri sahibinin taraf olduğu bir sözleşmenin uygulanması veya bir sözleşme yapılmadan önce veri sahibinin talebiyle adımlar atılması için, işleme faaliyetinin gerekli olması,

(c) Veri sorumlusunun tabi olduğu bir yasal yükümlülüğe uygunluk sağlanması amacı ile işleme faaliyetinin gerekli olması,

(d) Veri sahibinin veya başka bir gerçek kişinin hayati menfaatlerinin korunması amacı ile işleme faaliyetinin gerekli olması,

(e) Kamu yararına gerçekleştirilen bir görevin yerine getirilmesi veya veri sorumlusuna verilen resmi bir yetkinin uygulanması hususunda işleme faaliyetinin gerekli olması,

(f) Özellikle veri sahibinin çocuk olması halinde veri sahibinin kişisel verilerin korunmasını gerektiren menfaatleri veya temel hakları ve özgürlüklerinin bir veri sorumlusu veya üçüncü bir kişi tarafından gözetilen meşru menfaatlere ağır basması haricinde, söz konusu menfaatler doğrultusunda işleme faaliyetinin gerekli olması.

1. Rıza

a. Rıza Tanımları

Tüzük uyarınca veri sahibinin rızası, *"veri sahibinin bir beyan yoluyla ya da açık bir onay eylemiyle kendisine ait kişisel verilerin işlenmesine onay verdiğini gösteren özgür bir şekilde verilmiş spesifik, bilinçli ve açık göstergedir."*[350] Diğer düzenlemelere bakılırsa rıza, 95/46/EC sayılı Direktif'te veri sahibinin *"kendisine dair kişisel verilerin işlenmesi için veri sahibinin*

[350] Geçerli biz rızadan bahsedebilmek için medeni hukuk anlamında aranan koşullar, kişisel verilerin korunması hukuku açından da gereklidir; örneğin hak ehliyet vb.

kabulüne işaret eden, özgürce ve bilgilendirme yapıldıktan sonra alınan rıza" şeklinde tanımlanmıştır. 6698 sayılı KVKK'da ise tek başına rıza kavramına yer verilmemiş, *"açık rıza"* ifadesi kullanılmıştır. KVKK'ya göre açık rıza *"belirli bir konuya ilişkin bilgilendirilmeye dayanan ve özgür iradeyle açıklanan rıza"*dır.[351] Bu tanımlardan yola çıkılarak Tüzük ile kişisel verilerinin işlenmesi için veri sahibinden alınması gereken rıza için öngörülen şartların kuvvetlendirildiği sonucuna ulaşılabilecektir.[352] Dolayısıyla her ne kadar Tüzükte sözcük olarak "açık rıza" kavramına yer verilmediyse de KVKK ile karşılaştırma yapıldığında "bilgilendirmeye dayalı bir rıza" alındığı için bunun da açık rıza olduğu görülmektedir.

Kişisel verilerin işlenmesi için gerekli olan rıza 95/46/EC sayılı Direktif'in 7/1 maddesinde net şekilde (unambiguously) verilmesi ve açık şekilde (explicit consent) verilmesi (95/46/EC, Rec. 33) şeklinde düzenlenmişti. GDPR'da ise rıza hususu çok daha ayrıntılı ve iradeyi esas alır şekilde düzenlenmiştir.[353] GDPR'ın 7/2 maddesine göre veri sahibinin rızasını yazılı bir beyan ile vermesi durumunda, rıza talebinin diğer hususlardan açık bir şekilde ayırt edilebilecek bir şekilde, anlaşılır ve kolay bir şekilde erişilebilir bir biçimde (clearly distinguishable from the other matters, in an intelligible and easily accessible form), açık ve sade bir dil (clear and plain language) kullanılarak sunulması gerekir. Rızanın varlığını veri sorumlusu (controller) ispatlamalıdır (GDPR, m. 7/1). Rızanın özgür bir şekilde verilip verilmediği değerlendirilirken, her şeyden önce rızanın bir hizmetin sağlanması da dahil olmak üzere bir sözleşmenin ifası ile ilgili olarak verilip verilmediği dikkate alınmalıdır (GDPR, m. 7/4). GDPR'ın 32. gerekçesinde de rızanın serbest bir şekilde, belirli, bilgilendirilmiş şekilde ve tereddüde mahal bırakmayacak açıklıkta (clear affirmative act establishing a freely given, spesific, informed and unambiguous indication) şekilde yazılı, elektronik yolla veya sözlü olarak verilebileceği düzenlenmiştir.[354] Veri sahibinin çocuk olması hali de Tüzüğün 8 inci maddesinde özel olarak düzenlenmiştir. Öncelikle veri sahibinin çocuk olması halinde, veri sahibinin kişisel verilerinin korunmasını gerektiren menfaatleri veya temel hakları ve özgürlüklerinin bir veri sorumlusu veya üçüncü bir kişi tarafından gözetilen meşru menfaatlere ağır basmaması gerekir ve veri işlemenin söz konusu menfaatler doğrultusunda gerekli olması gerekir (GDPR, m. 6/1-f). Veri sahibi çocuğun geçerli rızası için en az 16 yaşında olması gerekir. Çocuğun 16 yaşından küçük olması halinde, söz konusu veri işleme faaliyeti, ancak rızanın çocuk üzerinde

351 **Dülger**, s. 22, 23.
352 **Dülger**, s. 67.
353 **Eugenia Politou/Efthimios Alepis/Constantinos Patsakis**, "Forgetting Personal Data and Revoking Consent under the GDPR: Challenges and Proposed Solutions", Journal of Cybersecurity, V. 4, I. 1, January 2018.
354 Handbook on European Data Protection, s.112 vd.

velayet hakkı bulunan kişi tarafından verilmesi ve onaylanması halinde ve bu onay devam ettiği müddetçe hukuka uygun olacaktır (GDPR, m. 8/1).

b. Bilinç Unsuru

Tüzükteki tanımdan anlaşıldığı üzere, rıza "bilinçli" olmalıdır, yani veri sahibi rıza beyanında bulunmadan önce konuya ilişkin bilgi sahibi olmalıdır. Madde 29 Çalışma Grubu yapılacak bu bilgilendirmenin açık ve anlaşılabilir şekilde gerçekleştirilmesi ve işlenen veriler, işlemenin amaçları, verilerin muhtemel alıcıları ve veri sahibinin hakları gibi konularda tam ve eksizsiz bilgiler içermesi gerektiğini belirtmiştir.[355] Ayrıca, kişisel verilerin işlenmesine verilen rızanın konuya özel olması büyük önem arz etmektedir. Bu anlamda rıza "spesifik" olmalıdır ve rızanın hangi işleme faaliyetlerine yönelik olarak verildiği açıkça anlaşılabilmelidir.[356] Dolayısıyla, verilerin işlenmesine yönelik açıklanan genel bir rıza, Tüzük anlamında koşulları sağlayan bir hukuka uygunluk hali oluşturmayacaktır.[357]

c. Ayırt Edicilik, Anlaşılırlık ve Erişilebilirlik Unsuru

Veri sahibinin rızasının diğer hususlarla da ilgili olan yazılı bir beyan bağlamında verilmesi durumunda, yani beyanın rızadan başka konuları da kapsaması durumunda; rıza talebinin, diğer hususlardan açık bir şekilde ayırt edilebilecek bir şekilde, anlaşılır ve kolayca erişilebilir bir biçimde, açık ve sade bir dil kullanılarak sunulması gerekir. Söz konusu beyanın herhangi bir kısmının Tüzüğün ihlali niteliğinde olması durumunda bu kısmın bağlayıcı olmayacağı da açıkça düzenlenmiştir.[358]

Veri işlemesinin rızaya dayalı olduğu hallerde, rıza talebi açık bir şekilde ayırt edilebilir, anlaşılır ve kolay erişilebilir bir biçimde açık ve sade bir dil kullanılmak suretiyle sunulmalıdır (GDPR, m. 7/2). Rıza, yazılı form dışında elektronik veya sözlü olarak da sunulabilecektir (GDPR, rec. 32). Rıza, bir internet sitesini ziyaret esnasında kutuyu işaretleme şeklinde olabilecek, buna karşılık sessizlik (silence), önceden işaretlenen kutucuklar (pre-ticked boxes) veya hareketsizlik (inactivity) rıza olarak yorumlanamayacaktır. İşlenen her bir veri için ayrı rıza gereklidir. Rızanın verildiği durumlarda, veri sorumlusu veri sahibinin rızası bulunduğunu ispatlayabilmelidir (GDPR, rec. 42).

---

355 **Giakoumopoulos/Buttarelli/O'Flaherty**, s. 146; Article 29 Working Party (2007), Working Document on the processing of personal data relating to health in electronic health records (EHR), WP 131, Brüksel, 15 Şubat 2007.

356 **Develioğlu**, s. 52, 53.

357 **Giakoumopoulos/Buttarelli/O'Flaherty**, s. 112.

358 GDPR, m. 7(2).

Bu noktada ayrıca rıza formuna ilişkin yukarıdaki açıklamalarımı hatırlatıyor, tekrara girmemek adına okuyucuyu ilgli başlığa yönlendirmekle yetiniyorum.

d. Rızanın Geri Alınabilirliği

Önem arz eden bir diğer husus ise veri sahibinin her zaman rızasını geri alma hakkının bulunmasıdır. Veri sahibi, rıza vermeden önce bu hususta bilgilendirilmelidir. Ayrıca rızanın geri alınması, rızanın verilmesi kadar kolay olmalıdır.[359] Rızanın geri alınması ileriye yönelik bir hak olup, geçmişteki işlemler için bir etki doğurmaz.[360]

e. Rızanın Özgürce Verilmesi Unsuru

Ayrıca, rızanın geçerli olması için *özgür bir şekilde verilmesi* gereklidir. Bu anlamda, rızanın özgürce verilip verilmediği değerlendirilirken, her şeyden önce, bir hizmetin sağlanması da dahil olmak üzere, bir sözleşmenin ifasının, söz konusu sözleşmenin ifası için gerekmeyen kişisel verilerin işlenmesine yönelik bir rızaya bağlı olup olmadığına azami özen gösterilmesi gerektir.[361] Böylece Tüzük, taraflar arasında güç dengesizliğinin mevcut olduğu hallerde verilen rızayı açıkça geçersiz saymıştır.[362] Örneğin; Madde 29 Çalışma Grubu, işçilerin, işçi/işveren ilişkisinden kaynaklanan tabi olunuş nedeniyle neredeyse hiçbir zaman özgürce rıza verebilecek, rıza vermeyi reddedebilecek veya rızasını geri alabilecek bir pozisyonda olmadığını belirtmiştir. Buna göre, güç dengesizliği sebebiyle, işçiler, yalnızca rıza vermeyi reddetmelerine herhangi bir negatif sonucun bağlanmadığı nadir durumlarda özgür iradeleriyle rıza verebileceklerdir.[363] Başka bir örnek ise, yolcu isim kayıtlarının bir ülkenin göç idaresine aktarılmasına ilişkin yolcular ile bir havayolu arasında yapılan bir anlaşma düşünülebilir. Yolcuların ilgili ülkeyi ziyaret edebilmeleri için başka bir şansları olmadığından böyle bir anlaşmanın veri koruma hukuku anlamında özgür bir şekilde verilen bir rızaya dayandığını söylemek mümkün değildir. Bu verilerin hukuka uygun bir şekilde göç idaresine aktarımından bahsedilebilmesi için, bu aktarımın rızadan başka bir yasal dayanağı olması gerekir.[364]

---

359 GDPR, m. 7(3).
360 **Giakoumopoulos/Buttarelli/O'Flaherty**, s. 150.
361 GDPR, m. 7(4).
362 **Develioğlu**, s. 54.
363 **Giakoumopoulos/Buttarelli/O'Flaherty**, s. 144.
364 **Giakoumopoulos/Buttarelli/O'Flaherty**, s. 146.

f. Çocukların Rızası

Rıza ile ilgili belirtilmesi gereken diğer bir konu ise, doğrudan bir çocuğa bilgi toplumu hizmetleri[365] sağlanması ile ilgili olarak çocuğun kişisel verilerinin işlenmesidir. Tüzük uyarınca, bir çocuğa bilgi toplumu hizmeti sunulurken kişisel verilerinin işlenmesinin geçerli bir şekilde rızasına dayanabilmesi için çocuk en az 16 yaşında olmalıdır.[366] Çocuğun 16 yaşından küçük olması halinde, söz konusu işleme faaliyeti, ancak rızanın çocuk üzerinde velayet hakkı bulunan kişi tarafından verilmesi veya onaylanması halinde ve verildiği veya onaylandığı ölçüde hukuka uygundur.[367] Üye Devletler, belirlenen bu yaşı 13 yaşına kadar indirebilir.[368] Ayrıca, çocuklara ait verilerin işlenmesi ile ilgili getirilen bu düzenlemelerin, Üye Devletlerin sözleşmeler hukuku anlamında sözleşmenin geçerliliği, kurulması ve hükmüne ilişkin kurallarını etkilemeyeceği de Tüzükte belirtilmiştir.[369]

Veri sahibinin çocuk olduğu durumlarda rızanın geçerli olabilmesi için çocuğun en az 16 yaşında olması gerekir (GDPR, m. 8/1). Veri sahibinin 16 yaşından küçük olduğu durumlarda, rızanın velayet hakkı sahibi tarafından verilmesi veya çocuk tarafından verilip velayet hakkı sahibi tarafından onaylanması şarttır (GDPR, m. 8/1).

2. İşlemenin Bir Sözleşmenin Kurulması veya İfası İçin Gerekli Olması

Veri sahibinin taraf olduğu bir sözleşmenin uygulanması veya bir sözleşme yapılmadan önce veri sahibinin talebiyle adımlar atılması için işleme faaliyetinin gerekli olması durumunda gerçekleştirilecek işleme hukuka uygundur.[370]

3. İşlemenin Veri Sorumlusunun Hukuki Yükümlüğünü Yerine Getirebilmesi İçin Zorunlu Olması

Veri sorumlusunun tabi olduğu bir yasal yükümlülüğe uygunluk sağlanması amacı ile işleme faaliyetinin gerekli olması durumunda gerçekleştirilecek veri işleme hukuka uygundur.[371] Bu hukuka uygunluk sebebi, hem özel alandaki hem kamu alanındaki veri sorumluları için geçerlidir.[372] Söz konusu hukuki yükümlülük ilgili devletin yerel hukukundan veya AB

---

365 2015/1535 sayılı Avrupa Parlamentosu ve Konsey Direktifi m. 1(1)(b) uyarınca bilgi toplumu hizmetleri, uzaktan ve elektronik vasıtalarla ve hizmet alıcısının bireysel talebi sonucunda, kural olarak bedel karşılığı sağlanan hizmetlerdir.

366 **Develioğlu**, s. 54.

367 GDPR, m. 8(1).

368 GDPR, m. 8(1) son cümle.

369 GDPR, m. 8(3); **Develioğlu**, s. 55.

370 GDPR, m. 6(1)(b).

371 GDPR, m. 6(1)(c).

372 **Giakoumopoulos/Buttarelli/O'Flaherty**, s. 151.

hukukundan kaynaklanabilir. Kişisel verilerin işlenmesi için dayanak oluşturan ilgili mevzuatlar, AİHS'nin "özel ve aile hayatına saygı hakkı" ve AB Şartı'nın "özel ve aile yaşamına saygı" ve "kişisel bilgilerin korunması" hükümlerine uygun olmalıdır.[373]

4. İşlemenin İlgili Kişinin veya Diğer Bir Gerçek Kişinin Hayati Menfaatlerini Korumak İçin Gerekli Olması

Veri işleme faaliyetinin veri sahibinin veya başka bir gerçek kişinin hayati menfaatlerinin korunması amacı ile gerekli olması durumunda gerçekleştirilecek işleme hukuka uygundur.[374] Kural olarak, bu hükme dayanarak veri işleme, yalnızca işlemenin başka bir sebebe dayandırılmadığı durumlarda yapılmalıdır. Dolayısıyla bu hüküm kapsamında veri işleme yetkisi, ikincil niteliktedir.[375]

Bu düzenlemenin 6698 sayılı KVKK'da birebir karşılığı yoktur.

5. İşlemenin Kamu Yararı İçin Gerçekleştirilen Bir Görevin İfası İçin veya Veri Sorumlusunun Resmi Yetkisinin Kullanılması İçin Gerekli Olması

Veri işleme faaliyetinin kamu yararına gerçekleştirilen bir görevin yerine getirilmesi veya veri sorumlusuna verilen resmi bir yetkinin uygulanması hususunda gerekli olması durumunda gerçekleştirilecek işleme hukuka uygundur.[376] Bu çerçevede, resmi yetkinin veri sorumlusu tarafından kullanılıyor olması şart değildir. Bu yetkiye sahip bir üçüncü kişinin yetkisi kapsamındaki taleplerine göre hareket edilmesi de bu hukuka uygunluk sebebi kapsamındadır.[377]

Bu başlık altında veri işlemenin gerçekleştirilebilmesi için, söz konusu işlemenin AB hukukunda veya yerel ülke hukukunda yasal bir dayanağı olmalıdır. Söz konusu hukuki dayanak açık ve net, ayrıca öngörülebilir olmalıdır.[378] Ayrıca, AB üyesi devletlerin, Tüzükte yer alan veri işleme yetkisine ilişkin kuralların uygulanması için daha spesifik hükümler uygulamaya devam edebileceği veya uygulamaya koyabileceği açıkça düzenlenmiştir.[379]

6698 sayılı KVKK'da ise, Tüzüğe kıyasla daha geniş bir ifade kullanılmıştır ve kamu yararı şartı aranmaksızın veri işleme imkânının kanunlarda açıkça öngörülmesi halinde işlemenin hukuka uygun kabul edileceği düzenlenmiştir.[380]

---

373 **Giakoumopoulos/Buttarelli/O'Flaherty**, s. 152.
374 GDPR, m. 6(1)(d).
375 **Voigt/von dem Bussche**, s. 108.
376 GDPR, m. 6(1)(e).
377 **Develioğlu**, s. 64.
378 **Voigt/von dem Bussche**, s. 107, 108.
379 GDPR, m. 6(2).
380 **Develioğlu**, s. 65.

6. Veri İşlemenin Meşru Menfaatlere Ulaşmak Amacıyla Gerekli Olması

Veri sahibinin, özellikle çocuk olması halinde, kişisel verilerinin korunmasını gerektiren menfaatleri veya temel hakları ve özgürlüklerinin, bir veri sorumlusu veya üçüncü bir kişi tarafından gözetilen meşru menfaatlere ağır basması haricinde, söz konusu menfaatler doğrultusunda işleme faaliyetinin gerekli olması durumunda gerçekleştirilecek işleme hukuka uygundur.[381]

Meşru bir menfaatin varlığı her olay bazında dikkatle incelenmelidir.[382] Veri sorumlusunun veri işleme faaliyetinden meşru menfaati olduğu belirlenirse, bu meşru menfaat ile veri sahiplerinin menfaatleri veya temel hak ve özgürlükleri arasında bir denge kurulması gerekir.[383] Böyle bir değerlendirme sırasında veri sahibinin makul beklentileri de hesaba katılmalıdır. Veri sahibinin haklarının veri sorumlusunun meşru menfaatlerine ağır basması durumunda, veri sorumlusu, veri işlemenin veri sahibinin hakları üzerindeki etkilerini minimuma indirme amacıyla tedbirler alıp güvenceler getirebilir, böylece dengeyi tersine döndürerek bu hukuka uygunluk sebebine dayanabilir.[384]

ABAD, içtihatlarında "denge testi"ni detaylıca incelemiştir. Örneğin; *Valsts policijas Rīgas reģiona pārvaldes Kārtības policijas pārvalde*[385] davasında, ABAD, meşru menfaatlere dayanarak kişisel veri işlemesinin gerçekleştirebilmesi için üç şartın tümünün sağlanması gerektiğini belirtmiştir[386]:

(1) Kişisel verinin açıklanacağı üçüncü kişinin meşru bir menfaati olmalıdır,

(2) Bu meşru menfaate ulaşmak için ilgili kişisel verinin işlenmesi zorunlu olmalıdır,

(3) Veri sahibinin temel hak ve özgürlükleri veri sorumlusunun veya üçüncü kişilerin meşru menfaatlerinden önemli olmamalıdır.

ABAD ayrıca menfaatler dengesinin olay bazında değerlendirilmesi ve her olayda veri sahibinin haklarının uğrayacağı zararın ağırlığı gibi faktörlerin dikkate alınması gerektiğini ifade etmiştir.[387]

---

381 GDPR, m. 6(1)(f).
382 GDPR, Preamble, Gerekçe 47.
383 Article 29 Working Party (2014), Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC, 4 Nisan 2014.
384 Article 29 Working Party (2014), Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC, 4 Nisan 2014.
385 ABAD, C-13/16, Valsts policijas Rīgas reģiona pārvaldes Kārtības policijas pārvalde v. Rīgas pašvaldības SIA'Rīgas satiksme', 4 Mayıs 2017.
386 Rīgas satiksme, p. 28-34.
387 **Giakoumopoulos/Buttarelli/O'Flaherty**, s. 156, 157.

Kişisel verilerin "meşru menfaatler"e dayanarak işlenmesi durumunda, veri sahibinin, kendi özel durumu ile ilgili gerekçelere dayalı olarak, kendisi ile ilgili kişisel verilerin işlenmesine herhangi bir zamanda itiraz etme hakkı bulunur.[388] İşlemenin devamı için inandırıcı meşru bir sebep sunmadıkça veri sorumlusu işlemeyi durdurmalıdır.[389]

B. Özel Nitelikli Kişisel Verilerin İşlenmesinde Hukuka Uygunluk Nedenleri

Kişilerin ırkı, etnik kökeni, siyasi düşüncesi, felsefi inancı, dini, mezhebi veya diğer inançları, kılık ve kıyafeti, dernek, vakıf ya da sendika üyeliği, sağlığı, cinsel hayatı, ceza mahkumiyeti ve güvenlik tedbirleriyle ilgili verileri ile biyometrik ve genetik verileri özel nitelikli kişisel verilerdir ve bu verilerin işlenmesi kural olarak yasaktır.[390] Tüzüğün 9. maddesinin 2. fıkrasında belirtilen istisnaların mevcudiyetinde ise özel nitelikli kişisel veriler işlenebilecektir:

(a) Veri sahibinin belirtilen bir veya daha fazla sayıda amaca yönelik olarak söz konusu kişisel verilerin işlenmesine açık bir şekilde rıza göstermesi;

(b) Birlik veya Üye Devlet hukuku çerçevesinde ya da Üye Devlet hukuku uyarınca yapılan ve veri sahibinin temel hakları ve menfaatlerine yönelik uygun güvencelerin sağlandığı bir toplu sözleşme çerçevesinde izin verildiği sürece, veri sorumlusunun veya veri sahibinin istihdam ve sosyal güvenlik ve sosyal hukuku koruma alanındaki yükümlülüklerinin gerçekleştirilmesi ve spesifik haklarının kullanılması amacıyla işleme faaliyetinin gerekmesi;

(c) Veri sahibinin fiziksel veya hukuki olarak rıza veremeyecek durumda olması halinde, veri sahibi veya başka bir gerçek kişinin hayati menfaatlerinin korunması açısından işleme faaliyetinin gerekli olması;

(d) İşleme faaliyetinin bir vakıf, birlik veya kâr amacı gütmeyen başka bir organ tarafından siyasi, felsefi, dini veya sendika amacıyla uygun güvencelerle birlikte yürütülen meşru faaliyetleri esnasında işlemenin ve yalnızca organın üyeleri veya eski üyeleri ya da amaçlarıyla bağlantılı olarak kendisi ile düzenli olarak temas halinde bulunan kişilerle ilgili olması ve kişisel verilerin veri sahiplerinin rızası olmaksızın söz konusu organ dışında açıklanmaması koşuluyla gerçekleştirilmesi;

(e) İşleme faaliyetinin veri sahibi tarafından açık bir biçimde kamuya açıklanan kişisel verilerle ilgili olması;

---

388 GDPR, m. 21(1).
389 **Giakoumopoulos/Buttarelli/O'Flaherty**, s. 158.
390 GDPR, m. 9(1).

(f) Yasal iddialarda bulunulması, bu iddiaların uygulanması veya savunulması açısından veya mahkemeler kendi yargı yetkisi çerçevesinde hareket ettiğinde, işleme faaliyetinin gerekmesi;

(g) Gözetilen amaçla orantılı olan, veri koruma hakkının özüne saygı gösteren ve veri sahibinin temel hakları ve menfaatlerinin güvence altına alınması adına uygun ve spesifik tedbirler sağlayan Birlik veya Üye Devlet hukukuna dayalı olarak kayda değer ölçüde kamu yararı adına nedenlerden ötürü işleme faaliyetinin gerekmesi;

(h) Koruyucu hekimlik veya meslek hekimliği amaçları doğrultusunda, Birlik ya da üye devlet hukukuna dayalı olarak veya bir sağlık profesyoneli ile yapılan sözleşme uyarınca çalışanın çalışma kapasitesinin değerlendirilmesi, tıbbi tanı, sağlık veya sosyal bakım hizmetlerinin veya tedavinin sağlanması ya da sağlık veya sosyal bakım sistemleri ve hizmetlerinin yönetilmesi açısından işleme faaliyetinin gerekli olması;

(i) Özellikle mesleki gizlilik olmak üzere veri sahibinin hakları ve özgürlüklerine ilişkin güvence sağlanmasına uygun ve spesifik tedbirler sağlayan Birlik veya üye devlet hukukuna dayalı olarak, halk sağlığı alanında kamu yararına yönelik olarak işleme faaliyetinin gerekmesi;

(j) Kamu yararına yönelik arşivleme amaçları, bilimsel veya tarihi araştırma amaçları ya da istatistiki amaçlar doğrultusunda işleme faaliyetinin gerekmesi.

Ek olarak, Tüzükte, Üye Devletler genetik veriler, biyometrik veriler veya sağlık ile ilgili veriler ile alakalı olarak sınırlamalar da dahil olmak üzere ek koşullar uygulamaya devam edebileceği ya da ek koşullar getirebileceği düzenlenmiştir.[391]

III. Veri İşlemenin Güvenliğine İlişkin Kurallar

A. Veri Güvenliğine İlişkin Başlıca Hükümler

Veri işlemenin güvenliğine ilişkin kurallar, veri sorumlusu ve veri işleyeni, veri işleme faaliyetlerine herhangi bir izinsiz müdahaleyi önlemek için, uygun teknik ve düzenlemeye ilişkin tedbirler alma yükümlülüğü altına sokmaktadır.[392] Bu çerçevede, veri sorumlusu ve işleyen, son teknoloji, uygulama maliyetleri ve işleme faaliyetinin mahiyeti, kapsamı, bağlamı ve amaçlarının yanı sıra gerçek kişilerin hakları ve özgürlükleri açısından çeşitli olasılıklar ve ciddiyetlere sahip riskleri dikkate alarak, risk açısından uygun bir güvenlik seviyesi sağlamak üzere, uygun olduğu hallerde, uygun teknik ve düzenlemeye ilişkin tedbirler uygular.[393]

391 GDPR, m. 9(4).
392 **Giakoumopoulos/Buttarelli/O'Flaherty**, s. 165.
393 GDPR, m. 32.

Alınabilecek önlemlerden bazıları Tüzükte belirtilmiştir. Buna göre (a) kişisel verilerde takma ad kullanımı ve şifreleme; (b) işleme sistemleri ve hizmetlerinin gizliliği, bütünlüğü, elverişliliği ve esnekliğinin sürekli olarak sağlanabilmesi; (c) fiziksel veya teknik bir olay halinde, kişisel verilerin elverişliliği ve kişisel verilere erişimin vakitlice eski haline getirilebilmesi; (d) işleme faaliyetinin güvenliliğinin sağlanmasına yönelik olarak teknik ve düzenlemeye ilişkin tedbirlerin etkililiğinin düzenli olarak sınanması, ölçülmesi ve değerlendirilmesine ilişkin süreç,[394] gibi tedbirler veri işlemenin güvenliğinin sağlanması amacıyla uygulanabilecektir. Ayrıca, veri güvenliğinin sağlanması için alınacak en genel tedbirin, kişisel verilerin sadece gerçekten gerekli olduğu durumlarda ve gerekli olduğu ölçüde kullanılması olduğu unutulmamalıdır.[395]

Belirtilmelidir ki, veri güvenliğinin sağlanabilmesi için doğru teçhizata –donanım ve yazılım– sahip olunması yeterli değildir. Bu amacın gerçekleştirilmesi için dahili organizasyonel kurallara yer verilmesi gerekir. Bu kurallar, örneğin, çalışanlara veri güvenliği hakkında bilgi verilmesini ve veri koruma hukuku kapsamındaki sorumluluklarının anlatılmasını, kişisel verilerin kullanımının yalnızca yetkili kişinin talimatlarına veya genel kurallara uygun olarak gerçekleştirilmesini, kişisel verilerin işlenmesi ile ilgili yetki sınırlarını ve sorumlulukları net olarak belirlemeyi içerebilir.[396]

Ayrıca, Tüzük, veri işlemenin güvenliği için, bir kişisel veri ihlali olması durumunda, kişisel veri ihlalinin gerçek kişilerin hakları ve özgürlükleri açısından bir riske sebebiyet vermesinin muhtemel olması halinde, veri sorumlusuna ihlali denetim makamına bildirme yükümlülüğü getirmiştir.[397]

Bir veri sorumlusunun veya işleyenin veri güvenliğini geliştirmesi için alabileceği önlemler arasında kişisel veri koruma görevlilerinin atanması, çalışanların veri güvenliği hakkında eğitilmesi, düzenli olarak denetleme, sızma ve kalite testlerinin yapılması sayılabilir.[398]

B. Gizlilik

Tüzükte gizlilik genel bir prensip olarak kabul edilmiştir.[399] Tüzüğün 5. maddesinin 1. fıkrasının (f) bendi, kişisel verilerin *"yetkisiz veya yasa dışı işlemeye karşı ve kazara kayba, imhaya veya tahribe karşı koruma da dahil olmak üzere teknik veya düzenlemeye ilişkin uygun tedbirlerin*

394 GDPR, m. 32(1).
395 **Dülger**, s. 177.
396 **Giakoumopoulos/Buttarelli/O'Flaherty**, s. 165.
397 GDPR, m. 33.
398 **Giakoumopoulos/Buttarelli/O'Flaherty**, s. 168.
399 **Giakoumopoulos/Buttarelli/O'Flaherty**, s. 169.

kullanılması suretiyle kişisel verilerin güvenliğini sağlayan bir şekilde işlenmesi gerektiği" ilkesini, *"bütünlük ve gizlilik"* adı altında düzenlemiştir. Ayrıca 32. maddede, yukarıda belirtildiği üzere, yüksek seviyede veri güvenliğinin sağlanması için veri sorumlusu ve işleyenin uygun teknik ve düzenlemeye ilişkin tedbirler alması gerektiği hüküm altına alınmıştır; bu kapsamda kişisel verilerde takma ad kullanımı ve şifreleme, işleme sistemleri ve hizmetlerinin gizliliği, bütünlüğü, elverişliliği ve esnekliğinin sürekli olarak sağlanabilmesi gibi önlemler örnek olarak gösterilmiştir. Bunun yanında, 28. maddede veri sorumlusu ile veri işleyen arasında veri işlemeye ilişkin detayların bir sözleşme veya diğer bir hukuki tasarruf ile düzenlemesi gerektiği ve bu sözleşme veya diğer hukuki tasarrufta, veri işleyenin, kişisel verileri işleme yetkisi bulunan kişilerin gizlilik taahhüdünde bulunmasını veya uygun bir yasal gizlilik yükümlülüğü altında bulunmasını sağlaması gerektiği belirtilmiştir.

Gizlilik yükümlülüğü, kişisel veriye ilişkin bilginin, yalnızca bir bireyin kendi özel durumu sebebiyle o kişi tarafından bilinmesi durumlarında gündeme gelmez. Böyle hallerde, yukarıda bahsedilen 28. ve 32. maddeler dikkate alınmaz. Çünkü, bu kişiler tarafından kişisel verilerin kullanılması Tüzüğün uygulama alanı içerisinde değildir.[400] Tüzüğün 2. maddesinin 2. fıkrasının (c) bendinde bu Tüzüğün *"tamamen kişisel veya ev faaliyeti esnasında bir gerçek kişi tarafından kişisel verilerin işlenmesine uygulanmayacağı"* açıkça belirtilmiştir. Bu noktada dikkat edilmesi gereken husus ise, ABAD'ın *Bodil Lindqvist*[401] davasında, bu istisnanın dar yorumlanması gerektiğini ifade ettiğidir.[402]

Gizlilik yükümlüğünün bir diğer görünüşü ise *"haberleşmenin gizliliği"*dir ve bu yükümlülük E-Gizlilik Direktifi'ne tabidir. Bu direktifin elektronik haberleşmelerin gizliliğini sağlamaya ilişkin kuralları, Üye Devletlerin, haberleşmenin ve ilgili üst verilerin bunları kullanan kişiler tarafından veya kullanan kişilerin onayı ile gerçekleştirilenler dışında denetlenmesi veya dinlenmesinin önüne geçilmesini sağlaması gerektiğini düzenlemektedir.[403] E-Gizlilik Direktifi'nde ayrıca; ülkelerin ulusal hukuklarındaki düzenlemeler ile ulusal güvenlik, savunma, suçun önlenmesi ve tespiti amaçlarıyla ve yalnızca bu amaçlar için gerekli ve ölçülü ise, bu ilkeye istisna getirebileceği ifade edilmiştir.[404]

400 **Giakoumopoulos/Buttarelli/O'Flaherty**, s. 170.
401 ABAD, C-101/01, Criminal proceedings against Bodil Lindqvist, 6 Kasım 2003.
402 **Giakoumopoulos/Buttarelli/O'Flaherty**, s. 170.
403 E-Gizlilik Direktifi, m. 5(1); **Giakoumopoulos/Buttarelli/O'Flaherty**, s. 171.
404 E-Gizlilik Direktifi, m. 15(1); **Giakoumopoulos/Buttarelli/O'Flaherty**, s. 171.

C. Kişisel Veri İhlali Bildirimi

Kişisel verilerin güvenliğinin ihlali halinde, ihlal, ilgili kişi için teşkil ettiği risk göz önünde bulundurularak, denetim makamına ve ilgili kişiye bildirilmelidir.[405] Bu kapsamda, kişisel veri ihlali; iletilen, saklanan veya işlenen kişisel verilerin kazara veya yasa dışı yollarla imha edilmesi, kaybı, değiştirilmesi, yetkisiz şekilde açıklanması veya bunlara erişime yol açan bir güvenlik ihlalidir.[406] Veri ihlalleri bireylerin gizlilik ve veri koruma hakları üzerinde çok tehlikeli sonuçlar doğurabilir. Çünkü veri ihlali, veri sahibinin verisi üzerindeki kontrolünü kaybetmesi anlamına gelmektedir.[407] Bu bağlamda, Madde 29 Çalışma Grubu, ihlallerin kişisel veri üzerine üç etkisi olabileceğini ifade etmiştir: İfşa, kayıp ve/veya değişiklik.[408]

Tüzüğün lafzına dikkat edildiğinde, kişisel veri ihlalinden bahsedebilmek için kastın veya ihmalin varlığı önemli değildir, ihlalin nasıl ve neden gerçekleştiğinin bu açıdan bir önemi yoktur.[409] Bildirim yükümlülüğü ise her ihlalde doğmayacaktır.[410]

Tüzük uyarınca, bir kişisel veri ihlali olması durumunda, kişisel veri ihlalinin gerçek kişilerin hakları ve özgürlükleri açısından bir riske sebebiyet vermesinin muhtemel olmaması haricinde, veri sorumlusu, gereksiz gecikmeye mahal vermeden ve uygun olması halinde, ihlalden haberdar olduktan itibaren *en geç 72 saat içerisinde*, kişisel veri ihlalini yetkili denetim makamına bildirmelidir. Gecikme halinde, yapılan bildirimde gecikmenin sebeplerine de yer verilmelidir.[411] Tüzüğün ilgili düzenlemesinden anlaşılacağı üzere, bildirim yükümlülüğü yalnızca veri ihlalinin gerçek kişilerin hakları ve özgürlükleri açısından bir riske sebebiyet vermesinin muhtemel olduğu durumlarda söz konusu olacaktır.

Denetim makamlarına yapılacak kişisel veri ihlali bildiriminin, en azından, ilgili veri sahibi kategorileri ve yaklaşık sayısı ile ilgili kişisel veri kaydı kategorileri ve yaklaşık sayısı da dahil olmak üzere kişisel veri ihlalinin mahiyetini; veri koruma görevlisi veya daha fazla bilginin elde edilebileceği başka bir temas noktasının isim ve irtibat bilgilerini; kişisel veri ihlalinin olası sonuçlarını; kişisel veri ihlalinin olası olumsuz etkilerini azaltmak için alınanlar da dahil olmak

405 **Develioğlu**, s. 108.
406 GDPR, m. 4(12).
407 **Giakoumopoulos/Buttarelli/O'Flaherty**, s. 172.
408 Article 29 Working Party (2017), Guidelines on Personal data breach notification under Regulation 2016/679, WP250, 3 Ekim 2017, s. 6.
409 **Voigt/von dem Bussche**, s. 68.
410 **Voigt/von dem Bussche**, s. 68.
411 GDPR, m. 33(1).

üzere, kişisel veri ihlalinin ele alınması için veri sorumlusu tarafından alınan veya alınması önerilen tedbirleri içermesi gerekir.[412]

Tüzüğün veri ihlali bildirimine ilişkin düzenlemesi belirli yönlerden 108 No'lu Sözleşme ve 6698 sayılı KVKK'dan farklılık gösterir. 108 No'lu Sözleşme'ye göre veri sorumlularını, veri ihlalinin gerçek kişilerin hakları ve özgürlükleri açısından bir riske sebebiyet vermesinin muhtemel olduğu durumlarda ihlali *"gecikmeksizin"* yetkili denetim makamına bildirmelidir.[413] Ayrıca, 6698 sayılı KVKK'da işlenen kişisel verilerin kanuni olmayan yollarla başkaları tarafından elde edilmesi hâlinde, veri sorumlusunun bu durumu *"en kısa sürede"* ilgilisine ve Kurula bildirmesi gerektiği düzenlenmiştir.[414] Burada değinilmesi gereken diğer bir nokta ise, kanunun kişisel veri ihlalini kişisel verilerin "kanuni olmayan yollarla başkaları tarafından elde edilmesi" olarak tanımlamış olmasıdır. Dolayısıyla, Tüzüğün getirdiği düzenlemenin daha kapsamlı ve detaylı olduğunu söylemek mümkündür.

Tüzükte, veri ihlali bildiriminin denetim makamına *"en geç 72 saat içinde"* yapılması öngörülmüşken, gerçek kişilerin hakları ve özgürlükleri açısından yüksek bir riske sebebiyet vermesi muhtemel olan veri ihlallerini, veri sorumlusu, veri sahibine *"gereksiz bir gecikmeye mahal vermeden"* iletmelidir.[415] Bu bildirimde kişisel veri ihlalinin mahiyeti açık ve sade bir dille açıklanmalıdır;[416] ayrıca bu bildiriminde, denetim makamına yapılan bildirimdekilere benzer bilgilere yer verilmelidir.[417] Bazı durumlarda ise veri sorumlusunun veri sahibine bildirim yapma zorunluluğu yoktur. Örneğin; veri sorumlusu uygun teknik ve düzenlemeye ilişkin koruma tedbirleri almış ve bu tedbirleri kişisel veri ihlalinden etkilenen kişisel verilere uygulamış ise bildirim yükümlülüğü altında değildir.[418] Veri sorumlusunun ihlalden sonra söz konusu yüksek riskin gerçekleşme ihtimalinin azalması için önlem almış olması durumunda da bildirim gerekmeyecektir.[419] Son olarak, eğer bildirim ölçüsüz bir çaba gerektirecekse, veri sorumlusundan bu bildirimi gerçekleştirmesi beklenemez; böyle bir durumda, veri sahibi ihlal hakkında başka yollarla bilgilendirilebilir, örneğin; kamuya yönelik bir bildirim ile.[420]

412 GDPR, m. 33(3).
413 Convention 108, m. 7(2).
414 6698 Sayılı Kişisel Verilerin Korunması Kanunu, m. 12(5).
415 GDPR, m. 34(1).
416 GDPR, m. 34(2).
417 **Giakoumopoulos/Buttarelli/O'Flaherty**, s. 173.
418 GDPR, m. 34(3)(a).
419 GDPR, m. 34(3)(b).
420 GDPR, m. 34(3)(c).

Denetim makamını ve veri sahibini kişisel veri ihlalleri hakkında bilgilendirme yükümlülüğü esasen veri sorumlularına ilişkin olarak düzenlenmiştir. Fakat bildirime konu olacak ihlaller, veri işleyen nezdinde de gerçekleşebilir.[421] Bu nedenle, veri işleyen, bir kişisel veri ihlalinden haberdar olduktan sonra, "herhangi bir gecikmeye mahal vermeden" veri sorumlusuna bildirimde bulunmalıdır.[422]

IV. Hesap Verebilirlik ve Uyum Sağlanmasına İlişkin Kurallar

Hesap verebilirlik prensibi, veri korumasına ilişkin kuralların etkili bir şekilde uygulanması için oldukça önemlidir. Bu bağlamda, veri sorumlusu, veri koruma kurallarına uyumlu hareket ettiğini göstermek zorundadır, dolayısıyla bunu gösterebilecek durumda olmalıdır. Ayrıca, hesap verebilirliğin yalnızca ihlal gerçekleştikten sonra ortaya çıktığı düşünülmemelidir. Veri sorumlularının, veri işlemenin her aşamasında, verilerin korunmasına uygun ve elverişli bir veri işleme politikası uyarınca faaliyet göstermesi gerekir. Tüzük, veri sorumlularının, veri işlemeyi kurallar ile uyumlu bir şekilde gerçekleştirdiklerini gösterebilmeleri ve gösterecek durumda olmaları için uygun teknik ve düzenlemeye ilişkin önlemler almaları gerektiğini belirtmektedir.[423]

A. Veri Koruma Görevlileri

Tüzükte, belirli durumlarda, veri sorumlularının veri koruma kurallarına uygun faaliyet göstermesi hususunda onlara bilgi ve tavsiye verecek "veri koruma görevlileri" atanmasını öngörmüştür. Veri koruma görevlileri, ayrıca, denetim makamları, veri sahipleri ve atandıkları kuruluş arasında bir aracı görevi görür.[424]

Veri koruma görevlisi atamak, 108 No'lu Sözleşme uyarınca veri koruma kurallarına uyumluluğu göstermek için tercih edilebilecek yöntemlerden biri olarak değerlendirilmekteydi. Tüzükte ise, bu durumun aksine, veri koruma görevlisinin atanması her zaman veri sorumları ve işleyenlerinin takdirinde olmayıp, bazı durumlarda zorunludur.[425] Tüzükte (i) işleme faaliyetinin bir kamu kuruluşu veya organı tarafından gerçekleştirilmesi, (ii) veri sorumlusu veya işleyenin temel faaliyetlerinin yapıları, kapsamları ve/veya amaçları gereği veri sahiplerinin düzenli ve sistematik bir şekilde büyük çaplı olarak izlenmesini gerektiren işleme faaliyetlerinden meydana gelmesi veya (iii) veri sorumlusu veya işleyenin temel faaliyetlerinin özel kategorilerdeki verilerin veya mahkumiyet kararları ve ceza gerektiren suçlara ilişkin kişisel verilerin büyük çaplı olarak

421 **Giakoumopoulos/Buttarelli/O'Flaherty**, s. 173.
422 GDPR, m. 33(2).
423 **Giakoumopoulos/Buttarelli/O'Flaherty**, s. 174.
424 **Giakoumopoulos/Buttarelli/O'Flaherty**, s. 175.
425 **Giakoumopoulos/Buttarelli/O'Flaherty**, s. 175.

işlenmesinden meydana gelmesi durumunda bir veri koruma görevlisi belirlenmesinin zorunlu olduğu düzenlenmiştir.[426] Bu düzenlemede kullanılan "sistematik bir şekilde büyük çaplı olarak izlemek" ve "temel faaliyetler" gibi terimler Tüzükte tanımlanmamış olsa da, Madde 29 Çalışma Grubu bunların nasıl yorumlanması gerektiği ile alakalı kılavuzlar yayınlamıştır.[427] Örneğin; bir hastane ve bir sağlık sigortası şirketi, faaliyetlerinin çoğu özel kategorilerdeki kişisel verilerin büyük çaplı olarak işlenmesinden oluşan veri sorumlularıdır.[428]

Tüzükte, veri koruma görevlisinin belirlenmesinin zorunlu olduğu yukarıdaki açıklanan durumlar haricinde de veri sorumlusu veya işleyenin ya da birlikler ve veri sorumlusu veya işleyeni temsil eden diğer organların bir veri koruma görevlisi belirleyebileceği düzenlenmiştir. Ayrıca, Birlik veya Üye Devlet hukuklarında, sayılan durumlar dışında başka kuruluşlar içinde veri koruma görevlisi atama zorunluluğu getirilebilir ve bu hallerde, bu kişi, birlik veya organların bir veri koruma görevlisi belirlemesi gerekmektedir.[429]

Bir veri koruma görevlisi atandığına, veri sorumlusu ve işleyen, bu kişinin kişisel verilerin korunmasına ilişkin tüm konulara uygun bir şekilde ve zamanında müdahil olmasını sağlar.[430] Örneğin; veri koruma görevlisi, veri koruma etki değerlendirmesi yapılmasına ilişkin tavsiye verilmesine dahil olmalıdır.[431] Veri koruma görevlisinin görevlerini efektif bir şekilde yerine getirebilmesi için, veri sorumluları ve veri işleyenler, ona gereken kaynakları sağlamalıdır.[432] Örneğin; görevlerinin yerine getirilmesi ile ilgili olarak veri koruma görevlilerine maddi kaynak, altyapı ve teçhizatlar sağlanmalı, veri koruma görevlileri uzmanlıklarını geliştirebilmeleri ve güncel kalabilmeleri için sürekli eğitime tabii tutulmalıdır.[433]

İlaveten, Tüzükte, veri koruma görevlilerinin bağımsız bir şekilde hareket edebilmelerinin sağlanması için bazı teminatlar düzenlenmiştir. Bu bağlamda, veri sorumlusu ve işleyen, veri koruma görevlisinin görevlerini yerine getirmesi ile ilgili olarak hiçbir talimat almamasını sağlar. Ayrıca, veri koruma görevlisi, görevlerinin yerine getirilmesi nedeniyle veri sorumlusu ya da işleyen tarafından işten çıkarılamaz veya cezalandırılamaz.[434]

---

426 GDPR, m. 37(1).
427 Article 29 Working Party (2017), Guidelines on Data Protection Officers (DPOs), WP 243 rev.01, last revised and adopted 5 April 2017.
428 **Giakoumopoulos/Buttarelli/O'Flaherty**, s. 175, 176.
429 GDPR, m. 37(4).
430 GDPR, m. 38(1).
431 **Giakoumopoulos/Buttarelli/O'Flaherty**, s. 175, 176.
432 GDPR, m. 38(2).
433 **Giakoumopoulos/Buttarelli/O'Flaherty**, s. 177.
434 GDPR, m. 38(3).

Veri koruma görevlisinin görevleri, en azından; veri sorumluları ve işleyenler ile işleme faaliyetleri gerçekleştiren çalışanların veri koruma hükümleri uyarınca yükümlülükleri hususunda bilgilendirilmesi ve onlara tavsiyede bulunulmasını, işleme faaliyetlerine müdahil personelin bilinçlendirilmesi ve eğitimi ve ilgili denetimler de dahil olmak üzere veri sorumlusu ve işleyenin kişisel verilerin korunmasına ilişkin politikalarına uyumluluğun izlenmesini, talep üzerine veri koruma etki değerlendirmesine ilişkin tavsiyede bulunulmasını, denetim makamıyla işbirliği yapılmasını, ön istişare de dahil olmak üzere işleme faaliyetine ilişkin konularda denetim makamına yönelik bir temas noktası olarak hareket edilmesini ve, uygun olduğu hallerde, diğer her türlü konu ile ilgili olarak danışmanlık verilmesini içerir.[435]

AB kuruluş ve organlarının elinde bulunan kişisel verilere ilişkin 45/2001 sayılı Direktif, her Birlik kuruluş ve organının veri güvenlik görevlisi ataması gerektiğini düzenlemiştir.[436] Veri koruma görevlisi, bu kapsamda, bu direktifin hükümlerinin AB kuruluş ve organlarında doğru bir şekilde uygulandığını ve veri sahipleri ile veri sorumlularının hak ve yükümlülükleri hakkında bilgilendirilmiş olduğunu garantiye almak ile görevlendirilmiştir.[437] Tüzük ile aynı doğrultuda, 45/2001 sayılı Direktif de, veri koruma görevlilerinin görevlerini yerine getirirken bağımsız olması ve bu kişilere görevleri için gerekli eleman ve kaynakların sağlanması gerektiğini belirtmiştir.[438]

GDPR ile kabul edilen önemli yeniliklerden birisi de belirli ölçekteki veri sorumlusu/işleyen şirketlerin, kişisel verilerin korunması konularına müdahil olabilecek (GDPR, m. 38/1), veri koruma mevzuatı ve uygulaması konusunda uzman olan (GDPR, rec. 97) bir kişiyi veri koruma görevlisi olarak bulundurmakla yükümlü kılmasıdır. Veri koruma görevlisi, denetim makamları ile veri sahipleri ve veri sorumlusu/işleyen arasında bağlantıyı sağlar ve GDPR uyumluluğunu sağlamayı kolaylaştırdığı için de veri sorumlusu/işleyen şirketlerin sorumluluğunda köşe taşı olarak kabul edilir.[439] Veri sorumlusu/işleyen şirketler veri koruma görevlisine gereken kaynakları sağlamalıdır. Veri koruma görevlisi, veri işleme ile uğraşan kişi/grup/organizasyonlar için önemli bir destekçi/katkı sağlayıcı olarak görülmelidir. Veri koruma görevlisinin görevleri şu şekilde belirlenmiştir (GDPR; m. 39/1):

435 GDPR, m. 39(1).
436 **Giakoumopoulos/Buttarelli/O'Flaherty**, s. 177.
437 Veri koruma görevlilerinin tüm görevleri için bknz. Regulation (EC) No. 45/2001.
438 **Giakoumopoulos/Buttarelli/O'Flaherty**, s. 177.
439 Handbook on European Data Protection Law, s. 175.

- Veri sorumlusu/işleyen ile işleme faaliyetleri gerçekleştiren çalışanların GDPR ve diğer ulusal veri koruma mevzuatı uyarınca yükümlülükler hususunda bilgilendirilmeleri ve onlara tavsiyede bulunulması,

- İşleme faaliyetlerine müdahil personelin bilinçlendirilmesi ve eğitimi ile ilgili denetimler dahil olmak üzere veri sorumlusu/işleyenin kişisel verilerinin korunmasına ilişkin politikalarına uyumluluğun izlenmesi,

- Talep üzerine veri koruma etki değerlendirmesine ilişkin tavsiyede bulunmak,

- Denetim makamıyla iş birliği yapmak

- İşleme faaliyetine ilişkin konularda (ön istişare dahil) denetim makamına yönelik bir temas noktası olmak ve uygun olan durumlarda konuya ilişkin danışılması.

Veri koruma görevlisi, işleme faaliyetinin niteliği, kapsamı, bağlamı ve amaçları ile işleme faaliyetlerinin risklerini göz önünde bulundurarak görevlerini yerine getirmelidir (GDPR, m. 39/2). Veri koruma görevlisi, veri sorumlusu/işleyenin bir çalışanı olabilir ve hizmet sözleşmesine dayalı olarak görevini yerine getirebilir (GDPR, m. 37/6). Veri sorumlusu, veri koruma görevlisinin irtibat bilgilerini yayımlamak ve denetim makamına iletmekle yükümlüdür (GDPR, m. 37/7).

B. Faaliyetlerin Kaydı

Veri işleme kurallarına uyumlu hareket edildiğinin gösterilebilmesi ve dolayısıyla veri işleme faaliyetlerinden sorumlu tutulabilmek için, genellikle, kişilerin aktivitelerini belgelendirmesi ve kaydetmesi gereklidir.[440] Ayrıca, işletme faaliyetlerinin kaydedilmesi, denetim makamlarının veri işlemenin hukuka uygunluğunu denetlemesine de olanak tanır.[441] Tüzükte, her veri sorumlusunun ve, uygun olduğu hallerde, veri sorumlusunun temsilcisinin kendi sorumluluğu altındaki işleme faaliyetlerine ilişkin bir kayıt tutması gerektiği hüküm altına alınmıştır.[442] Mevzubahis bu kayıt, aşağıdaki bilgilerin tamamını içermelidir:

(a) Veri sorumlusu ve uygun olduğu hallerde, ortak veri sorumlusu, veri sorumlusunun temsilcisi ve veri koruma görevlisinin isim ve irtibat bilgileri;

(b) İşleme amaçları;

(c) İşleme ile ilgili veri sahibi kategorileri ve kişisel veri kategorileriyle ilgili bir açıklama;

(d) Üçüncü ülkeler veya uluslararası kuruluşlardaki alıcılar da dahil olmak üzere, kişisel verilerin açıklandığı veya açıklanacağı alıcı kategorileri;

---

440 **Giakoumopoulos/Buttarelli/O'Flaherty**, s. 178.
441 GDPR, m. 30(5); **Giakoumopoulos/Buttarelli/O'Flaherty**, s. 179.
442 GDPR, m. 30(1).

(e) Uygun olduğu hallerde, uygun güvencelere ilişkin belgelendirme de dahil olmak üzere, üçüncü ülke veya uluslararası kuruluşa yönelik kişisel veri aktarımları;

(f) Mümkün olması halinde, farklı kategorilerdeki verilerin silinmesiyle ilgili öngörülen süre sınırları;

(g) Mümkün olması halinde, teknik ve düzenlemeye ilişkin güvenlik tedbirlerine yönelik genel bir açıklama.[443]

Veri sorumluları haricinde, Tüzükte ayrıca veri işleyenlerin ve uygun olduğu hallerde, işleyenin temsilcilerinin de bir veri sorumlusu adına gerçekleştirilen tüm kategorilerdeki işleme faaliyetlerine ilişkin olarak kayıt tutma yükümlülüğü olduğu öngörülmüştür.[444] Tüzüğün kabul edilmesinden önce, veri sorumlusu ve veri işleyen arasındaki sözleşmede yalnızca veri sorumlusunun yükümlülükleri düzenlendiğinden, açık olarak veri işleyenlere faaliyetlerinin kaydını tutma yükümlülüğü getirilmesi büyük bir gelişme olarak değerlendirilmektedir.[445]

Ek olarak, Tüzük, işletme faaliyetlerinin kaydedilmesi yükümlülüğüne bir istisna getirmiştir. Buna göre, 250'den az kişi istihdam eden bir işletme veya kuruluş için veri sorumlusu veya veri işleyen için böyle bir yükümlülük doğmayacaktır. Fakat, işletme faaliyetlerinin kaydedilmesi yükümlülüğünden muafiyet için ayrıca veri sorumlusu veya işleyenin gerçekleştirdiği işleme faaliyetlerinin veri sahiplerinin hakları ve özgürlükleri açısından bir riske sebebiyet vermesinin muhtemel olmaması, işleme faaliyetinin nadiren gerçekleştirilmesi veya işleme faaliyetinin özel nitelikli verileri ya da mahkûmiyet kararları ve ceza gerektiren suçlara ilişkin kişisel verileri kapsamaması gerekir.[446]

C. Veri Koruma Etki Değerlendirmesi ve Ön İstişare

Veri işleme faaliyetleri, işlemenin doğasına ve kapsamına bağlı olarak değişen seviyelerde bazı riskleri içlerinde barındırırlar. Bu çerçevede, veri sorumluları, veri işleme faaliyetlerine başlamadan önce, planlanan işlemenin risklerinin bireylerin hakları açısından doğurabileceği sonuçları incelemeli ve değerlendirmelidir. Bu değerlendirme, veri sorumlularının muhtemel riskleri önceden belirlemesi, ele alması ve hafifletmesine; dolayısıyla veri işleme sonucu mevzubahis risklerin bireylerin hakları üzerindeki negatif etkisinin sınırlanmasına olanak

443 GDPR, m. 30(1).
444 GDPR, m. 30(2).
445 **Giakoumopoulos/Buttarelli/O'Flaherty**, s. 179.
446 GDPR, m. 30(5); **Giakoumopoulos/Buttarelli/O'Flaherty**, s. 179.

sağlayacaktır.[447] Bu kapsamda veri koruma etki değerlendirmesi *önleyici* bir veri koruma aracıdır.[448]

Tüzükte, bir veri işlemenin gerçek kişilerin hakları ve özgürlükleri açısından yüksek bir riske sebebiyet vermesinin muhtemel olduğu hallerde, veri sorumlusuna, işleme faaliyetinden önce, bu işleme faaliyetinin kişisel verilerin korunmasına olan etkisine ilişkin bir değerlendirme yapması yükümlülüğü getirilmiştir.[449] Tüzük, ayrıca, yüksek risk teşkil eden ve dolayısıyla veri koruma etki değerlendirmesine en çok gerek görülen işleme faaliyetlerini de belirtmiştir. Buna göre, veri işlemenin (i) gerçek kişilerle ilgili kişisel özellikler hususunda, profil çıkarma da dahil olmak üzere, otomatik işlemeye dayalı olan ve gerçek kişi ile ilgili hukuki sonuçlar doğuran veya gerçek kişiyi kayda değer şekilde etkileyen kararların dayandığı sistematik ve kapsamlı bir değerlendirmeyi; (ii) özel nitelikli kişisel verilerin veya mahkumiyet kararları ve ceza gerektiren suçlara ilişkin kişisel verilerin büyük çaplı olarak işlenmesini veya (iii) kamunun erişebileceği bir alanın büyük çaplı olarak sistematik bir şekilde izlenmesini içermesi hallerinde, bu veri işlemenin yüksek risk taşıdığı ve veri koruma etki değerlendirmesinin gerekli olduğu kabul edilmiştir.[450]

Veri koruma etki değerlendirmesi yükümlülüğü ile ilgili olarak, denetim makamı, bu yükümlülüğe tabi olan ve bu yükümlülükten muaf olan işleme faaliyeti türlerine ilişkin birer liste oluşturmalı ve bu listeleri kamuya açıklamalıdır.[451]

Veri koruma etki değerlendirmesinin yapılması gereken hallerde, veri sorumluları, veri işlemenin amaçlarını, gerekliliği ve ölçülülüğünü, ayrıca bireylerin haklarına ilişkin oluşturduğu muhtemel riskleri değerlendirmelidir.[452] Söz konusu etki değerlendirmesinde ayrıca kişisel verilerin korunmasının sağlanması ve Tüzüğe uygun hareket edildiğinin gösterilmesiyle ilgili güvenceler, güvenlik tedbirleri ve mekanizmalar da dahil olmak üzere risklerin ele alınması hususunda öngörülen tedbirler de yer almalıdır.[453]

Madde 29 Çalışma Grubu, veri koruma etki değerlendirmeleri ve bir işlemenin yüksek risk doğurup doğurmayacağının belirlenmesi ile ilgili esaslar düzenlemiştir. Bu doğrultuda, bir işleme bazında veri koruma etki değerlendirmesinin gerekli olup olmadığının tespiti için dokuz kriter geliştirmiştir; bu çerçevede bakılması gereken, veri işleme faaliyetinin şunları içerip içermediğidir:

447 **Giakoumopoulos/Buttarelli/O'Flaherty**, s. 179.
448 **Voigt/von dem Bussche**, s. 47.
449 GDPR, m. 35(1).
450 GDPR, m. 35(3).
451 GDPR, m. 35(4), 35(5).
452 **Giakoumopoulos/Buttarelli/O'Flaherty**, s. 180; GDPR, m. 35(7)(a)-35(7)(c).
453 GDPR, m. 35(7)(d).

(1) Değerlendirme ve notlandırma,

(2) Hukuki veya başka önemli sonucu olan otomatik karar verme,

(3) Sistematik izleme,

(4) Özel nitelikli veriler,

(5) Geniş kapsamlı veri işleme,

(6) Eşlenmiş veya birleştirilmiş veri kümeleri,

(7) Hassas veri sahiplerine ilişkin veriler,

(8) Yenilikçi kullanım veya teknolojik veya organizasyonel çözümlerin uygulanması,

(9) Veri işlemenin kendisinin veri sahiplerinin bir hakkını kullanmasını veya bir sözleşmeden veya hizmetten yararlanmasını engellemesi.[454]

Madde 29 Çalışma Grubu, sayılan dokuz halden yalnız ikisinden azının varlığı durumunda, veri işleme faaliyetinin yüksek risk teşkil etmeyeceğini, dolayısıyla veri koruma etki değerlendirmesi yapılmasına gerek olmadığını ifade etmiştir.[455] Ayrıca, Madde 29 Çalışma Grubu, veri koruma etki değerlendirmesi yapılmasının gerekliğinden emin olunamayan durumlarda, veri sorumlularının veri koruma kuralları ile uyumu hususunda katkı sağlaması sebebiyle, bu değerlendirmenin gerçekleştirilmesini tavsiye etmektedir.[456] Son olarak, Madde 29 Çalışma Grubu, yeni bir veri işleme teknolojisinin tanıtılması halinde, veri koruma etki değerlendirilmesi yapılmasını önemli görmektedir.[457]

Veri koruma etki değerlendirmesi sonucunda, veri sorumlusunun riski hafifletmek için tedbir almaması durumunda veri işlemenin bireylerin hakları için yüksek risk teşkil edeceği anlaşılırsa, veri sorumlusu işleme faaliyetinden önce denetim makamına danışmalıdır.[458]

Veri sorumlusu şirketler, daha GDPR yürürlüğe girmeden önce GDPR uyumluluğu için gerekli hazırlıkları yapmaya başlamışlardır. Bu kapsamda, veri sorumlusu öncelikle teknolojinin mevcut durumu, uygulama maliyeti, işleme faaliyetinin niteliği, kapsamı, bağlamı ve amaçlarının yanı sıra işleme faaliyetinin gerçek kişilerin hak ve özgürlükleri bakımından içerdiği riskleri

---

454 Article 29 Working Party (2017), Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in high risk" for the purposes of Regulation 2016/679, WP 248 rev.01, Brussels, 4 Ekim 2017.

455 **Giakoumopoulos/Buttarelli/O'Flaherty**, s. 181.

456 Article 29 Working Party (2017), Guidelines on Data Protection Impact Assessment (DPIA) andcdetermining whether processing is "likely to result in high risk" for the purposes of Regulation 2016/679, WP 248 rev.01, Brussels, 4 Ekim 2017, s. 9.

457 Article 29 Working Party (2017), Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in high risk" for the purposes of Regulation 2016/679, WP 248 rev.01, Brussels, 4 Ekim 2017, s. 9.

458 GDPR, m. 36

dikkate alarak hem verinin işleme yönteminin belirlenmesi hem de işleme faaliyeti sırasında, uygun teknik ve organizasyonel tedbirleri uygulamalı (takma ad kullanımı gibi), veri koruma prensiplerinin etkili bir şekilde uygulanmasını temin etmeli (asgari düzeyde veri işlenmesi ilkesi/data minimisation gibi) ve bu şekilde veri sahiplerinin haklarını koruma altına almalıdır (GDPR, m. 25/1).

Bu esaslar dahilinde kişisel verinin işlenmesinin, o kişinin hakları ve özgürlükleri açısından yüksek bir riske sebebiyet vermesi ihtimalinin bulunması halinde (likely to result high risk), veri sorumlusu, henüz verinin işlenmesinden önce, bu işleme faaliyetinin kişisel verilerin korunmasına etkisine ilişkin bir "veri koruma etki değerlendirmesi (data protection impact assesment-DPIA)" yapmakla yükümlüdür (GDPR, m. 35/1). Bu değerlendirme asgari olarak şu hususları içermelidir (GDPR, m. 35/7):

- Öngörülen işleme faaliyeti ve işleme amaçlarına ilişkin sistematik açıklama

-İşleme faaliyetinin amaç ile kıyasen gerekliliği ve orantılılığına ilişkin değerlendirme,

-Veri sahibinin hak ve özgürlüklerine ilişkin risklere yönelik değerlendirme,

- Veri sahibinin kişisel verilerinin korunmasına yönelik tedbirler ve mekanizmalar.

Dolayısıyla, veri sorumlusu şirket kişisel verilerin korunmasına ilişkin asgari şartları sağlamak ve gerektiğinde veri koruma etki değerlendirmesi yapmakla yükümlüdür. Veri işleyenleri de kendisinden talep edilmesi veya gerekli olan durumlarda, veri koruma etki değerlendirmesi konusunda veri sorumlusuna yardım etmekle yükümlü kılınmıştır (GDPR, rec. 95).

D. Davranış Kuralları (Codes of Conduct)

Tüzük, Üye Devletler, denetim makamları, Kurul ve Komisyon, çeşitli işleme sektörlerinin spesifik özellikleri ve mikro, küçük ve orta büyüklükteki işletmelerin spesifik ihtiyaçlarını dikkate alarak, Tüzüğün düzgün bir şekilde uygulanmasına katkıda bulunması amaçlanan davranış kurallarının hazırlanmasını teşvik etmesi için çağrıda bulunmuştur.[459] Bu çerçevede davranış kurallarının amacı, soyut ve teknik hukuk kurallarına, uygulamaya yönelik ve pratik bir yorum kazandırmaktır.[460] Bu nedenle, davranış kuralları, belirli bir sektör ile veya veri işleme faaliyetlerine ilişkin teknolojiler ile ilgili çözümler sağlamaya yöneliktir.[461]

459 GDPR, m. 40.
460 **Voigt/von dem Bussche**, s. 73.
461 **Voigt/von dem Bussche**, s. 73.

Davranış kuralları, Tüzüğün herhangi bir boyutuna ilişkin olarak hazırlanabilir. Tüzüğün 40. maddesinin 2. fıkrasında uygulanmasını belirlemek amacıyla davranış kuralları hazırlanabilecek hususlardan bazıları örnekleme yoluyla sayılmıştır. Bunlar:

(a) Adil ve şeffaf veri işleme,

(b) Veri sorumluları tarafından spesifik bağlamlarda gözetilen meşru menfaatler,

(c) Kişisel verilerin toplanması,

(d) Kişisel verilerde takma ad kullanımı,

(e) Kamuoyuna ve veri sahiplerine sağlanan bilgiler,

(f) Veri sahiplerinin haklarının kullanımı,

(g) Çocuklara sağlanan bilgiler ve çocukların korunması ve çocuklar üzerinde velayet hakkına sahip olanların rızasının alınma şekli,

(h) İşleme faaliyetinin güvenliğinin sağlanmasına yönelik tedbirler,

(i) Kişisel veri ihlallerinin denetim makamlarına ve veri sahiplerine bildirilmesi,

(j) Üçüncü ülkelere veya uluslararası kuruluşlara kişisel veri aktarılması veya

(k) veri sorumluları ve veri sahipleri arasında ihtilafların çözümüyle ilgili mahkeme dışı işlemler ve diğer uyuşmazlık çözüm usulleri.

Yine 40. maddenin 2. fıkrasında, davranış kurallarının veri koruma otoriteleri ve veri sorumlusu veya veri işleyen kategorilerini temsil eden diğer organlar tarafından hazırlanabileceği, değiştirilebileceği veya kapsamlarının genişletebileceği düzenlenmiştir. Bu kuruluşlar/organlar, davranış kurallarını hazırlarken menfaat sahiplerine danışmalı, fikir ve önerilerini dikkate almalıdır.[462]

Ayrıca, davranış kuralları, Tüzüğün maddi olarak yorumlanmasının dışında; bu kurallara uyumluluğun izlenmesi için, kuralların konusu ile ilgili uygun bir uzmanlık seviyesine sahip olan ve bu amaca yönelik olarak yetkin denetim makamı tarafından akredite edilen bir organın[463], söz konusu görevi gerçekleştirmesine olanak sağlayacak usul kurallarına da yer vermelidir.[464]

Davranış kuralları hazırlandıktan sonra ilgili kuruluş/organ, kurallar, değişiklik veya kapsam genişletmeye ilişkin taslağı yetkin denetim makamına ibraz eder. Denetim makamı bu taslağın Tüzük ile uyumlu olup olmadığı konusunda bir görüş sunar. Denetim makamı, yeterli güvenceleri sağladığını tespit etmesi durumunda söz konusu taslağı onaylar.[465]

462 GDPR, Gerekçe 99; **Voigt/von dem Bussche**, s. 73.
463 GDPR, m. 41(1).
464 **Voigt/von dem Bussche**, s. 74.
465 GDPR, m. 40(5).

Davranış kurallarının birden çok Üye Devletteki işleme faaliyetlerine ilişkin olmadığı hallerde denetim makamı tarafından onaylanması durumunda, yetkili denetim makamı bu kuralları tescil eder ve yayımlar.[466] Veri sorumluları, Tüzüğün belirli yönleri ile uyumlarını göstermek için tescil edilmiş ve yayınlanmış bu davranış kurallarına bağlı kalabilirler. Fakat, bir davranış kuralına bağlı kalarak uyumluluğun gösterilebilmesi yalnızca ilgili Üye Devletin denetim makamının mevzubahis davranış kurallarını tescil etmiş ve yayımlamış olması ihtimalinde mümkündür.[467]

Davranış kurallarının çeşitli Üye Devlerdeki işleme faaliyetlerine ilişkin olduğu durumlarda ise, yetkili ulusal denetim makamı öncelikle Kurul'un taslağa ilişkin görüşünü almalıdır.[468] Kurul'un taslağın Tüzük ile uyumlu olduğunu onaylaması durumunda, Kurul taslağı Komisyon'a ibraz eder.[469] Komisyon da taslağın Tüzük ile uyumluluğunu onaylarsa, Komisyon, uygulama tasarrufları yolu ile bu taslağın AB kapsamında genel geçerliliğe sahip olduğuna karar verir[470] ve genel geçerliliğe sahip olduğuna karar verilen onaylı kuralların uygun şekilde ilan edilmesini sağlar. [471]

Ek olarak, yukarıda belirtildiği üzere, davranış kurallarına uyumluluğun izlenmesi için, yetkili denetim makamı, kuralların konusu ile ilgili uygun bir uzmanlık seviyesine sahip olan *bağımsız* bir organ akredite edecektir.[472] Bu organ, veri sorumlusu ve işleyenin davranış kuralları ile uyumluluğunu izleyerek, bu kuralların ihlal edilmesi halinde, veri sorumlusu veya işleyenin kurallardan askıya alınması veya çıkarılması da dahil olmak üzere, uygun işlemleri gerçekleştirecektir.[473] Ayrıca bu organ böylesi işlemler ve bu işlemlerin gerçekleştirilme sebepleri hususunda yetkili denetim makamını bilgilendirmelidir.[474]

Akreditasyon için gerekli kriterler yetkili denetim makamları tarafından detaylıca belirlenecek olmakla birlikte,[475] Tüzüğün 41. maddesinin 2. fıkrası uyarınca ilgili organ, aşağıdaki özellikleri taşıması halinde, davranış, kurallarına uyumluluğun izlenmesi amacı ile akredite edilebilir:

(a) Kuralların konusuna ilişkin *bağımsızlık ve uzmanlığa* sahip olması,

466 GDPR, m. 40(6).
467 GDPR, m. 40(7).
468 **Voigt/von dem Bussche**, s. 74.
469 GDPR, m. 40(8).
470 GDPR, m. 40(9).
471 GDPR, m. 40(10).
472 GDPR, m. 41(1).
473 GDPR, m. 41(4).
474 GDPR, m. 41(4).
475 GDPR, m. 41(3).

(b) İlgili veri sorumlusu ve işleyenlerin davranış kurallarını uygulamaya, bu kişilerin bu kuralların hükümlerine uyumluluğunu izlemeye ve bu kuralların işleyişini düzenli olarak gözden geçirmeye elverişliliğin değerlendirmesini sağlayan usuller oluşturmuş olması,

(c) Kurallara veya kuralların bir veri sorumlusu veya işleyen tarafından uygulanmış olma veya uygulanma şekline ilişkin ihlallere yönelik şikâyetlerin ele alınması hususunda usuller ve yapıları oluşturmuş olması ve bu usuller ile yapıları veri sahipleri ile kamuoyuna şeffaf hale getirmiş olması ve

(d) Görev ve vazifelerinin bir çıkar çatışmasına neden olmaması.

Son olarak, akreditasyon koşullarının yerine getirilmemesi veya artık yerine getirilmemesi halinde veya organ tarafından gerçekleştirilen eylemlerin Tüzüğü ihlal ettiği hallerde, yetkin denetim makamı bu organın akreditasyonunu kaldırabilecektir.[476]

E. Belgelendirme

Veri koruma belgelendirme mekanizmaları, veri koruma mühürleri ve işaretleri (belgelendirme", veri sorumlusu ve işleyenlerin Tüzük ile uyumluluğunu göstermelerini sağlayabilecek diğer yöntemlerdir.[477] Bu kapsamda Tüzük; Üye Devletlerin, denetim makamlarının, Kurul ve Komisyonun, veri sorumlusu ve işleyeni belgelendirmeye teşvik etmesini istemiştir.[478] Belgelendirme mekanizmalarında mikro, küçük ve orta ölçekli işletmelerin spesifik ihtiyaçlarının dikkate alması gerekliliği açıkça düzenlenmiştir.[479] Ayrıca, Tüzükte belgelendirmenin gönüllülük esasına dayandığı ve şeffaf bir süreç vasıtasıyla sağlandığı ifade edilmiştir.[480]

Belgelendirme mekanizmaları, bir veri sorumlusu veya işleyenin Tüzük kapsamındaki veri koruma standartlarına uygun işleme faaliyeti gösterdiklerini kanıtlamaya olanak sağladığından, bu veri sorumlusu veya işleyene duyulan güveni artıracak ve bu kişilerin rekabet avantajını kuvvetlendirecektir.[481] Buna rağmen, sağlanan bir belgelendirmenin veri sorumlusu veya işleyenin Tüzüğe uyma sorumluluğunu azaltmayacağı ve bu yetkili denetim makamlarının görev ve yetkilerine halel getirmeyeceği unutulmamalıdır.[482]

476 GDPR, m. 41(5).
477 **Giakoumopoulos/Buttarelli/O'Flaherty**, s. 183.
478 GDPR, m. 42(1).
479 GDPR, m. 42(1).
480 GDPR, m. 42(3).
481 **Voigt/von dem Bussche**, s. 77.
482 GDPR, m. 42(4).

Tüzük, belgelendirmenin nasıl gerçekleştirileceğine ilişkin olarak detaylı kurallar içermemekte, yalnızca temel bilgiler vermektedir.[483] Buna göre, bir belgelendirme, yetkili denetim makamı veya belgelendirme organları tarafından sağlanabilir.[484] Söz konusu belgelendirme organlarının yetkili denetim makamı veya ulusal akreditasyon organı tarafından akredite edilmesi gereklidir.[485] Bu çerçevede, belgelendirme organlarının akredite edilebilmeleri için:

(a) Belgelendirme konusuna ilişkin *bağımsızlık ve uzmanlığa* sahip olmaları,

(b) Yetkili denetim makamı tarafından veya Kurul tarafından onaylanan kriterlere riayet etmeyi taahhüt etmiş olmaları,

(c) Veri koruma belgelendirmesi, mühürleri ve işaretlerinin verilmesi, düzenli aralıklarla gözden geçirilmesi ve geri çekilmesine ilişkin usuller oluşturmuş olmaları,

(d) Belgelendirme veya belgelendirmenin bir veri sorumlusu veya işleyen tarafından uygulanmış olma veya uygulanma sekline ilişkin ihlallere yönelik şikâyetlerin ele alınması hususunda usuller ve yapıları oluşturmuş olmaları ve bu usuller ile yapıları veri sahipleri ile kamuoyuna şeffaf hale getirmiş olmaları ve

(e) Görev ve vazifelerinin bir çıkar çatışmasına neden olmamaları gereklidir.[486]

Akreditasyon azami beş yıllık bir süre için verilebilir ve belgelendirme organının sayılan gereklilikleri yerine getirmesi koşuluyla, aynı koşullar altında, yenilenebilir.[487] Ayrıca, akreditasyon koşullarının yerine getirilmemesi veya artık yerine getirilmemesi halinde veya bir belgelendirme organı tarafından gerçekleştirilen eylemlerin Tüzüğü ihlal ettiği hallerde, yetkili denetim makamı veya ulusal akreditasyon organı ilgili belgelendirme organının akreditasyonunu kaldırabilecektir.[488]

Belgelendirme almak için veri sorumlusu veya işleyen, belgelendirme usulünün gerçekleştirilmesi için gerekli tüm bilgileri ve işleme faaliyetlerine erişimi, belgelendirme organına veya yetkili denetim makamına sunmalıdır.[489] Belgelendirme en çok üç sene için sağlanabilir ve veri sorumlusu veya işleyenin ilgili kriterlere uyumunun devam etmesi şartıyla yenilenebilir.[490]

483 **Voigt/von dem Bussche**, s. 77.
484 GDPR, m. 42(5).
485 GDPR, m. 43(1).
486 GDPR, m. 43(2).
487 GDPR, m. 43(4).
488 GDPR, m. 43(7).
489 GDPR, m. 42(6).
490 GDPR, m. 42(7).

V. Özel ve Olağan Veri Koruması

A. Özel Veri Koruması

Veri sorumlusu, veri koruma ilkelerinin etkili bir şekilde uygulanması ve Tüzüğün gerekliliklerinin yerine getirilmesine yönelik olarak gerekli güvencelerin entegre edilmesi amacı ile uygun teknik ve düzenlemeye ilişkin tedbirler alarak veri sahiplerinin haklarını korunmasını sağlamalıdır.[491] Bu tedbirler hem işleme yönteminin belirlenmesi esnasında hem de işleme faaliyeti esnasında uygulanmalıdır.[492] Ayrıca, ilgili tedbirlere karar verilmesi ve tedbirlerin uygulanması esnasında, veri sorumlusu, son teknolojiler, uygulama maliyeti ve işleme faaliyetinin mahiyeti, kapsamı, bağlamı ve amaçlarının yanı sıra işleme faaliyetinin gerçek kişilerin hakları ve özgürlükleri acısından teşkil ettiği çeşitli olasılıklar ve ciddiyetlere sahip riskleri de dikkate almalıdır. [493]

B. Olağan Veri Koruması

Veri sorumlusu, olağan durumlarda, yalnızca işleme amacı için gerekli olan kişisel verilerin işlenmesini sağlamaya yönelik uygun teknik ve düzenlemeye ilişkin tedbirler almalıdır.[494] Söz konusu yükümlülük toplanan kişisel veri miktarı, bunların işlenme derecesi, saklama süresi ve bunlara erişilebilirliğe uygulanır.[495] Örneğin, bu yükümlülük doğrultusunda alınan bir tedbir, bir işverenin bütün işçilerinin veri sahibinin kişisel verisine erişememesine olanak sağlamalıdır.[496]

d. Mahremiyet Artırıcı Teknolojilerin Benimsenmesi (Privacy by default / by design)

Yeni bilgi teknolojileri, karşılaştığımız mahremiyet ve veri koruma risklerini artırırken öte yandan bu riskleri bertaraf etmek için ortaya konulan yöntemleri de geliştirmektedir. Mahremiyet artırıcı teknolojiler (privacy enhancing technologies- PETs) adı verilen bu yöntemlerle, teknolojiyi kullanan bireylerin kişisel bilgilerinin gizli tutulması sağlayan araçlar çeşitlendirilir ve etkinleştirilir. Bunu yaparken de, araçların hukuka uygun olması ve teknolojik sistemlerin işlevselliğinin devam ettirilmesi amaçlanır. Bu kapsamda toplanan kişisel verileri asgari düzeye indirmek, anonimlik sağlamak için takma ad kullanımı veya anonim veri bilgileri kullanmak, kullanıcının bilinçli surette rızasının alınması gibi yöntemler tercih edilir.

---

491 GDPR, m. 25(1).
492 GDPR, m. 25(1).
493 GDPR, m. 25(1).
494 GDPR, m. 25(2).
495 GDPR, m. 25(2).
496 **Giakoumopoulos/Buttarelli/O'Flaherty**, s. 184.

GDPR'ın 25. maddesi mahremiyet artırıcı teknolojilerin iki yöntemi olan "Tasarımla Veri Koruması (Privay by Design)" ve "Olağan Veri Koruması (Privacy by Default-Varsayılan Ayarlarla Veri Koruması)" hususu düzenlemiştir. Buna göre tekniğin bilinen durumu, uygulama maliyeti ve verinin işleme mahiyeti, kapsamı ve amaçları ile riskler dikkate alınmak suretiyle, veri koruma ilkelerinin etkili bir şekilde uygulanması amacıyla tasarlanan takma ad kullanımı gibi uygun teknik ve kurumsal tedbirler (Technical and Organizational Measures-TOM) veri sorumlusu tarafından uygulanacak ve bu şekilde veri sahiplerinin hakları koruma altına alınacaktır (GDPR, m. 25/1). Olağan durumda koruma özellikle, veri sahibinin müdahalesi olmaksızın, kişisel verilerin belirsiz sayıda kişinin erişimine açılmamasını sağlayacaktır (GDPR, m. 25/2). Bu maddenin gerekliliklerinin yerine getirilmesinde, veri sorumlularının standartlarının yeterliliklerinin tespiti için GDPR'ın 42. maddesine uygun şekilde onaylı bir belgelendirme mekanizması benimsenebilecektir.

Veri sorumlusu ve işleyenin tekniğin bilinen durumu (son teknoloji), uygulama maliyetleri ve işleme faaliyetinin niteliği, kapsamı, bağlamı ve amaçlarının yanı sıra gerçek kişilerin hak ve özgürlükleri açısından riskleri dikkate alarak, uygun güvenlik seviyesi sağlamak üzere teknik ve organizasyona ilişkin şu tedbirleri uygulayacaktır (GDPR, m. 32/1):

- Kişisel verilerde takma ad kullanımı ve şifreleme,

- İşleme sistemleri ve hizmetlerinin gizliliği, bütünlüğü, elverişliliği ve esnekliğinin sürekli surette sağlanabilmesi,

- Fiziksel veya teknik bir durumda, kişisel verilerin elverişliliğinin ve kişisel verilere erişimin vakit kaybetmeksizin (timely) eski haline getirilebilmesi,

- İşleme faaliyetinin güvenliliğinin sağlanmasına yönelik olarak teknik ve organizasyonel tedbirlerin etkililiğinin düzenli olarak sınanması, ölçülmesi ve değerlendirilmesine ilişkin süreç.

Veri güvenliğinin sağlanması açısından dikkate alınması gereken tekniğin bilinen durumu (state of the art) kavramı GDPR'da tanımlanmamıştır. Patent hukukunda tekniğin bilinen durumu, patent başvurusu tarihinden önce, yazılı veya sözlü tanıtım vasıtasıyla, kullanım veya başka herhangi bir yolla kamuya sunulan her şeyi (everything made available to the public) kapsamaktadır.[497] Cambridge Sözlüğü'nde tekniğin bilinen durumu "çok modern, en yeni fikir ve yöntemlerin kullanıldığı" şeklinde tanımlanmıştır.[498] Buna karşılık Wikipedia'da tekniğin bilinen

[497] Bu konuda bkz. **Tamer Soysal**, Tarımda Biyoteknoloji Uygulamaları ve Patent Hakları (Agricultural Biotech Patent Law), Adalet Yayınevi, 2019.

[498] Cambridge Dictionary, https://dictionary.cambridge.org/dictionary/english/state-of-the-art (Son Erişim Tarihi: 19.03.2019)

durumu "genel gelişmenin, cihaz, teknik veya bilimsel alanda belirli bir zamanda başarılan en yüksek seviye" şeklinde ifade edilmiştir.[499] Tekniğin bilinen durumunun en önemli özelliği zamana göre değişmesi ve dinamik bir kavram olmasıdır. Veri koruma alanında tekniğin bilinen durumu ise daha çok siber güvenlik ile ilişkilendirilmekte ve etkin güvenlik yöntem ve teknolojilerinin sürekli surette geliştirilmesinin öncüsü olan inovasyonu ifade eder şekilde anlaşılmaktadır.[500] Bu yenilikler dikkate alınırken uygulama maliyeti (the costs of implementation) de dikkate alınmak zorundadır (GDPR, m. 25/1, 32/1). Dolayısıyla veri sorumlusu ve işleyenler de bu yeni olanakları uygulayan yetkin güvenlik şirketleri ile çalışmak durumunda olacaklardır.

VI. Sınıraşan Veri Transferleri

Tüzük, AB sınırları içerisinde verilerin serbest akışını öngörürken, kişisel verilerin yurtdışına aktarılması için belirli şartların gerçekleşmesi ve Tüzüğün 5. Bölümünde açıklanan kurallara uyulması gerektiğini düzenlemiştir.[501] Bu bağlamda, AB'nin politik bir birlik olması ve Birlik içinde serbest veri dolaşımının hedeflenmesi nedeniyle "yurt dışına aktarılma" özel bir anlama sahip olup, AB dışındaki üçüncü ülkelere veya uluslararası kuruluşlara veri aktarımı anlamına gelmektedir.[502] Tüzükte açıkça belirtildiği üzere, kişisel verilerin Birlik içerisinde serbest dolaşımı, gerçek kişilerin kişisel verilerin işlenmesiyle ilgili olarak korunması ile bağlantılı sebeplerle kısıtlanamaz veya yasaklanamaz.[503] Ayrıca belirtilmelidir ki serbest veri akışı alanı Avrupa Ekonomik Alan Sözleşmesi ile genişletilmiştir.[504]

Kurallar detaylı olarak incelenmeye başlamadan önce dikkate alınması gereken diğer bir husus ise, suçun önlenmesi, soruşturulması, tespiti veya kovuşturulması veya cezai süreçlerin yürütülmesi amacıyla işlenen kişisel verilerin Üye Devlet ve Avrupa Ekonomik Alanı içindeki serbest dolaşımının Tüzüğe değil, 2016/680 sayılı Direktif'e tabi olduğudur.[505]

Tüzük uyarınca bir üçüncü ülkeye veya uluslararası kuruluşa veri aktarımı yapılabilmesi için, kişisel verilerin her şeyden önce Tüzüğe uygun olarak elde edilmiş olması ve Tüzüğe uygun olarak işleniyor olması gereklidir.[506] Tüzüğe uygun olarak elde edilmiş ve işlenmesi

499 Wikipedia, https://en.wikipedia.org/wiki/State_of_the_art (Son Erişim Tarihi: 19.03.2019)
500 Solving the GDPR Puzzle, Data Protection with State of the Art Cybersecurity, https://www.softcat.com/assets/uploads/pdfs/gdpr/Solving-the-GDPR-puzzle.pdf, s. 16 (Son Erişim Tarihi: 19.03.2019)
501 **Giakoumopoulos/Buttarelli/O'Flaherty**, s. 250; GDPR, m. 44(1).
502 **Develioğlu**, s. 73.
503 GDPR, m. 1(3).
504 **Giakoumopoulos/Buttarelli/O'Flaherty**, s. 252.
505 **Giakoumopoulos/Buttarelli/O'Flaherty**, s. 252.
506 **Develioğlu**, s. 73.

gerçekleştirilen kişisel veriler, iki şekilde üçüncü bir ülke veya uluslararası kuruluşa aktarılabilir: Avrupa Birliği Komisyonunun uygunluk kararı çerçevesinde veya Komisyon'un uygunluk kararı olmamasına rağmen belirli şartların varlığı halinde.[507]

A. Avrupa Birliği Komisyonunun Uygunluk Kararı Çerçevesinde Aktarım

Tüzük, Komisyonun bir üçüncü ülke veya söz konusu üçüncü ülke dahilindeki bir bölge veya bir ya da daha fazla sayıda sektörün ya da uluslararası bir kuruluşun *yeterli düzeyde bir koruma sağladığına karar verdiği hallerde*, spesifik bir onaya gerek olmaksızın bu ülke veya uluslararası kuruluşa yönelik bir kişisel veri aktarımı gerçekleştirebileceğini düzenlemiştir.[508] Bu maddedeki *"yeterli düzeyde bir koruma sağlamak"* ABAD tarafından *"üçüncü ülkenin temel hak ve özgürlüklere ilişkin olarak sağladığı korumanın temel olarak AB hukukunca sağlanan garantiler ile eş düzeyde olması"* olarak yorumlanmıştır.[509]

Komisyon, yabancı ülkelerin yeterli düzeyde bir koruma sağlayıp sağlamadığına bu ülkelerin yerel hukuklarını, tabi olduğu uluslararası yükümlülüklerini ve sahip olduğu bağımsız denetim mekanizmalarını inceleyerek karar verir.[510] Komisyon, ilgili üçüncü ülke veya uluslararası kuruluşun yeterli düzeyde bir koruma sağladığına kanaat getirirse, bağlayıcı olan *"uygunluk kararı"* verebilir.[511] Komisyon, bu kararı yalnızca tüm ülke çapında her alanda geçerli olmak üzere vermek yerine, söz konusu ülke içerisindeki bir bölge veya bir ya da daha fazla sayıda sektöre ilişkin olarak da verebilir.[512] Bu kararın varlığı halinde dahi, bir kişinin verilerinin üçüncü bir ülkeye aktarımına ilişkin olarak ilgili ülke tarafından yeterli seviyede korumanın sağlanmadığı iddiasında bulunması durumunda, yerel denetim makamlarının bu iddiayı incelemeye yetkisi vardır.[513]

Uygunluk kararı ile ilgili değinilmesi gereken önemli bir nokta, 95/46/EC sayılı Direktif'te hem Üye Devletlerin hem Avrupa Birliği Komisyonunun bu kararı alma imkânı düzenlenmişken, Tüzük bu kararın yalnızca Komisyon tarafından alınabileceğini öngörmüştür.[514]

---

507 **Develioğlu**, s. 74.
508 GDPR, m. 45(1).
509 ABAD, C-362/14, Maximillian Schrems v. Data Protection Commissioner [GC], 6 Ekim 2015, para. 96.
510 Bkz: **Hakan Üzeltürk**, Avrupa Birliği Genel Veri Koruma Düzenlemesi, Yeditepe Üniversitesi Hukuk Fakültesi Dergisi, C. XV, S. 2, İstanbul, 2018, s. 168; **Develioğlu**, s. 75.
511 **Giakoumopoulos/Buttarelli/O'Flaherty**, s. 254.
512 **Giakoumopoulos/Buttarelli/O'Flaherty**, s. 255; GDPR, m. 45(3).
513 **Giakoumopoulos/Buttarelli/O'Flaherty**, s. 254, 255.
514 **Develioğlu**, s. 74.

Komisyon, haklarında uygunluk kararı verilmiş üçüncü ülkeler ve uluslararası kuruluşlarda meydana gelen gelişmeleri *sürekli* olarak izler.[515] Verilen uygunluk kararları *en az dört yılda bir* tüm gelişmeler dikkate alınarak gözden geçirilmelidir.[516] Bunun yanında, elde edilen bilgiler ışığında, uygunluk kararının geri alınması, değiştirilmesi veya askıya alınması her zaman mümkündür.[517] Böyle bir durumun varlığı halinde Komisyon ile ilgili üçüncü ülke veya uluslararası kuruluşlar arasında söz konusu durumun giderilmesi amacıyla görüşmeler de gerçekleştirebilir.[518]

95/46/EC sayılı Direktif'e dayalı olarak Komisyon tarafından kabul edilen kararların, Tüzük uyarınca kabul edilen bir Komisyon Kararı ile değiştirilene, yenilenene veya yürürlükten kaldırılana kadar yürürlükte kalacağı Tüzükte açıkça belirtilmiştir.[519]

Son olarak, Tüzükte, Komisyon'un yeterli düzeyde bir korumanın sağlandığı veya artık sağlanmadığına karar verdiği üçüncü ülkeler, bir üçüncü ülke içerisindeki bölgeler ve sektörler ile uluslararası kuruluşların Avrupa Birliği Resmi Gazetesi ve web sitesinde yayımlanacağı düzenlenmiştir.[520]

B. Avrupa Birliği Komisyonunun Uygunluk Kararı Bulunmayan Hallerde Aktarım

Avrupa Birliği Komisyonu tarafından alınan bir karar olmaması halinde, ancak bir veri sorumlusu veya işleyenin uygun güvenceler sağlamış olması halinde ve uygulanabilir veri sahibi hakları ve veri sahiplerine yönelik etkili kanun yollarının mevcut olması koşuluyla, söz konusu veri sorumlusu veya işleyen bir üçüncü ülke veya uluslararası bir kuruluşa kişisel veri aktarabilir.[521]

Bu kapsamda uygun güvenceler, bir denetim makamından spesifik bir onay alınmasına gerek olmaksızın nasıl sağlanabileceği Tüzükte sayılmıştır. Buna göre, uygun güvenceler aşağıdaki yöntemlerle sağlanabilir:

(a) Kamu kuruluşları veya organları arasında yasal bağlayıcılığı bulunan ve uygulanabilir bir belge,

(b) Bağlayıcı kurumsal kurallar,

(c) Komisyon tarafından kabul edilen standart veri koruma şartları,

(d) Bir denetim makamı tarafından kabul edilen ve Komisyon tarafından onaylanan standart veri koruma şartları,

---

515 GDPR, m. 45(4).
516 GDPR, m. 45(3).
517 **Develioğlu**, s. 75.
518 **Giakoumopoulos/Buttarelli/O'Flaherty**, s. 255.
519 GDPR, m. 45(9).
520 GDPR, m. 45(8).
521 GDPR, m. 46(1).

(e) Onaylı davranış kuralları,

(f) Onaylı bir belgelendirme mekanizması.[522]

Bu yöntemlere ek olarak, yetkili denetim makamı tarafından onaylanmaları halinde veri sahibi veya işleyen ile üçüncü ülke ya da uluslararası kuruluştaki kişisel veri sorumlusu, işleyeni ya da alıcısı arasındaki özelleştirilmiş sözleşme maddeleri de verilerin yurt dışına aktarımı hususunda uygun bir güvence teşkil edebilir.[523] Aynı şekilde, yetkili denetim makamı tarafından onaylanması koşuluyla, kamu kuruluşları ya da organları arasındaki idari düzenlemelere eklenecek olan uygulanabilir ve etkili veri sahibi haklarını kapsayan hükümler de uygun bir güvence olarak değerlendirilebilir. [524]

C. Spesifik Durumlara Yönelik Hukuka Uygunluk Nedenleri

Tüzükte, bir uygunluk kararı veya uygun güvenceler olmaması durumunda dahi, belirli bazı hallerin varlığı halinde üçüncü bir ülkeye veya uluslararası bir kuruluşa kişisel veri aktarımı gerçekleştirilebileceği düzenlenmiştir. Bu haller Tüzükte sınırlı olarak sayılmış olup aşağıdaki gibidir:

(a) Veri sahibinin, bir yeterlilik kararı ve uygun güvencelerin bulunmaması nedeniyle söz konusu aktarımların kendisine yönelik risklerin haberdar edilmesinin ardından, önerilen aktarıma açık bir şekilde rıza göstermesi,

(b) Aktarımın veri sahibi ile veri sorumlusu arasındaki bir sözleşmenin yürütülmesi veya veri sahibinin talebiyle alınan sözleşme öncesi tedbirlerin uygulanması acısından gerekli olması,

(c) Aktarımın veri sorumlusu ile başka bir gerçek veya tüzel kişi arasında veri sahibi yararına yapılan bir sözleşmenin imzalanması veya yürütülmesi açısından gerekli olması,

(d) Aktarımın kamu yararına ilişkin önemli sebeplerden dolayı gerekli olması,

(e) Aktarımın yasal iddialarda bulunulması, bu iddiaların uygulanması veya savunulması acısından gerekli olması,

(f) Aktarımın veri sahibi veya diğer kişilerin hayati menfaatlerinin korunması acısından gerekli olması,

(g) Aktarımın istişareye açık olan bir sicilden yapılması.[525]

Aktarımın bir uygunluk kararına veya uygun güvencelerin sağlanmış olmasına veya yukarıda açıklanan hukuka uygunluk nedenlerine dayanmadığı hallerde, üçüncü bir ülke veya

522 GDPR, m. 46(2).
523 GDPR, m. 46(3).
524 GDPR, m. 46(3).
525 GDPR, m. 49(1).

uluslararası bir kuruluşa yönelik bir aktarım, yalnızca aktarımın yinelemeli olmaması, yalnızca sınırlı sayıda veri sahibini ilgilendirmesi, veri sahibi tarafından gözetilen ve veri sahibinin menfaatleri veya hakları ile özgürlüklerin ağır basmadığı zorlayıcı meşru menfaatler doğrultusunda gerekli olması ve veri sahibinin veri aktarımı ile ilgili tüm durumları değerlendirmiş olması ve bu değerlendirmeye dayalı olarak kişisel verilerin korunması ile ilgili uygun güvenceler sağlamış olması durumunda, gerçekleştirilebilir.[526]

Madde 29 Çalışma Grubuna göre, spesifik durumlara göre hukuka uygunluk nedenine dayanan yurt dışına veri aktarımları; istisnai nitelikte olmalı ve her bireye ilişkin durum için ayrı olarak değerlendirilmelidir, ayrıca bu yöntem yinelemeli olmamalı ve geniş kapsamlı aktarımlar için kullanılmamalıdır.[527]

D. Uluslararası Anlaşmalara Dayalı Aktarımlar

Avrupa Birliği ve Üye Devletler, üçüncü ülkelerle, belirli amaçlarla kişisel verilerin üçüncü ülkelere aktarımını düzenleyen uluslararası anlaşmalar imzalayabilir.[528] İmzalanacak anlaşmalar, ilgili bireyin kişisel verilerinin korunmasını sağlayacak uygun güvenceler içermelidir. [529]Tüzük, bu uluslararası anlaşmalara halel getirmez.[530]

§ 4. Bağımsız Denetim

Bağımsız denetim, Avrupa veri koruma hukukunun vazgeçilmez unsurlarından biridir. Nitekim, AB Şartı'nın 8. maddesinin 3. fıkrasında kişisel bilgilerin korunmasına ilişkin kurallara uyumun bağımsız bir makam tarafından denetleneceği öngörülmüştür.[531] Tüzükte, her Üye Devlet'in, gerçek kişilerin işleme faaliyeti ile ilgili temel hakları ve özgürlüklerini korumak ve Birlik içerisinde kişisel verilerin serbest akışını kolaylaştırmak üzere, bir ya da daha fazla sayıda bağımsız kamu kurulusunun (denetim makamı) bu Tüzüğün uygulamasının izlenmesinden sorumlu olmasını sağlaması gerektiği öngörülmüştür.[532] Bağımsız denetimin kişisel verilerin korunması için önemi mahkeme içtihatlarına da yansımıştır. Örneğin, *Schrems*[533] davasında ABAD, Komisyon tarafından yurt dışına transfer için verilmiş bir uygunluk kararı olması durumunda dahi, ulusal

526 GDPR, m. 49(1).
527 Article 29 Working Party (2005), Working document on a common interpretation of Article 26 (1) of Directive 95/46/EC of 24 October 1995, WP 114, Brussels, 25 Kasım 2005.
528 **Giakoumopoulos/Buttarelli/O'Flaherty**, s. 265, 266.
529 **Giakoumopoulos/Buttarelli/O'Flaherty**, s. 265, 266.
530 GDPR, Gerekçe 102.
531 **Giakoumopoulos/Buttarelli/O'Flaherty**, s. 189.
532 Bkz: **Üzeltürk**, s. 170-172, GDPR, m. 51(1).
533 ABAD, C-362/14, Maximillian Schrems v. Data Protection Commissioner [GC], 6 Ekim 2015, para. 41.

denetim makamına bu konuda bir şikâyette bulunulması durumunda, ulusal denetim makamının bu şikâyeti özenle incelemesi gerektiğini belirtmiştir.[534]

I. Bağımsızlık

Tüzükte, her denetim makamının Tüzük uyarınca görevlerini yerine getirirken ve yetkilerini kullanırken *tamamen bağımsız* olarak hareket etmesi gerektiği açıkça düzenlenmiştir.[535] Denetim makamının, üyelerinin ve çalışanlarının direkt veya dolaylı dış etkilere karşı bağımsız kalabilmesi, veri koruma ile ilgili hususlara ilişkin karar verilirken objektifliğin sağlanabilmesi için oldukça önemli bir gerekliliktir.[536] Örneğin; ABAD, *Avrupa Komisyonu v. Avusturya* davasında, Avusturya Veri Koruma Merciinin işgücünün Federal İdare tarafından sağlanmasının ve İdare'yi sürekli bilgilendirme yükümlülüğü bulunmasının AB Veri Koruma Hukukunda öngörülmüş denetim makamının bağımsızlığı şartını ihlal ettiğini ifade etmiştir.[537]

Tüzükteki düzenleme uyarınca, denetim makamlarının görevlerini yerine getirirken ve yetkilerini kullanırken tamamen bağımsız olabilmesi için:

(i) Her denetim makamının üyeleri, Tüzük uyarınca görevlerini yerine getirirken ve yetkilerini kullanırken, doğrudan veya dolaylı dış etkilerden bağımsız hareket etmeli ve hiç kimseden talimat talebinde bulunmalı veya talimat almamalıdır.[538]

(ii) Her denetim makamının üyeleri görevlerine uygun olmayan eylemlerden kaçınmalıdır ve görev süreleri boyunca, maddi getirisi olsun ya da olmasın, bu göreve uygun olmayan hiçbir işle iştigal etmemelidir.[539]

(iii) Her Üye Devlet görevlerini etkili bir şekilde yerine getirebilmeleri ve yetkilerini etkili bir şekilde kullanabilmeleri için gereken insan kaynağı, teknik ve mali kaynaklar, binalar ve altyapının her denetim makamına sağlanmasını temin etmelidir.[540]

(iv) Her Üye Devlet her denetim makamının kendi personelini kendisinin seçmesini ve bu makamın kendi personelinin olmasını sağlamalıdır.[541]

---

534 **Giakoumopoulos/Buttarelli/O'Flaherty**, s. 190.
535 GDPR, m. 52(1).
536 **Giakoumopoulos/Buttarelli/O'Flaherty**, s. 191.
537 ABAD, C-614/10, European Commission v. Republic of Austria [GC], 16 Ekim 2012, para. 59, 63.
538 GDPR, m. 52(2).
539 GDPR, m. 52(3).
540 GDPR, m. 52(4).
541 GDPR, m. 52(5).

(v) Her Üye Devlet her denetim makamının tabi olduğu mali kontrolün denetim makamının bağımsızlığını etkilememesini ve genel devlet bütçesi veya ulusal bütçenin parçası olabilecek ayrı yıllık kamu bütçelerinin bulunmasını sağlamalıdır.[542]

II. Yetki ve Görevler

Denetim makamı, ulusal hukukta Tüzük ile uyumluluğu sağlayan esas organdır. Bu amaçtan hareketle, denetim makamlarının izlemenin ötesine geçen, proaktif ve önleyici denetleme faaliyetlerini de içeren geniş görev ve yetkileri vardır. Görevlerini ifa edebilmeleri için denetim makamlarının soruşturmaya ve tavsiye vermeye ilişkin ve düzeltici yetkileri olması gerekmektedir. Denetim makamlarının yetkileri Tüzüğün 58. maddesinde sayılmıştır:

(a) Veri sorumluları ve veri sahiplerine verilerin korunmasına ilişkin her konuda tavsiye vermek,

(b) Standart sözleşme maddeleri, bağlayıcı kurumsal kurallar veya idare düzenlemeleri onaylamak,

(c) İşleme faaliyetlerini araştırmak ve buna bağlı olarak müdahale etmek,

(d) Veri sorumlularının faaliyetlerinin denetimi için ilgili bazı bilgilerin arzını talep etmek,

(e) Veri sorumlularını uyarmak veya kınamak ve kişisel veri ihlali bildirimlerinin veri sahiplerine gönderilmesine karar vermek,

(f) Verinin düzeltilmesine, engellemesine, silinmesine veya yok edilmesine karar vermek,

(g) İşleme faaliyetlerine geçici veya kati bir sınırlama getirmek,

(h) Bir konuyu mahkemeye havale etmek.[543]

Denetim makamının görevlerini yerine getirebilmesi ve yetkilerini kullanabilmesi için, bir inceleme ile ilgili gerekli tüm kişisel veri ve bilgilere, ayrıca veri sorumlusunun ilgili bilgileri tuttuğu mülklere erişimi olmalıdır.[544] ABAD, veri sahipleri için verilerin korunmasının etkili bir şekilde sağlanabilmesi için denetim makamının yetkilerini geniş yorumlanması gerektiğini ifade etmiştir.[545]

Her denetim makamı, kendi bölgesinde yetkilerini kullanmayı yetkilidir.[546] Bunun yanında Tüzük *"tek durak noktası"* mekanizması kurmakta ve farklı denetim makamları arasında iş birliği yapılmasını gerekli kılmaktadır. Buna göre, sınır ötesi veri işleme faaliyetleri olan hallerde etkili iş

542 GDPR, m. 52(6).
543 **Giakoumopoulos/Buttarelli/O'Flaherty**, s. 194, 195; GDPR, m. 58.
544 **Giakoumopoulos/Buttarelli/O'Flaherty**, s. 195.
545 Guide to General Data Protection Regulatin.
546 **Giakoumopoulos/Buttarelli/O'Flaherty**, s. 195.

birliğinin sağlanabilmesi için, Tüzük, bir baş denetim makamının, veri sorumlusunun ana veya tek işletmesinin denetim makamını olarak kurulmasını öngörmektedir.[547]

Bağımsız denetim makamları ayrıca talep ve şikayetler ile ilgilenmeye, verilerin korunmasına ilişkin toplum bilinci oluşturmaya ve kişisel verilerin işlenmesine ilişkin yasal ve idari düzenlemeler için ulusal karar mekanizmalarında yer alan kişilere tavsiye sağlama yetkileri mevcuttur.[548]

Tüzüğün *"tek durak noktası"* mekanizması uyarınca, bir Üye Devlette birden fazla denetim makamının kurulmuş ise, söz konusu Üye Devlet bu makamları Kurul'da temsil edecek denetim makamını tayin eder ve diğer makamların 63. maddede atıfta bulunulan tutarlılık mekanizmasına ilişkin kurallara uyumluluğunu sağlayacak mekanizmayı ortaya koyar.

III. İş Birliği

Tüzük, denetim makamları arasında iş birliğine ilişkin genel bir çerçeve çizmekle birlikte, sınır ötesi veri işleme faaliyetleri ile ilgili olarak denetim makamlarının iş birliği için daha spesifik kurallar öngörmektedir.[549]

Tüzük uyarınca denetim makamları, Tüzük'ün tutarlı bir şekilde yürütülmesi ve uygulanması amacıyla birbirlerine ilgili bilgileri ve karşılıklı desteği sağlamalıdır, ayrıca birbirleriyle etkili iş birliğine yönelik tedbirleri uygulamaya koymalıdır.[550] Bu kapsamda karşılıklı yardım, özellikle, ön onaylar ve istişarelerin, denetimlerin ve soruşturmaların yürütülmesine ilişkin talepler gibi bilgi talepleri ve denetim tedbirlerini kapsar.[551]

Tüzüğün *"tek durak noktası"* mekanizması uyarınca, bir veri sorumlusu veya işleyenin birden çok Üye Devlette işletmesi varsa veya tek işletmesi olmasına rağmen işleme faaliyetleri birden çok Üye Devletteki veri sahiplerini önemli ölçüde etkiliyorsa, ana (veya tek) işletmenin denetim makamı, veri sorumlusu veya işleyenin sınır ötesi faaliyetlerine ilişkin olarak baş makamdır.[552]

Yüksek seviyede bir veri korumasının sağlanabilmesi için, baş denetim makamı yalnız hareket etmemeli, veri sorumluları veya işleyenler tarafından gerçekleştirilen kişisel veri işlemeye yönelik kararlar alınması için ilgili diğer denetim makamları ile iş birliği yapmalıdır.[553] İlgili

---

547 **Giakoumopoulos/Buttarelli/O'Flaherty**, s. 197; GDPR, m. 56(1).
548 **Giakoumopoulos/Buttarelli/O'Flaherty**, s. 197.
549 **Giakoumopoulos/Buttarelli/O'Flaherty**, s. 197.
550 GDPR, m. 61(1).
551 GDPR, m. 61(1).
552 **Giakoumopoulos/Buttarelli/O'Flaherty**, s. 198.
553 **Giakoumopoulos/Buttarelli/O'Flaherty**, s. 198.

denetim makamları arasındaki iş birliği; karşılıklı bilgi paylaşımı, karşılıklı yardım, ortak soruşturma ve izlemeler gerçekleştirilmesini içerebilir.[554] Bu iş birliği, tutarlılığın sağlanması ve görüş birliğine ulaşılması için gösterilmesi gereken bir çabadır.[555]

Her denetim makamı başka bir denetim makamının karşılıklı yardım talebine herhangi bir *gecikmeye mahal verilmeksizin* ve talebi aldıktan sonra *en geç, bir ay içerisinde* yanıt vermelidir.[556]

Veri sorumlusunun birden çok Üye Devlette işletmesinin bulunması halinde denetim makamları, ortak soruşturmalar ve ortak yaptırım tedbirleri de dahil olmak üzere, diğer üye devletlerin denetim makamlarının üyeleri veya personelinin müdahil olduğu ortak çalışmalar gerçekleştirebilir.[557]

IV. Avrupa Veri Koruma Kurulu (European Data Protection Board)

Veri koruma kurallarının AB içinde etkili ve istikrarlı bir biçimde uygulanmasını temin etme hususunda önem teşkil eden diğer bir kurum ise Avrupa Veri Koruma Kurulu'dur (Kurul).[558] Tüzük, Kurul'u tüzel kişiliğe sahip bir AB organı olarak kurmuştur.[559] Kurul, 95/46/EC sayılı Direktif'in, Komisyon'a bireylerin kişisel verilerin işlenmesi ve gizliliğe ilişkin haklarını etkileyen AB faaliyetleri hakkında tavsiye vermesi, direktifin yeknesak uygulanmasını teşvik etmesi ve Komisyon'a veri koruması ile ilgili konularda uzman görüşü sağlaması amacıyla kurduğu Madde 29 Çalışma Grubunun halefidir.[560]

Kurul her üye devletin bir denetim makamı başkanı ile Avrupa Veri Koruma Denetmeni veya bunların ilgili temsilcilerinden meydana gelir.[561]

Kurul'un görevleri, Tüzüğün 64, 65 ve 70. maddelerinde detaylıca anlatılmış olup, bu görevler üç ana başlık altında toplanabilir:

- **Tutarlılık:** Kurul, üç halde hukuki bağlayıcılığı olan bir karar alabilir:

(i) Bir denetim makamı "tek durak noktası" hallerinden birinde ilgili ve gerekçeli bir itiraz ileri sürmüşse,

(ii) Hangi denetim bakamının "baş denetim makamı" olduğu konusunda çelişkili görüşler varsa,

554 GDPR, m. 60(1)-60(3).
555 **Giakoumopoulos/Buttarelli/O'Flaherty**, s. 198.
556 GDPR, m. 61(2).
557 GDPR, m. 62(1).
558 **Giakoumopoulos/Buttarelli/O'Flaherty**, s. 199.
559 GDPR, m. 68(1).
560 **Giakoumopoulos/Buttarelli/O'Flaherty**, s. 199, 200.
561 GDPR, m. 68(3).

(iii) Yetkili denetim makamı Kurul'un görüşünü talep etmemişse veya Kurul görüşüne uygun hareket etmiyorsa.[562]

Kurul'un bu bağlamdaki temel görevi, Tüzüğün tüm AB'de tutarlı bir şekilde uygulanmasını sağlamaktır.[563]

- **Danışma:** Kurul'un görevleri, Komisyon'a AB'de veri korumaya ilişkin herhangi bir konu ile ilgili olarak tavsiye vermeyi de içermektedir.[564]
- **Rehberlik:** Kurul, ayrıca, Tüzüğün tutarlı bir şekilde uygulanmasını sağlamak ve denetim makamları arasında iş birliği ve bilgi değişimini sağlamak amacıyla kılavuzlar, tavsiyeler ve örnek uygulamalar yayınlar. Ek olarak, Kurul, veri sahibi ve işleyen birliklerini davranış kuralları ve veri koruma belgelendirme mekanizmaları ve mühürleri oluşturmak hususunda teşvik etmelidir.[565]

Son olarak değinilmesi gereken diğer bir nokta ise, Kurul'un kararlarına karşı ABAD'a başvurulabileceğidir.[566]

V. Tutarlılık Mekanizması

Tüzüğün bütün Üye Devletler'de yeknesak bir şekilde uygulanmasını sağlamak için bir tutarlılık mekanizması öngörülmüştür. Buna göre, Tüzük'ün AB içerisinde tutarlı bir şekilde uygulanmasına katkıda bulunulması amacıyla, denetim makamları, Tüzükte belirtilmiş tutarlılık mekanizması vasıtasıyla, birbirleriyle ve uygun olduğu hallerde, Komisyon ile işbirliği yapmalıdır.

Bu doğrultuda tutarlılık mekanizması iki durumda kullanılır. Bunlardan ilki, Tüzüğün 64. maddesi uyarınca yetkili bir denetim makamının belirli tedbirlerden birini kabul etmeyi amaçlaması halinde veya standart sözleşme maddelerinin tespit edilmesi için bildireceği görüşlere ilişkindir. İkincisi ise Kurul'un "tek durak noktası" durumlarında denetim makamları için verdiği bağlayıcı kararlar ve denetim makamının Kurul'un görüşünü sormadığı veya görüşüne bağlı kalmadığı hallerdir.[567]

VI. İvedilik Prosedürü

İstisnai durumlarda, ilgili bir denetim makamının veri sahiplerinin hakları ve özgürlüklerinin korunmasına yönelik olarak acil bir şekilde harekete geçmesine ihtiyaç varsa, söz konusu denetim makamı, tutarlılık mekanizmasından veya iş birliği prosedüründen ayrılarak, üç,

562 GDPR, m. 65(1).
563 **Giakoumopoulos/Buttarelli/O'Flaherty**, s. 200.
564 **Giakoumopoulos/Buttarelli/O'Flaherty**, s. 200.
565 **Giakoumopoulos/Buttarelli/O'Flaherty**, s. 201.
566 **Giakoumopoulos/Buttarelli/O'Flaherty**, s. 201.
567 **Giakoumopoulos/Buttarelli/O'Flaherty**, s. 201.

ayı geçmeyecek belirli bir süre için geçerli olacak şekilde ve ilgili Devlet sınırları içinde hukuki sonuç, doğurmak üzere ivedilikle geçici tedbirler alabilir.[568] Geçici tedbiri alan denetim makamı, gecikmeksizin, söz konusu tedbirleri alma sebeplerini, ilgili diğer denetim makamlarına, Kurul'a ve Komisyon'a bildirir.[569] Aynı denetim makamı, gerekçelerini belirterek Kurul'dan acil bir görüş veya nihai bir karar vermesini talep edebilir. Bu talep, ilgili kişilerin hak ve özgürlüklerin korunmasına yönelik acil bir şekilde harekete geçilmesinin gerektiği bir durumda uygun bir tedbir almadığı hallerde, herhangi bir denetim makamı tarafından, gerekçeleri açıklanarak ileri sürülebilir.[570] Bu bağlamda acil bir görüş, veya acil bir nihai karar Kurul üyelerinin salt çoğunluğuyla iki hafta içerisinde alınır.[571]

§ 5. Veri Sahiplerinin Hakları ve Kısıtlamaları

I. Veri Sahiplerinin Hakları

A. Bilgilendirilme Hakkı

Veri sahiplerinin kendilerine ait kişisel verilerin işlenip işlenmediğini, hangi kişisel verilerinin işlendiğini bilmesi, kişinin verileri üzerindeki kontrolünü sağlayabilmeleri ve kişisel verilerin korunması hukukundan kaynaklanan haklarını kullanabilmeleri açısından oldukça büyük önem taşır. Bu nedenle, Tüzük, veri sorumlularına, planlanan bir veri işlemesi için kişisel veri topladıkları zaman, veri sahiplerini bilgilendirme yükümlülüğü getirmiştir. Bu yükümlülüğün doğması için veri sahibinin veri sorumlusundan bilgilendirilme talep etmesi aranmamış olup, veri sorumlusunun işlemek üzere kişisel veri toplanması yeterlidir.[572] Çünkü, veri sahiplerinin, hangi verilerinin nasıl toplandığını, kullanıldığını veya işlendiğini, veri işleme faaliyetlerinin barındırdığı riskleri, bu risklere karşı düzenlenen güvenceleri, işlemeye ilişkin haklarını bilme hakları mevcuttur.[573] Aksi takdirde bireylerin kendi verileri üzerinde kontrol sağlamaları ve işleme sebebiyle ortaya çıkabilecek olumsuz sonuçlardan korunmaları mümkün olmayacaktır. Yukarıda detaylıca açıklanan *"şeffaflık ilkesi"* ile önlenmeye çalışılan da tam olarak bu tehlikelerdir.

Tüzüğün 12. maddesi uyarınca, veri sorumlusu, işleme faaliyeti ile alakalı aşağıda detaylıca anlatılacak her türlü bilgiyi *öz, şeffaf, anlaşılır ve kolayca erişilebilir* bir biçimde, açık ve sade bir dil kullanarak veri sahibine sağlama yükümlülüğü altındadır.[574] Bu bilgiler, veri sahibine; *yazılı*

568 GDPR, m. 66(1); **Develioğlu**, s.143.
569 GDPR, m. 66(1).
570 GDPR, m. 66(3).
571 GDPR, m. 66(4).
572 **Giakoumopoulos/Buttarelli/O'Flaherty**, s. 207.
573 GDPR, Gerekçe 39.
574 GDPR, m. 12(1).

olarak veya uygun olduğu hallerde, *elektronik yollar da dahil olmak üzere diğer yollarla*, ayrıca veri sahibi tarafından talep edilmesi durumunda, veri sahibinin kimliğinin diğer yollarla doğrulanması koşuluyla, *sözlü* olarak sağlanabilir.[575] Ayrıca, veri sahiplerine sağlanacak bilgilerin, planlanan işleme faaliyetine yönelik anlamlı bir genel bakışın kolayca görülebilir, anlaşılabilir ve okunaklı bir biçimde sağlanması amacı ile standart simgelerle ile bir arada sağlanabileceği de Tüzükte düzenlenmiştir.[576]

Bilgilendirilme hakkına ilişkin örnek kararlardan biri *Smaranda Bara ve Diğerleri v. Casa Naţională de Asigurări de Sănătate ve diğerleri*[577] davasına ilişkindir. Bu davada ABAD, ulusal idare, öncesinde başvuruculara haber vermeksizin bilgilerini Ulusal Sağlık Sigortası Fonuna aktarmıştır. ABAD, veri sahiplerinin verilerinin işlendiği hakkında bildirilmesinin, bu kişilerin işlenen verilere erişim, bu verileri düzeltme veya bu verilerin işlenmesine itiraz haklarının kullanılmasını büyük ölçüde etkilediğinden oldukça önemli olduğunu belirtmiştir. Mahkeme, belirli şartlar altında bilgilendirilme hakkının kısıtlanabileceğinin düzenlendiğini ifade etse de olayda bu koşullar gerçekleşmediğinden, başvuruculaların, verileri Ulusal Sağlık Sigortası Fonuna aktarılmadan önce bilgilendirilmeleri gerektiğine hükmetmiştir.[578]

Tüzükte, kişisel verilerin sahibinden toplanması ve sahibinden alınmaması durumları için farklı düzenlemeler öngörülmüştür. Buna göre, kişisel veriler sahibinden toplandığında veri sahipleri:

(i) veri sorumlusunun ve varsa, veri sorumlusunun temsilcisinin kimlik ve irtibat bilgileri,

(ii) varsa, veri koruma görevlisinin irtibat bilgileri,

(iii) kişisel verilerin planlanan işlenme amaçlarının yanı sıra işleme faaliyetinin yasal dayanağı,

(iv) işleme faaliyetinin veri sorumlusunun veya 3. bir kişinin menfaatine dayanması durumunda bu kişiler tarafından gözetilen meşru menfaatler;

(v) varsa, kişisel verilerin alıcıları veya alıcı kategorileri;

(vi) kişisel verilerin üçüncü bir ülke veya uluslararası kuruluşa aktarılmasının amaçlanıp amaçlanmadığı, aktarım kararının Komisyon tarafından bir yeterlilik kararına dayanıp

575 GDPR, m. 12(1).
576 GDPR, m.12(1).
577 ABAD, C-201/14, Smaranda Bara ve Diğerleri v. Casa Naţională de Asigurări de Sănătate ve Diğerleri, 1 Ekim 2015.
578 **Giakoumopoulos/Buttarelli/O'Flaherty**, s. 209.

dayanmadığı ya da aktarım kararına ilişkin uygun veya münasip güvencelere ilişkin atıf ve bunların bir nüshasının elde edilme yolları veya bunların nerede erişilir kılındığı,

(vii) kişisel verilerin saklanacağı süre veya bunun mümkün olmaması halinde, bu sürenin belirlenmesi amacı ile kullanılan kriterler,

(viii) veri işlemeye ilişkin olarak sahip olduğu haklar ve bunların nasıl kullanılacağı,

(ix) kişisel verilerin sağlanmasının yasal ya da sözleşmeye bağlı bir gereklilik mi yoksa bir sözleşme yapılması için gereken bir gereklilik mi olduğu ve ayrıca, veri sahibinin kişisel verileri sağlamak zorunda olup olmadığı ve söz konusu verilerin sağlanmamasının muhtemel sonuçları,

(x) profil çıkarma da dahil olmak üzere otomatik karar vermenin varlığı,

(xi) bir denetim makamına şikâyette bulunma hakkı,

(xii) rızayı geri çekme hakkının varlığı hususlarında bilgilendirilmelidir.[579]

Kişisel verilerin sahibinden alınmaması durumunda ise veri sorumlusu veri sahibini kişisel verinin nereden ve nasıl elde edildiği hakkında bilgilendirmelidir.[580] Her halükârda, veri sorumlusu, veri sahibine, verilerin sahibinden alınması halinde sayılanlara benzer bilgileri sağlamalıdır.

Ayrıca, amacın sınırlandırılması ve şeffaflık ilkeleri uyarınca, veri sorumlusunun başta veri sahibine belirttiğinden farklı bir amaçla işleme yapmayı planlaması halinde, veri sorumlusu, veri sahibini, bu yeni amaç hakkında bilgilendirmelidir. Bu bilgilendirmeyi gerçekleştirip veri sahibinin yeni amaca ilişkin rızasını almaksızın veri sahibinin ilave işleme gerçekleştirmesi mümkün değildir.[581]

Bilgilendirilmenin sağlanma zamanı kişisel verilerin sağlandığı kaynağa göre değişiklik gösterecektir. Buna göre, kişisel verilerin direkt sahibinden sağlandığı hallerde, veri sorumlusu bilgilendirmeyi verilerin toplanması sırasında gerçekleştirmelidir.[582] Kişisel verilerin sahibinden alınmadığı durumlarda ise veri sorumlusu bilgilendirmeyi makul bir süre içerisinde, ancak en geç bir ay içerisinde yapmalıdır.[583] Ayrıca, eğer verilerin başka bir alıcıya açıklaması öngörülmüşse en geç kişisel verilerin ilk açıklandığı zaman bu bilgilendirme gerçekleştirilmelidir.[584]

579 GDPR, m. 13(1), 13(2).
580 **Giakoumopoulos/Buttarelli/O'Flaherty**, s. 211.
581 **Giakoumopoulos/Buttarelli/O'Flaherty**, s. 211.
582 GDPR, m. 13(1).
583 GDPR, m. 14(3).
584 GDPR, m. 14(3)(c).

Bilgilendirme ücretsiz olarak sağlanmalıdır. Fakat, bir veri sahibinin taleplerinin asılsız veya ölçüsüz olduğunun, özellikle taleplerin tekrarlanması nedeniyle, açıkça anlaşıldığı hallerde, veri sorumlusu makul bir ücret talep edebilir veya taleple ilgili işlem yapmayı reddedebilir.[585]

Veri sahibinin halihazırda bu bilgilere sahip olduğu hallerde ve ölçüde bu yükümlülüğün doğmayacağı Tüzükte açıkça düzenlenmiştir.[586] Ayrıca, kişisel verilerin veri sahibinden alınmadığı hallerde; özellikle kamu yararına arşivleme amaçları, bilimsel veya tarihi araştırma amaçları ya da istatistiki amaçlar için gerçekleştirilen işlemelerde, ilgili bilgilerin sağlanmasının imkânsız olması veya ölçüsüz bir çaba gerektirmesi söz konusu ise bilgilendirme yükümlülüğü doğmayacaktır.[587]

B. Erişim Hakkı

Tüzükte bireylerin kendi kişisel verilerine erişim hakkı açıkça düzenlenmiştir. Buna göre, veri sahibinin kendisi ile ilgili kişisel verilerin işlenip işlenmediğini veri sorumlusundan teyit etme ve eğer işleme faaliyeti varsa, ilgili kişisel verilere ve belirli bilgilere erişim hakkı vardır.[588]

Tüzükte yer alan düzenleme uyarınca veri sahipleri kişisel verilere ilişkin olarak:

(i) işleme amaçları,

(ii) ilgili kişisel veri kategorileri,

(iii) kişisel verilerin açıklandığı veya açıklanacağı alıcılar veya alıcı kategorileri,

(iv) varsa, kişisel verilerin saklanması acısından öngörülen süre veya süre belirlenmemişse, bu sürenin belirlenmesi amacı ile kullanılan kriterler,

(v) kişisel verilerin düzeltilmesini ve silinmesini talep etme ve veri işlemenin sınırlandırılması haklarının varlığı,

(vi) bir denetim makamına şikâyette bulunma hakkı,

(vii) kişisel verilerin veri sahibinden elde edilmemesi halinde, bu verilerin kaynaklarına ilişkin mevcut bilgiler;

(viii) otomatik karar vermenin varlığı ve en azından bu hallerde, yürütülen mantığa ilişkin anlamlı bilgilerin yanı sıra söz konusu işleme faaliyetinin veri sahibi acısından önemi ve öngörülen sonuçları hakkında bilgi talep etme ve bilgi alma hakkına sahiptir.[589]

---

585 GDPR, m. 12(5).
586 GDPR, m. 13(4), 14(5)(a).
587 GDPR, m. 14(5)(b).
588 GDPR, m. 15(1).
589 GDPR, m. 15(1).

Erişim hakkı uyarınca, veri sorumlusu, işleme faaliyetinden geçen kişisel verilerin bir nüshasını veri sahibine sağlamalıdır.[590] Veri sahibine sağlanan her bilgi, anlaşılabilir olmalıdır.[591] Örneğin; teknik kısaltmalar içeren bir bilgi, kısaltmalar açıklanmadığı müddetçe yeterli sayılmayacaktır.[592]

ABAD içtihatları uyarınca, kişisel verilere erişim hakkı aşırı zaman sınırlamalarına tabi olmamalıdır. Örneğin; ABAD, *Rijkeboer* davasında, veri sahiplerine geçmişteki verilerine erişim hakkının sağlanmaması durumunda, bu kişilerin, verilerinin düzeltilmesi ve silinmesi gibi haklarını kullanmasının ve yasal yollara başvurup tazminat alabilmesinin mümkün olmayacağını belirtmiştir.[593] Dolayısıyla, veri sahiplerinin geçmişte gerçekleşmiş veri işleme faaliyetlerine ilişkin olarak makul derecede bilgi edinme şansları olmalıdır.[594]

C. Düzeltme Talep Hakkı

Verilerin doğruluğu, veri korumanın etkin olarak sağlanabilmesi için mutlaka sağlanması gereken bir özelliktir ve yukarıda açıklanan doğruluk ilkesi ile doğrudan ilgilidir.[595] Bu gereklilikten yola çıkılarak, Tüzükte, veri sahiplerinin kendileri ile ilgili doğru olmayan kişisel verilerin *gereksiz gecikmeye mahal verilmeksizin* düzeltilmesini veri sorumlusundan talep etme hakkı bulunduğu düzenlenmiştir.[596] Aynı zamanda, işlemenin amaçları dikkate alındığında, veri sahibini eksik olan kişisel verilerinin tamamlanmasını talep edebilir.

Düzeltmeyi talep etme hakkı verilerin hukuka uygun işlenmesine imkân sağladığından, veri sahipleri bu talepleri için herhangi bir neden belirtmek yükümlülüğü altında değildir.[597] Fakat, verilerin yanlışlığını veya eksikliğini gösterme noktasında ispat yükü veri sahibindedir.[598] Bu husus ile ilgili olarak AİHM'in *Ciubotaru v. Moldova*[599] kararı mevcuttur. Bu davada resmi kayıtlara Moldovalı etnik kimliğiyle kaydedilmiş olan başvurucu bunu Romanyalı olarak değiştirmek için talepte bulunmuş, fakat başvurucunun talebini kanıtlayamaması sebebiyle bu talep reddedilmiştir. Bu noktada, AİHM, devletlerin bir bireyin etnik kökeninin kaydını gerçekleştirirken nesnel kanıtların varlığını aramasını kabul edilebilir bulsa da söz konusu dava açısından başvurucu kendi

590 GDPR, m. 15(3).
591 **Giakoumopoulos/Buttarelli/O'Flaherty**, s. 218.
592 **Giakoumopoulos/Buttarelli/O'Flaherty**, s. 218.
593 ABAD, C-553/07, College van burgemeester en wethouders van Rotterdam v. M. E. E. Rijkeboer, 7 Mayıs 2009
594 **Giakoumopoulos/Buttarelli/O'Flaherty**, s. 218.
595 **Giakoumopoulos/Buttarelli/O'Flaherty**, s. 219.
596 GDPR, m. 16.
597 **Voigt/von dem Bussche**, s. 154, 155.
598 **Voigt/von dem Bussche**, s. 154.
599 AİHM, Ciubotaru v. Moldova, No. 27138/04, 27 April 2010, para. 51, 59.

etnik kimliğine ilişkin öznel bir düşünceden öte, Romanyalı etnik kökeninden insanlar ile arasında gerçekliği kanıtlanabilir bağlantıları zaten sunmuştur. Fakat, ulusal hukuk böyle bir durumda başvurucunun ebeveynlerinin Romanyalı etnik grubundan olduklarına dair kanıt sunulmasını aramaktadır. Moldova'nın tarihi düşünüldüğünde, böyle bir şart, Sovyet yetkililerinin kaydettiklerinden farklı bir etnik kimliğin kaydı için büyük bir engel oluşturmaktadır. Bu davada AİHM, Moldova'nın pozitif yükümlülüklerine uygun hareket etmeyerek başvurucunun özel hayata saygı hakkını ihlal ettiğine kanaat getirmiştir.[600]

Düzeltme hakkına ilişkin diğer bir husus ise, bu hakkın yalnızca "veri sahiplerine", "kendi kişisel verileri" ile ilgili tanınmış olduğudur. Buna göre, bir kişi, üçüncü bir kişinin kişisel verilerinin düzeltilmesi talebinde bulunamaz.[601]

D. Silinmeyi Talep Hakkı (Unutulma Hakkı)

Tüzükten önceki düzenlemelerde açık ve münhasır bir hak olarak yer almayan silinme hakkı, ilk olarak ABAD'ın *Google Spain*[602] kararı ile büyük dikkat çekmiş, daha sonra Tüzükte yer verilmek suretiyle güçlenmiştir.[603] Söz konusu *Google Spain* kararında, ABAD, Google'ın başvurucuya ilişkin güncel olmayan bilgileri silmek yükümlülüğü altında olup olmadığını incelemiştir. Bu davada, avukat olan başvurucu, sosyal güvenlik borçlarının yapılandırılması için mülkünü satmak zorunda kaldığına ilişkin bilgileri içerir gazete haberlerinin Google'da adı ile yapılan bir arama sonucu listelenmesinin 95/46/EC sayılı Direktif'e aykırılık teşkil ettiğini iddia etmiştir. Bu noktada ABAD, kişinin ismiyle yayınlanmış kişisel verilerinin geçersiz veya ilgisiz hale gelmesinden sonra ve artık bu verilerin işlenmesinin amaç için gerekli olmadığı halde, ilgili kişisel verilerin silinmesi gerektiğine hükmetmiştir.[604]

Bu hak çerçevesinde veri sahibinin kendisi ile ilgili kişisel verilerin herhangi bir gecikmeye mahal verilmeksizin silinmesini veri sorumlusundan talep etme hakkı bulunur. Buna bağlı olarak aşağıdaki hallerden birinin geçerli olması durumunda, veri sahibinin kişisel verileri herhangi bir gecikmeye mahal vermeksizin silme yükümlülüğü bulunur:

(a) kişisel verilerin toplanma veya işlenme amaçlarıyla ilişkili olarak artık gerekli olmaması,

---

600 **Giakoumopoulos/Buttarelli/O'Flaherty**, s. 219, 220.
601 **Giakoumopoulos/Buttarelli/O'Flaherty**, s. 155.
602 ABAD, C-131/12, Google Spain SL, Google Inc. v. Agencia Española de Protección de Datos (AEPD), Mario Costeja González [GC] ("Google Spain"), 13 Mayıs 2014.
603 Google Spain, s. 156.
604 **Dülger**, s. 167, 168.

(b) veri sahibinin işleme faaliyetinin dayandığı izni geri çekmesi ve işleme faaliyetiyle ilgili başka bir yasal gerekçe bulunmaması,

(c) veri sahibinin işleme faaliyetine itirazda bulunması ve işleme faaliyetine yönelik ağır basan meşru bir gerekçe bulunmaması,

(d) kişisel verilerin yasa dışı biçimde işlenmiş olması,

(e) veri sorumlusunun tabi olduğu Birlik veya üye devlet hukukundaki bir yasal yükümlülüğe uygunluk sağlanması amacı ile kişisel verilerin silinmesinin zorunlu olması,

(f) kişisel verilerin Tüzüğün 8(1) maddesinde atıfta bulunulan bilgi toplumu hizmetlerinin sağlanması ile ilgili toplanmış olması.[605]

Silinme hakkı kapsamında veri işlemenin hukuka uygun olduğunu ispat yükü, işleme faaliyetlerinin hukuka uygun olmasından sorumlu veri sorumlusundadır.[606] Ek olarak, hesap verebilirlik ilkesi gereğince veri sorumlusu daima veri işlemenin hukuki bir temele dayandığını gösterebilir durumda olmalıdır.[607]

Tüzük, silinmenin talep edilebilmesi hakkına bazı sınırlamalar getirmiştir. Buna göre, veriş işleme faaliyetinin:

(i) ifade ve bilgi edinme hakkının kullanılması,

(ii) veri sorumlusunun tabi olduğu Birlik veya üye devlet hukuku çerçevesinde işleme faaliyeti gerektiren bir yasal yükümlülüğe uygunluk acısından veya kamu yararına gerçekleştirilen bir görevin yerine getirilmesi veya veri sorumlusuna verilen resmi bir yetkinin uygulanması acısından,

(iii) halk sağlığı alanındaki kamu yararı sebeplerinden dolayı,

(iv) silinme hakkının ilgili işleme hedeflerinin yakalanmasını imkansız hale getirmesi veya yakalanmasına ciddi şekilde zarar vermesinin muhtemel olduğu ölçüde, kamu yararına arşivleme amaçları, bilimsel veya tarihi araştırma amaçları ya da istatistiki amaçlar doğrultusunda veya

(v) yasal iddialarda bulunulması, bu iddiaların uygulanması veya savunulması acısından gerekli olması halinde silinme talep edilemeyecektir.[608]

Veri sorumlusunun kişisel verileri kamuya açıklamış olduğu ve kişisel verileri silmek zorunda olduğu hallerde, veri sorumlusu, mevcut teknoloji ve uygulama maliyetini göz önünde bulundurarak, veri sahibinin silinmesini talep etmiş olduğu kişisel verileri isleyen diğer veri

605 GDPR, m. 17.
606 **Giakoumopoulos/Buttarelli/O'Flaherty**, s. 223.
607 **Giakoumopoulos/Buttarelli/O'Flaherty**, s. 223.
608 GDPR, m. 17(3).

sorumlularını silinme talebi hakkında bilgilendirmek üzere teknik tedbirler de dahil olmak üzere makul adımları atmalıdır.[609]

Bu hakka ilişkin olarak değinilmesi gereken son nokta ise, "unutulma hakkı" ve "silinme hakkının" aynı kavramlar olup olmadığına ilişkin bir tartışma mevcut olduğudur. Bu bağlamda, silinme hakkının yalnızca hukuka aykırı işleme, artık işleme amacı bakımından gereksiz olma gibi belirli durumların varlığı halinde, unutulma hakkının ise böyle bir sınırlama olmaksızın var olduğuna dair görüşler bulunmaktadır[610].

Bu makalede konuyu GDPR ekseninde ele aldığım için Tüzüğün konuya yaklaşımıyla paralel olarak silinmeyi talep etme hakkı ve unutulma hakkını aynı hak olarak incelemeye aldım. Tüzüğün 17. maddesi bu hakkı düzenlemekte ve hakkı *"silinmeyi talep etme hakkı (unutulma hakkı)"* olarak adlandırmaktadır. Bu nedenle esasen unutulma hakkının silinme hakkından daha kapsamlı ayrı bir hak olduğu yönündeki görüşü benimsemekle birlikte, GDPR eksenli bu makalemde de her iki hakkı ifade etmek için silinmeyi talep etme hakkı (unutulma hakkı) isim ve sınıflandırmasını kullandım.

E. İşlemenin Sınırlandırılması Hakkı

Tüzükte, belirli hallerin varlığı halinde, veri sahiplerinin, veri sorumlularının işletme faaliyetlerini geçici olarak kısıtlama hakları olduğu düzenlenmiştir.[611] Bu bağlamda sınırlamanın talep edilebileceği durumlar aşağıdaki gibidir:

(a) kişisel verilerin doğruluğuna veri sahibi tarafından itiraz edilmesi halinde, veri sahibinin kişisel verilerin doğruluğunu teyit etmesini sağlayan bir süre boyunca,

(b) işleme faaliyetinin yasa dışı olması ve veri sahibinin kişisel verilerin silinmesine itiraz etmesi ve bunun yerine verilerin kullanımının kısıtlanmasını talep etmesi,

(c) veri sahibinin işleme amaçlarına yönelik olarak artık kişisel verilere ihtiyaç duymaması, ancak veri sahibinin yasal iddialarda bulunulması, bu iddiaların uygulanması veya savunulması amacıyla söz konusu verilere ihtiyaç duyması,

(d) veri sorumlularının meşru gerekçelerinin veri sahibinin meşru gerekçelerine ağır basıp basmadığı doğrulanana kadar, veri sahibinin işleme faaliyetine itiraz etmesi.[612]

---

609 GDPR, m. 17(2).

610 Unutulma hakkı hakkında ayrıntılı bilgi için bkz. **Christina Markou**, "The Right to Be Forgotten: Ten Reasons Why It Should Be Forgotten", Law, Governence and Technology Series 20: Reforming Data Protection Law, Springer, 2015, ss. 203-226.

611 GDPR, m. 18.

612 GDPR, m. 18(1).

Veri işlemenin sınırlandırılmasının talep edildiği hallerde, bu hak, örneğin; seçilmiş verilerin geçici olarak başka bir işleme sistemine aktarılarak kullanıcıların bu verilere ulaşmasının engellenmesi, suretiyle kullanılabilir.[613]

Son olarak, veri sorumlusu, bir veri işleme faaliyetine ilişkin kısıtlamanın kaldırılmasından önce veri sahibini bu konuda bilgilendirmelidir.[614]

F. Veri Taşınabilirliği Hakkı

Veri taşınabilirliği hakkı, Tüzük ile birlikte veri sahiplerine tanınan, daha önce hiçbir belgede düzenlenmemiş bir haktır. Bu hak uyarınca, işleme faaliyetinin rızaya veya bir sözleşmeye dayanması veya işleme faaliyetinin otomatik yollarla gerçekleştirilmesi halinde, veri sahibinin kendisi ile ilgili olarak bir veri sorumlusuna sağlamış olduğu kişisel verileri yapılandırılmış, yaygın olarak kullanılan ve makine tarafından okunabilecek bir formatta alma hakkı vardır.[615] Veri sahiplerinin bu kişisel verileri, verilerin sağlandığı veri sorumlusunun herhangi bir engellemesi olmaksızın başka bir veri sorumlusuna iletme hakkı bulunur.[616]

Veri taşınabilirliği hakkının mevcut olduğu bir durumda, veri sahibinin, teknik açıdan uygulanabilir olması şartıyla, kişisel verilerini doğrudan bir veri sorumlusundan diğerine ilettirme hakkı bulunur.[617] Bu iletimi kolaylaştırmak için veri sorumluları birlikte çalışabilir formatlar geliştirmeli, böylece veri taşınabilirliği hakkının kullanılmasına olanak sağlamalıdır.[618]

Madde 29 Çalışma Grubunun rehberine göre, veri taşınabilirliği hakkı, veri sahibinin seçimini, kontrolünü ve güçlendirilmesini destekler; veri sahibine kendi kişisel verilerini kontrol etme imkânı tanır.[619] Buna göre, veri taşınabilirliği hakkı başlıca şu unsurlardan oluşur:

(a) veri sahiplerinin bir veri sorumlusu tarafından işlenen kendilerine ait kişisel verileri yapılandırılmış, yaygın olarak kullanılan ve makine tarafından okunabilecek bir formatta alma hakkı,

(b) kişisel verileri bir veri sorumlusundan diğerine, teknik olarak mümkün olması ihtimalinde, herhangi bir engelleme olmaksızın iletme hakkı,

---

613 **Giakoumopoulos/Buttarelli/O'Flaherty**, s. 227.
614 GDPR, m. 18(3).
615 GDPR, m. 20(1).
616 GDPR, m. 20(1).
617 GDPR, m. 20(2).
618 GDPR, Gerekçe 68.
619 Article 29 Working Party (2016), Guidelines on the right to data portability, WP 242, 13 Aralık 2016, 5 April 2017 (revize), s. 13.

(c) veri sahibinin veri taşıma talebi üzerine, veri sorumlusunun, veri sahibinin talimatları ile hareket etmesi rejimi,

(d) veri taşınabilirliği hakkının kullanılmasının diğer herhangi bir hakkı olumsuz yönde etkilememesi.[620]

G. İşlemeye İtiraz Hakkı

Veri sahibinin, kendi özel durumu ile ilgili gerekçelere dayalı olarak veya kişisel verilerinin doğrudan pazarlama amaçları doğrultusunda işlenmesi durumunda, söz konusu kişisel verinin işlenmesine itiraz hakkı bulunmaktadır.[621] Bu kapsamda, veri sahibinin veri işlemeye genel bir itiraz hakkı mevcut değildir.

Yukarıdaki ilk durum ile ilgili olarak, veri sahibi, kendi özel durumu ile ilgili gerekçelere dayalı olarak, işlemenin yasal dayanağını kamu yararı için gerçekleştirilen bir görevin ifası amacının veya veri sorumlusunun meşru menfaatlerinin oluşturduğu durumlarda, kendisi ile ilgili kişisel verilerin işlenmesine herhangi bir zamanda itiraz edebilir.[622] Veri sahibinin özel durumu ile ilgili gerekçelere dayalı olarak itiraz hakkının düzenlenmiş olmasının amacı, veri sahibinin veri koruma hakları ile diğer kişilerin veri işlemedeki meşru menfaatleri arasında bir denge kurulmasıdır.[623] Bu noktada ABAD, veri sahibinin haklarının, kural olarak, veri sorumlusunun ekonomik menfaatlerine üstün geldiğini belirtmiştir.[624] Ayrıca, Tüzükte, veri işlemeye devam edilmesini gerektiren hususların varlığına ilişkin ispat yükünün veri sorumlusunda olduğu açıkça düzenlenmiştir.[625] Veri sorumlusunun işleme faaliyetlerinin devamının gerekliliğini ispatlayamaması durumunda veri işlemeye devam etmesi mümkün değildir.[626]

Ayrıca, kişisel verilerin doğrudan pazarlama amaçları doğrultusunda işlenmesi durumunda ve doğrudan pazarlama ile alakalı olduğu ölçüde, veri sahibinin, kendisi ile ilgili kişisel verilerin söz konusu doğrudan pazarlama amacı ile işlenmesine herhangi bir zamanda ve ücretsiz olarak itiraz etme hakkı bulunur.[627]

---

620 **Giakoumopoulos/Buttarelli/O'Flaherty**, s. 229.
621 **Giakoumopoulos/Buttarelli/O'Flaherty**, s. 229.
622 GDPR, m. 21(1).
623 **Giakoumopoulos/Buttarelli/O'Flaherty**, s. 230.
624 Google Spain, para. 81.
625 GDPR, m. 21(1).
626 **Giakoumopoulos/Buttarelli/O'Flaherty**, s. 231; GDPR, m. 21(1).
627 GDPR, m. 21(2); **Giakoumopoulos/Buttarelli/O'Flaherty**, s. 231.

H. Yalnızca Otomatik İşleme Faaliyetine Dayalı Bir Karara Tabi Olmama Hakkı

Tüzük uyarınca, veri sahibinin kendisi ile ilgili hukuki sonuçlar doğuran veya benzer biçimde kendisini kayda değer şekilde etkileyen, profil çıkarma da dahil olmak üzere, yalnızca otomatik işleme faaliyetine dayalı bir karara tabi olmama hakkı bulunur.[628] Ancak, söz konusu işleme:

(i) veri sahibi ve bir veri sorumlusu arasında bir sözleşme yapılması veya uygulanması için gerekli ise veya,

(ii) veri sorumlusunun tabi olduğu ve veri sahibinin hakları ile özgürlükleri ve meşru menfaatlerinin güvence altına alınması amacıyla uygun tedbirlerin de belirtildiği Birlik veya üye devlet hukuku çerçevesinde işlemeye izin verilmiş ise veya,

(iii) veri sahibinin açık rızası mevcut ise,

bu şartlarda verilen bir karar yalnızca otomatik işlemeye dayalı olsa dahi hukuka aykırılık oluşturmaz.[629]

Madde 29 Çalışma Grubu, yalnızca otomatik işleme faaliyetine dayalı bir karara tabi olmama hakkının genel bir yasaklama hükmü olduğunu ve veri sahibinin böyle bir karara proaktif olarak itiraz etmesinin aranmadığını belirtmektedir.[630]

Değinilmesi gereken diğer bir nokta ise, yukarıda açıklandığı üzere, veri sahibinin bilgilendirilme hakkı kapsamında veri sorumlusunun ona sağlaması gereken bilgiler arasında profil çıkarma dahil olmak üzere otomatik karar vermenin varlığının da yer aldığıdır.[631] Ayrıca, erişim hakkı çerçevesinde, veri sahibinin, profil çıkarma da dahil olmak üzere otomatik karar vermenin varlığı ve bu hallerde yürütülen mantığa ilişkin anlamlı bilgilerin yanı sıra söz konusu işleme faaliyetinin veri sahibi acısından önemi ve öngörülen sonuçları hakkında bilgi talep etme hakkı mevcuttur.[632]

Bu hak uyarınca veri sorumlusu, en azından veri sorumlusu acısından insan müdahalesinin sağlanması hakkı başta olmak üzere, veri sahibinin kendi görüşünü ifade etme ve karara karşı çıkma yönündeki hakları ile özgürlükleri ve meşru menfaatlerinin güvence altına alınması amacı ile uygun tedbirler uygulamalıdır.[633] Daha önce bahsedildiği gibi, kişilerin verilerinin üzerinde kontrol

628 GDPR, m. 22(1).
629 GDPR, m. 22(2).
630 Article 29 Working Party, Guidelines on Automated Individual Decision-Making and profiling for the purposes of Regulation 2016/679, WP 251, 3 Ekim 2017, s. 15.
631 GDPR, m. 13(2)(f).
632 GDPR, m.15(1)(h).
633 GDPR, m. 22(3).

sağlayabilmeleri oldukça önemli ve Tüzük tarafından da dikkate alınmış bir husustur. Bu nedenle, karar mekanizmalarına insan müdahalesinin dahil olması, aksi durumda ortaya çıkabilecek olumsuz sonuçların önlenmesi açısından önem arz etmektedir.[634]

II. Kısıtlamalar

Veri sorumlusu veya işleyenin tabi olduğu Birlik veya Üye Devlet hukuku bir yasama tedbiri vasıtasıyla; temel haklar ve özgürlüklerin özüne saygı gösterilmesi ve demokratik bir toplumda aşağıdaki belirtilmiş hususların güvence altına alınması acısından gerekli ve orantılı bir tedbir teşkil etmesi durumunda öngörülen haklar ve yükümlülüklerin kapsamını kısıtlayabilir:

(a) milli güvenlik,

(b) savunma,

(c) kamu güvenliği,

(d) kamu güvenliğine yönelik tehditlere karşı güvence sağlanması ve bu tehditlerin önlenmesi de dâhil olmak üzere suçların önlenmesi, soruşturulması, tespiti veya kovuşturulması ya da cezaların infaz edilmesi,

(e) başta Birliğin veya bir Üye Devletin önemli bir ekonomik veya mali çıkarına olmak üzere parasal hususlar ile bütçe ve vergilendirmeye ilişkin hususlar, halk sağlığı ve sosyal güvenlik de dahil, Birlik ya da bir üye devletin genel kamu yararına yönelik diğer önemli hedefler,

(f) yargı bağımsızlığının ve adli süreçlerin korunması,

(g) düzenlenmiş, mesleklere ilişkin etik kurallarının ihlalinin önlenmesi, soruşturulması, tespiti ve kovuşturulması,

(h) nadiren olsa dahi, (a) ila (e) ve (g) bentlerinde belirtilen durumlarda resmi yetkinin kullanımı ile bağlantılı bir izleme, denetleme veya düzenleme işlevi,

(i) veri sahibinin veya başkalarının haklarının ve özgürlüklerinin korunması,

(j) medeni hukuktan kaynaklanan taleplere ilişkin kararların icrası.[635]

Kısıtlamalarla ilgili olarak getirilen yasama tedbirinde, ilgili işlemenin veya işleme kategorilerinin amaçları, kişisel veri kategorileri, getirilen kısıtlamaların kapsamı, kötüye kullanım veya yasa dışı yollarla erişim veya aktarımın engellenmesine yönelik güvenceler, veri sorumlusu veya veri sorumlusu kategorilerinin belirlenmesi, işleme veya işleme kategorilerinin mahiyeti, kapsamı ve amaçları dikkate alınarak saklama süreleri ve uygulanabilir güvenceler, veri

634 **Giakoumopoulos/Buttarelli/O'Flaherty**, s. 235.
635 GDPR, m. 23(1).

sahiplerinin hakları ve özgürlüklerine yönelik riskler ve kısıtlama amacına halel getirmemesi durumunda, veri sahiplerinin kısıtlamayla ilgili bilgi sahibi olma hakkı belirtilmelidir.[636]

III. Kanun Yolları, Sorumluluk, Cezalar ve Tazminat

A. Denetim Makamına Şikâyette Bulunma Hakkı

Her veri sahibi, kendisi ile alakalı kişisel verilerin işlenmesinin hukuka aykırı olarak gerçekleştiğini düşünmesi durumunda, başka bir idari veya adli çözüm yoluna halel gelmeksizin, yetkili denetim makamına şikâyette bulunma hakkına sahiptir.[637] Bu hak kapsamında, yetkili denetim makamı bir veri sahibi veya bir organ, kuruluş ya da bir birlik tarafından yapılan şikâyetleri ele almalı ve şikâyetin konusunu, uygun olduğu ölçüde, soruşturmalı ve özellikle daha ayrıntılı soruşturma ya da başka bir denetim makamı ile koordinasyonun gerekmesi durumunda, şikâyet sahibini soruşturmanın ilerlemesi ve sonucu konusunda makul bir süre içerisinde bilgilendirmelidir.[638] Tüzükte ayrıca denetim makamlarının bazı tedbirler alarak şikayetlerin sunulmasını kolaylaştırması gerektiği öngörülmüştür.[639]

Denetim makamı şikâyete ilişkin bir karar verdiğinde, her gerçek veya tüzel kişinin bu denetim makamının kendileriyle ilgili yasal *bağlayıcılığı* olan kararlarına karşı etkili bir kanun yoluna başvurma hakkı vardır.[640] Bu hak veri sahipleri için söz mevcut olduğu gibi, veri sorumluları ve işleyenler için de uygulama alanı bulur.[641]

B. Etkili Bir Kanun Yoluna Başvurma Hakkı

1. Genel Olarak

Etkili bir kanun yoluna başvurma hakkı hem AİHS hem AB Şartı altında temel haklardan biri olarak kabul edilmiş ve bu hakka büyük önem atfedilmiştir. Örneğin, *Schrems* davasında, ABAD, veri sahiplerinin kişisel verilerine erişimleri, kişisel verilerini düzeltmeleri veya silmeleri için herhangi bir kanun yolu öngörmeyen bir yasal düzenlemenin, AB Şartının 47. maddesinde düzenlenen *"etkili hukuki bir yola başvurma"* temel hakkının özünü zedeleyeceğine karar vermiştir.[642]

Yukarıda bahsedildiği üzere, denetim makamlarının *bağlayıcı* kararlarına karşı ilgili kişilerin kanun yoluna başvurma hakkı mevcuttur. Burada dikkat edilmesi gereken nokta, bu hakkın

---

636 GDPR, m. 23(2).
637 GDPR, m. 77(1).
638 GDPR, m. 57(1)(f).
639 GDPR, m. 57(2).
640 GDPR, m. 78(1).
641 **Giakoumopoulos/Buttarelli/O'Flaherty**, s. 238.
642 ABAD, C-362/14, Maximillian Schrems v. Data Protection Commissioner [GC], 6 Ekim 2015.

denetim makamının yalnızca "bağlayıcı" kararlarına karşı doğmasıdır.[643] Denetim makamının görüş bildirme gibi bağlayıcı olmayan kararlarına karşı ilgililer kanun yoluna başvuramayacaklardır.[644]

Tüzük uyarınca, kişisel verilerinin Tüzük'e aykırı bir şekilde işlenmesi sonucu bu Tüzük kapsamındaki haklarının ihlal edildiğini değerlendirdiği hallerde, her veri sahibi etkili bir kanun yoluna başvurma hakkına sahiptir.[645] Mevzubahis kanun yolunun "etkili" olabilmesi için veri sahiplerinin ilgili davayı açabilecekleri yetkili mahkemeler oldukça önem taşımaktadır; çünkü, veri sorumlusu veya veri sahiplerine dava açılabilecek mahkemelerin sınırlanması, veri sahiplerinin çeşitli zorluklarla karşılaşmasına sebebiyet verebilecektir.[646] Bu doğrultuda, Tüzükte bu davaların veri sorumlusu veya işleyenin bir işletmesinin ya da veri sahibinin mutat meskeninin bulunduğu üye devletin mahkemelerinde açılabileceği düzenlenmiştir.[647] Veri sahibi veya işleyenin, bir üye devletin kamu yetkilerinin kullanımı ile ilgili olarak hareket eden bir kamu kuruluşu olması halinde ise dava açılabilecek mahkemelere sınır getirilmiş ve bu kişilere ilişkin davaların söz konusu kuruluşun bulunduğu üye devletin mahkemelerinde açılacağı düzenlenmiştir.[648]

Ayrıca, (i) bir veri sahibi, veri sorumlusu, veri işleyen veya denetim makamının direkt ve bireysel olarak kendilerini ilgilendiren Avrupa Veri Koruma Kurulunun bir kararını iptal etmek amacıyla veya (ii) bir veri sahibinin herhangi bir AB kuruluş ve organın veri koruma hukukunu ihlal ettiği iddiasına dayanarak ABAD'a başvurma hakkı vardır. İkinci halde bu başvuru, ABAD'ın ilk derece mahkemesi olan AB Genel Mahkemesine (The General Court, EGC) yapılacaktır.[649]

2. Kar Amacı Gütmeyen Bir Organ, Kuruluş veya Birlik Tarafından Temsil Edilme Hakkı

Tüzüğün 80. maddesi uyarınca; veri sahiplerinin, bir Üye Devlet hukuku uyarınca düzgün şekilde kurulmuş, kamu yararına yasal hedefleri bulunan ve veri sahiplerinin kişisel verilerinin korunmasına ilişkin hakları ve özgürlüklerinin korunması alanında aktif olan kar amacı gütmeyen bir organ, kuruluş, veya birliğe, şikâyeti onun adına yapması, 77, 78 ve 79. maddelerde atıfta bulunulan hakları onun adına kullanması ve Üye Devlet hukukunda sağlanması koşuluyla, onun adına tazminat alma hakkını kullanma yetkisi verme hakkı bulunur.[650] Söz konusu organ, kuruluş,

643 **Giakoumopoulos/Buttarelli/O'Flaherty**, s. 239.
644 GDPR, Gerekçe 143.
645 GDPR, m. 79(1).
646 **Giakoumopoulos/Buttarelli/O'Flaherty**, s. 240.
647 GDPR, m. 79(2).
648 GDPR, m. 79(2).
649 **Giakoumopoulos/Buttarelli/O'Flaherty**, s. 240.
650 GDPR, m. 80(1).

veya birlik tarafından temsil edilme hakkı, bireylerin, onların uzmanlığından ve organizasyonel ve finansal kapasitelerinden faydalanmasına, dolayısıyla haklarını efektif olarak kullanılabilmesine olanak sağlar.[651]

C. Sorumluluk ve Tazminat

Etkili bir kanun yoluna başvurma hakkı, kişisel verileri hukuka aykırı olarak işlenen bireylerin böyle bir işleme sonucunda uğradıkları zararlar için tazminat talep edebilme hakkını içinde barındırır.[652] Tüzükte, Tüzüğe ilişkin bir ihlal sonucu *maddi veya manevi* zarar gören herhangi bir kişinin, yaşanan zarara ilişkin olarak veri sorumlusu veya işleyenden tazminat alma hakkına sahip olduğu açıkça düzenlenmiştir.[653] Bu maddedeki "zarar" kavramı, ABAD'ın içtihatları ışığında ve Tüzüğün amaçlarına uygun olarak geniş yorumlanmalıdır.[654]

Tüzük uyarınca, işleme faaliyetine müdahil herhangi bir veri sahibi Tüzüğü ihlal eden işleme faaliyetinin sebep olduğu zarardan sorumludur.[655] Bir veri işleyen ise ancak Tüzüğün özellikle veri işleyenlerine yönelik yükümlülüklerine uyum göstermediği veya veri sorumlusunun hukuka uygun talimatları dışında veya bu talimatlara aykırı hareket ettiği hallerde, işleme faaliyetinin sebep olduğu zarardan sorumludur.[656]

Birden fazla veri sorumlusu veya işleyenin ya da hem bir veri sorumlusu hem de bir veri işleyenin aynı işleme faaliyetinde bulunduğu ve işleme faaliyetinin sebep olduğu herhangi bir zarardan sorumlu olduğu hallerde, veri sahibinin etkili bir şekilde tazminin sağlanması amacıyla, her veri sorumlusu veya işleyenin tüm zarardan sorumlu tutulacağı Tüzükte düzenlenmiştir.[657] Fakat, böyle bir durumda, tek bir veri sorumlusu veya işleyen zararın tamamını tazmin ederse, bu veri sorumlusu ve işleyen aynı işleme faaliyetine müdahil diğer veri sorumlusu veya işleyenlerden zarardan sorumlu oldukları kısma tekabül eden tazminat kısmını isteyebilecektir.[658] Böyle bir düzenleme getirilmesinin nedeni tazminatın, uğranılan zarara ilişkin olarak "tam ve eksiksiz" olarak sağlanması oldukça önem teşkil eden bir husus olmasıdır.[659]

---

651 **Giakoumopoulos/Buttarelli/O'Flaherty**, s. 245.
652 **Giakoumopoulos/Buttarelli/O'Flaherty**, s. 246.
653 GDPR, m. 82(1).
654 GDPR, Gerekçe 146.
655 GDPR, m. 82(2).
656 GDPR, m. 82(2).
657 GDPR, m. 82(4).
658 GDPR, m. 82(5).
659 **Giakoumopoulos/Buttarelli/O'Flaherty**, s. 246.

Tüzükte ayrıca zarara sebep olan olaydan hiçbir şekilde sorumlu olmadığını kanıtlaması halinde, bir veri sorumlusu veya işleyenin bu sorumluluktan muaf tutulabileceği düzenlenmiştir.[660]

D. Cezalar

Tüzük, Üye Devletlerin denetim makamlarını Tüzüğün ihlal edilmesi halinde idari cezalar uygulamaları hususunda yetkilendirmiştir. Tüzük ile getirilen idari para cezalarına konu olabilme, yeni ve oldukça önemli bir düzenlemedir. Cezaların seviyeleri, yerel makamların ceza verip vermeme noktasında dikkat etmesi gereken durumlar, uygulanabilecek en yüksek ceza gibi konular Tüzükte açıkça düzenlenmiş olup, böylece AB içerisinde cezalara ilişkin olarak yeknesak bir sistem oluşturulması amaçlanmıştır.[661]

Tüzüğün getirdiği düzenlemeye göre; veri işlemenin temel ilkeleri ve rızanın koşullarına aykırılık, veri sahiplerinin haklarının ihlali ve Tüzüğün yurt dışına veri aktarımına ilişkin kurallarına uyulmaması durumunda, denetim makamları 20.000.000 Euro'ya kadar veya veri sorumlusu veya işleyenin bir teşebbüs olması halinde, bir önceki mali yılın yıllık dünya çapındaki cirosunun %4'üne kadar idari para cezası (hangi meblağ yüksek ise o geçerli olmak üzere) kesme yetkisi vardır.[662] Diğer ihlaller ile ilgili olarak ise denetim makamı 10.000.000 Euro'ya kadar veya veri sorumlusu veya işleyenin bir teşebbüs olması halinde, bir önceki mali yılın yıllık dünya çapındaki cirosunun %2'sine kadar idari para cezası (hangi meblağ yüksek ise o geçerlidir) kesebilecektir.[663]

Her münferit durumda, denetim makamı, bir idari para cezası kesilip kesilmeyeceğine ve idari para cezasının miktarına karar verirken, aşağıdaki hususları dikkate alır:

(a) ihlalin mahiyeti, ciddiyeti ve süresinin yanı sıra etkilenen veri sahibi sayısı ve veri sahiplerinin yaşadığı zarar düzeyi,

(b) ihlalin kasıtlı olması veya ihmalkârlıktan kaynaklanması,

(c) veri sahiplerinin yaşadığı zararın azaltılması için veri sorumlusu veya işleyen tarafından gerçekleştirilen herhangi bir işlem olup olmadığı,

(d) kendileri tarafından uygulanan teknik ve düzenlemeye ilişkin tedbirler dikkate alındığında, veri sorumlusu veya işleyenin sorumluluk derecesi,

(e) veri sorumlusu veya işleyenin geçmişte konuyla ilgili ihlalleri,

660 GDPR, m. 82(3).
661 **Giakoumopoulos/Buttarelli/O'Flaherty**, s. 247.
662 GDPR, m. 83(5); **Giakoumopoulos/Buttarelli/O'Flaherty**, s. 248.
663 GDPR, m. 83(4); **Giakoumopoulos/Buttarelli/O'Flaherty**, s. 248.

(f) ihlalin düzeltilmesi ve ihlalin olası olumsuz etkilerinin azaltılması amacı ile denetim makamı ile gerçekleştirilen işbirliği derecesi,

(g) ihlalden etkilenen kişisel veri kategorileri,

(h) veri sorumlusu veya işleyenin ihlali bildirip bildirmediği ve bildirdiyse ne ölçüde bildirdiği başta olmak üzere, denetim makamının ihlalden haberdar edilme şekli,

(i) aynı konu ile ilgili olarak daha önceden veri sorumlusu veya işleyene ilişkin alınmış tedbirlere uyum,

(j) onaylı davranış kurallarına veya onaylı belgelendirme mekanizmalarına uygun hareket edilip edilmemesi,

(k) ihlal nedeniyle doğrudan veya dolaylı olarak elde edilen maddi menfaatler veya kaçınılan zararlar gibi durumun özellikleri acısından geçerli diğer ağırlaştırıcı veya hafifletici faktörler.[664]

Ayrıca, denetim makamlarının idari para cezası kesme yetkileri dışında, çeşitli *"düzeltici"* yetkileri mevcuttur.[665] Örneğin; denetim makamları ihtarda bulunabilir, kınama cezası verebilir, bir işleme yasağı da dahil olmak üzere geçici veya kati bir sınırlama getirebilir.

Diğer bir önemli nokta ise, Tüzükte, Üye Devletler'in Tüzüğe ilişkin ihlaller acısından geçerli olan diğer cezalara ilişkin kurallar belirleyebileceği belirtilmiştir.[666] Buna göre, Üye Devletler, Tüzüğün ve Tüzük gereğince kabul edilen yerel düzenlemelerin ihlal edildiği durumlar için ceza verilmesine ilişkin kurallar düzenleyebilir.[667] Bu noktada dikkat edilmesi gereken, yerel hukuklarda getirilen düzenlemelerin aynı suçtan dolayı iki kere yargılama yapılamayacağı prensibini (*ne bis in idem*) ihlal etmemesi gerektiğidir.[668] Örneğin; Almanya'nın Federal Veri Koruma Yasasında (Bundesdatenschutzgesetz), bazı veri koruma kurallarının kasıtlı ihlalinin bir suç teşkil ettiğini düzenlenmiştir.[669] Örnek vermek gerekirse, çok sayıda veri sahibinin kamuya açık olmayan kişisel verilerinin hukuka aykırı olarak aktarılması durumunda para veya üç yıla kadar hapis cezası öngörülmüştür.

e. Güçlü İhlal Uygulamaları (Stronger Enforcement of Infringements)

664 GDPR, m. 83(2).
665 GDPR, m. 58.
666 GDPR, m. 84(1).
667 GDPR, Gerekçe 149.
668 GDPR, Gerekçe 149.
669 Bundesdatenschutzgesetz, m. 42.

GDPR ile getirilen en önemli yeniliklerden bir tanesi de sorumluluğun kapsamının genişletilmesi ile birlikte verilebilecek para cezalarının da dikkate değer şekilde artırılmış olmasıdır. GDPR düzenlemelerini ihlal eden şirketler yıllık 20 milyon Avro veya ihlalde bulunan şirketin bir önceki mali yılı, yıllık dünya çapındaki cirosunun % 4'üne kadar idari para cezasına tabi olma riski bulunmaktadır (GDPR, m. 83/5). Bu müeyyide hem veri sorumlusu hem veri işleyen şirketlere karşı uygulanabilecektir. Bir veri sorumlusu veya veri işleyenin aynı veya bağlantılı işleme faaliyetlerine yönelik olarak GDPR hükümlerini kasıtlı (intentionally) veya ihmalkârlıkla (negligently) ihlal etmesi durumunda, toplam idari para cezası meblağı en ağır ihlal için belirtilen 20 milyon Avro'yu aşamayacaktır (GDPR, m. 83/3 ve 83/5).

İdari para cezası kesilmesine karar verilirken ve para cezasının miktarı belirlenirken şu hususlar dikkate alınacaktır:

i. İlgili işleme faaliyetinin niteliği, kapsamı, amacı dikkate alındığında ihlalin niteliği, ciddiyeti ve süresinin yanı sıra etkilenen veri sahibi sayısı ve veri sahiplerinin yaşadığı zarar düzeyi,

ii. İhlalin kasıt veya ihmal ile işlenmesi durumu,

iii. Veri sahiplerinin zararının azaltılması için veri sorumlusu veya işleyen tarafından gerçekleştirilen işlemler,

iv. GDPR 25 ve 32. maddeleri uyarınca uygulanan teknik ve organizasyona ilişkin tedbirler göz önünde bulundurulmak suretiyle, veri sorumlusu veya işleyenin sorumluluk derecesi,

v. Veri sorumlusu veya işleyenin geçmişte konuyla ilgili diğer ihlal durumları,

vi. İhlalin düzeltilmesi ve ihlalin olası olumsuz etkilerinin azaltılması amacı ile denetim makamı ile gerçekleştirilen iş birliği derecesi,

vii. İhlalden etkilenen kişisel veri kategorileri,

viii. Veri sorumlusu veya işleyenin ihlali bildirip bildirmediği, denetim makamının ihlalden haberdar edilme şekli,

ix. GDPR 58/2 maddesine uygun alınan diğer tedbirlere uyum durumu,

x. İhlal nedeniyle doğrudan veya dolaylı olarak elde edilen maddi menfaatler veya kaçınılan zararlar gibi halin icabına göre geçerli diğer ağırlaştırıcı ve hafifletici nedenler,

xi. Veri sorumlusu / işleyenin GDPR 40 ve 42. maddelerinde düzenlenen onaylı belgelendirme mekanizmalarına uygun hareket edip etmedikleri.

Her denetim makamı, 83. maddede sayılan idari para cezaları verilmesinin, her münferit durumda etkin (effective), orantılı (proportionate) ve caydırıcı (dissuasive) olmasını sağlamakla yükümlü tutulmuştur (GDPR, m. 83/1).

GDPR ile şirketlerin durumunu ağırlaştıran bir diğer husus da, veri sorumlusu şirket/işleyenlerin veri işlemenin rızaya dayandığı hallerde, rızanın varlığını ispat ile yükümlü tutulmalarıdır (GDPR, m. 7/1, rec. 42). Veri sorumlusu ayrıca GDPR'ın 5/1. maddesinde düzenlenen ilkelere uygun davrandığını ortaya koymakla yükümlü tutulmuştur (GDPR, m. 5/2, rec. 24). Bu hususların da GDPR ile getirilen güçlü ihlal araçlarını tamamlayıcı nitelikte olduğu söylenebilir.

GDPR ihlalinden dolayı ilk para cezaları da verilmeye başlamıştır. Avusturya'da bir bahis şirketi, güvenlik nedeniyle koyduğu kameranın görüş açısının geniş olması ve GDPR kapsamında korunan kamuyu görüntülemesi nedeni ile 4800 Euro; Portekiz'de bir hastane kendi çalışanı olmadığı halde 985 fizik tedavi doktoruna ait aktif bilgileri barındırması nedeni ile bilgi güvenilirliği, bütünlüğü ve asgari düzeyde veri işleme ilkelerine aykırı davranmak nedeni ile iki kez 150.000 Euro ve bir kez 100.000 Euro para cezası ile cezalandırılmıştır. Son olarak Almanya'da Knuddels.de sosyal ağ şirketi, 1.8 milyon kayıtlı kullanıcısına ait e-posta ile kullanıcı adı ve şifrelerinin sızdırılması nedeni ile 20.000 Euro para cezası ile cezalandırılmıştır.[670]

§ 6. Avrupa Birliği Genel Veri Koruma Tüzüğünün Uygulanması

Yukarıda detaylıca açıklandığı üzere, Tüzüğün oldukça geniş bir uygulama alanı vardır ve Tüzük oldukça geniş ve ayrıntılı haklar tanımış ve sorumluluklar yüklemiştir. Tüzüğün kurduğu bu sistemin uygulamadaki yansımasının etkili olarak gerçekleştirilmesi büyük önem taşımaktadır.

Bu bağlamda, Tüzüğün getirdiği düzenlemelerin uygulamaya konması için dört aşamalı bir yaklaşım izlenmesinin faydalı bir hareket biçimi olacağı düşünülmektedir. Bu dört aşama:

(1) boşluk analizi,

(2) risk analizi,

(3) proje idaresi ve kaynak/bütçe planlaması ve

(4) uygulamaya koymadır.[671]

Bu yaklaşım kısmen, uygulamaya koyma aşamalarını zaman ve kapsamlarına göre sınırlanmış farklı aşamalara ayıran Şelale Modelini (Waterfall Model) temel almaktadır.[672] Bir

---

670 How much are the first fines for GDPR infringement, December 12, 2018, https://www.pandasecurity.com/mediacenter/news/first-sanctions-gdpr-infractions/ (Son Erişim Tarihi: 15.03.2019)

671 **Voigt/von dem Bussche**, s. 245.

672 **Voigt/von dem Bussche**, s. 246.

işleme faaliyetinin çeşitli Üye Devleri etkilemesi halinde ise, veri koruma sistemini yerel özelliklere uyarlamak amacıyla, beşinci bir aşama gerekli olabilecektir.[673]

I. Birinci Adım: Boşluk Analizi

İlk adım olarak, ilgili kuruluş, kendisinin hali hazırda mevcut olan veri koruma standartlarını analiz etmeli ve bunları Tüzük kapsamında gerekli yükümlülükleri karşılamak için gerekenlerle karşılaştırmalıdır. Bunun için, bu kuruluşun farklı departmanlardaki veri işlemeden sorumlu kişiler değerlendirme aşamasına dahil edilmelidir. Mevzubahis analiz çalıştay, karşılıklı görüşme ve öz değerlendirme gibi farklı şekillerde gerçekleştirebilir; bu noktada önemli olan ise ne tür işleme faaliyetlerinin hangi amaçlarla gerçekleştirildiği, hangi tür verilerin işlendiği, kuruluş içindeki sorumluluklarının nasıl dağıldığı ve ne gibi güvenceler alındığı konularının üzerinde durulmasıdır.[674]

Boşluk analizi yapılırken, ilgili kuruluşun spesifik olarak gerçekleştirdiği veri işleme faaliyetleri ve bu tür işlemeler için Tüzük tarafından getirilen yükümlülükler dikkate alınmalıdır. Bu aşamanın tamamlanması için, kuruluş, kendi veri koruma standartları ile olması gerekenleri kıyaslayacak ve veri korumasına ilişkin boşlukları tespit edecektir. [675] Bu boşluk, diğer aşamalarda giderilmeye çalışılacaktır.

II. İkinci Adım: Risk Analizi

Yukarıda pek çok defa bahsedildiği üzere, veri işleme faaliyetinin veri sahiplerinin hak ve özgürlükleri açısından taşıdığı risk miktarı, sorumlulukların belirlenmesi açısından üzerinde oldukça durulmuş bir değişkendir. Bu bağlamda, kuruluşlar farklı departmanları incelemeli ve bu departmanlardaki veri işleme faaliyetlerinin risk dereceleri ortaya konulmalıdır. Bu noktada, özellikle, veri sahiplerinin hakları ve özgürlükleri açısından en çok risk barındıran ve yüksek miktarlı cezalara sebebiyet verme ihtimali en yüksek olan veri işleme faaliyetleri üzerinde durulmalıdır.[676]

Bu aşamanın tamamlanması için, ilgili kuruluş, kendisinin çeşitli işleme faaliyetlerinin taşıdığı riskleri de dikkate alarak, tespit edilmiş veri koruma boşluğu doğrultusunda yeni veri koruma standartlarının uygulamaya konulması amacıyla bir stratejik proje taslağı hazırlamalıdır.[677]

673 **Voigt/von dem Bussche**, s. 246.
674 **Voigt/von dem Bussche**, s. 246.
675 **Voigt/von dem Bussche**, s. 246.
676 **Voigt/von dem Bussche**, s. 247.
677 **Voigt/von dem Bussche**, s. 247.

III. Üçüncü Adım: Proje İdaresi ve Kaynak/Bütçe Planlaması

Söz konusu proje planı üzerinden, Tüzüğün hükümlerinin uygulanmaya konulması amacıyla kuruluş genelinde bir veri koruma organizasyonu oluşturmalıdır. Bu çerçevede, mevzubahis organizasyon, yeniden yapılanma için gerekli bütçe ve kaynakları, yasal masraflar, BT masrafları ve çalışan ihtiyacı da dahil olmak, üzere dikkate almalıdır. Bu noktada hali hazırda bir veri koruma görevlisinin var olması oldukça yarar sağlayabilecektir.[678]

Kuruluş, en çok etkilenen alanlardaki kilit mevkideki personellere projeye ilişkin sorumluluklar tahsis etmelidir. Uygun olduğunda, AB görevlileri tarafından bir "baş" proje müdürü atanacaktır. Baş proje müdürü, veri koruma hakkında uzman bilgisine sahip bağımsız bir danışman olabilir.[679]

Bu aşamanın tamamlanması için, veri koruma kavramı kesinlik kazanmalıdır.[680]

IV. Dördüncü Adım: Uygulamaya Koyma

Son aşamada, Tüzük ile uyum içerisindeki yeni veri koruma standartları, bir önceki aşamada kesinlik kazandırılan veri koruma kavramı uyarınca uygulamaya konulacaktır. Kuruluşun yönetimi, farklı departmanların işleme faaliyetlerinin yeni standartlara uygunluğunun sağlanması noktasında proje müdürlerine yardım edeceklerdir.[681] Kuruluş bünyesinde farkındalık yaratılması ve çalışanların veri işleme faaliyetlerini hukuka uygun olarak gerçekleştirmeleri hususunda eğitilmeleri için çalıştay organize edilmesi faydalı bir yöntem olarak görülmektedir.[682]

Bu aşamanın tamamlanması için, yeni veri işleme standartları başarılı bir şekilde uygulamaya konulmuş ve kuruluşun olağan işleyişinin bir parçası haline gelmiş olmalıdır.[683] Tüzük ile uyumluluğun sağlanabilmesi için bu aşamadan sonra da veri işleme faaliyetleri sürekli olarak izlenmeli ve bu standartlar devam ettirilmelidir.[684]

V. Beşinci Adım: Ek Ulusal Gereklilikler

Tüzük, veri korumasına ilişkin kuralların belirlenmesi noktasında devletlere önemli ölçüde takdir marjı bırakmaktadır. Dolayısıyla, Üye Devletler, ek veri koruma gerekliliklerini düzenleyebileceklerdir.[685] Bu noktada, birden çok AB Üyesi Devlette veri işleme faaliyeti

678 **Voigt/von dem Bussche**, s. 247.
679 **Voigt/von dem Bussche**, s. 247.
680 **Voigt/von dem Bussche**, s. 247.
681 **Voigt/von dem Bussche**, s. 247.
682 **Voigt/von dem Bussche**, s. 247.
683 **Voigt/von dem Bussche**, s. 248.
684 **Voigt/von dem Bussche**, s. 248.
685 **Voigt/von dem Bussche**, s. 249.

gerçekleştiren veya birden çok AB Üyesi Devleti etkileyen kuruluşlar, farklı ulusal mevzuatlardan etkilenip etkilenmeyeceklerini tespit etmelidir.[686]

SONUÇ

GDPR, AB veri koruma rejiminin elden geçirilmesi ve modernleştirilmesidir. Bireyler açısından yeni koruma ve güvence mekanizmaları getiren bu yeni araç, her gün sayısız veri işleyen, depolayan ve kullanıcılara sunan şirketler açısından ise yeni yükümlülükler getirmektedir. Üstelik GDPR'ın genişleyen uygulama alanı nedeniyle sadece AB'de yerleşik şirketler değil, AB dışındaki şirketler açısından da bu yeni duruma uyum sağlamak zorunlu bir hâl almıştır.

Makalenin I. Bölüm'ünde "kişisel verilerin korunması hakkı"nın gelişimi, uluslararası düzenlemelerde nasıl yer aldığı incelenerek değerlendirilmeye çalışılmıştır. Bu çerçevede, bu hakkın yeni bir hak olmadığı fakat münhasır bir hak olarak anlaşılması ve düzenlenmesinin teknolojik gelişmeler ve dijital çağın gerekleri ile birlikte ortaya çıktığını söylemek mümkündür. Kişisel verilerin korunması ile ilgili en güncel ve en detaylı düzenleme 25 Mayıs 2018'de yürürlüğe giren Avrupa Birliği Genel Veri Koruma Tüzüğüdür. Bu Tüzük ile kişisel verilerin korunması hukukunun AB'de yeknesaklaştırılması amaçlanmış olup, Tüzük makalenin II. Bölüm'ünde detaylıca incelenmiştir.

Bu makalenin II. Bölüm'ünde 2016/679 sayılı Avrupa Birliği Genel Veri Koruma Tüzüğü kişisel verilerin korumasına ilişkin kavramların tanımı, Tüzüğün uygulama alanı, getirdiği yenilikler, yer verdiği ilkeler, getirdiği güvenceler, yüklediği sorumluluklar, kurduğu sistem ve bu sistemin nasıl uygulamaya konulabileceği detaylıca ve bir bütün olarak incelenmiştir. İlk bakışta Tüzüğün genelinde fark edilebilen ve onu önceki düzenlemelerden ayıran en önemli farklılık, Tüzüğün AB'de kişisel verilerin korunması hukukunun yeknesaklaştırılması amacıyla oldukça ayrıntılı ve etkili bir sistem kurma çabasıdır.

Tüzük, bu hedeften yola çıkarak hem tamamen yeni düzenlemelere yer vermiş, hem de daha önceden var olan düzenlemeleri daha somut ve detaylı olarak düzenlemiştir. Bu doğrultuda öncelikle Tüzüğün bölgesel kapsamı artırılmış ve belirli hallerde Tüzüğün AB dışındaki ülkelere de uygulanabilir olduğu öngörülmüştür. Kapsamın artırılmasının yana sıra, genel olarak hukuki bir işleme faaliyetinden bahsedebilmek için gereken şartlar ağırlaştırılmış ve veri sahiplerine yeni haklar tanınmış ve veri sahiplerinin önceden mevcut hakları genişletilmiştir. Bu doğrultuda Tüzük ile birlikte "unutulma hakkı" ve "veri taşınabilirliği hakkı" ilk kez yasal bir zeminde

686 **Voigt/von dem Bussche**, s. 249.

düzenlenmiştir. Ayrıca genel itibariyle veri sorumluları ve işleyenlerin yükümlülükleri arttırılmış ve somutlaştırılmıştır. Bu kapsamda, belirli durumlarda, veri sorumlularının veri koruma kurallarına uygun faaliyet göstermesi hususunda onlara bilgi ve tavsiye verecek veri koruma görevlileri atanması gerekliliği ilk kez açık olarak düzenlenmiştir. İlaveten, kişisel verileri ihlalinin ortaya çıkması durumunda veri sorumlularına ve veri işleyenlere bu ihlali denetim makamı ve ilgililere bildirme yükümlülüğünün öngörülmüş olması Tüzük ile getirilen önemli bir yeniliktir. Son olarak değinilmesi gereken başka bir yenilik ise, Üye Devletlerin denetim makamlarının Tüzüğün ihlal edilmesi halinde idari cezalar uygulamaları hususunda yetkilendirilmiş olmasıdır. Bu noktada ihlal halinde kesilebilecek cezaların oldukça yüksek düzenlenmiş olması da dikkat çeken bir noktadır.

GDPR'ın 83. maddesiyle benimsenen ağır idari para cezaları da dikkate alındığında, tüm veri işleyenlerin, özellikle şirketlerin GDPR uyumluluğunun sağlanmasının önemi daha açık şekilde ortaya çıkmaktadır.

Sonuç olarak, Tüzük, genel anlamıyla, AB'de yeknesak bir kişisel verilerin korunması hukuku oluşturmak amacıyla, var olanlara kıyasla daha kapsamlı ve detaylı bir sistem kurmuş, hükümlere aykırılıklar içinse oldukça ağır cezalar öngörmüştür. Anlatılan amaçlar düşünüldüğünde, 96/46/EC sayılı Direktif'ten temel alınarak tasarlanmış ve Tüzüğün onaylanmasından kısa bir süre önce yürürlüğe girmiş 6698 sayılı KVKK'nın, Tüzük baz alınarak geliştirilmesi oldukça faydalı olacaktır.

KAYNAKÇA

Albrecht, Jan Philipp, "How The GDPR Will Change The World", Eur. Data Prot. L. Rev. 287, 2016.

Bhatia, Punit, Contents of Data Protection Policy according to GDPR, https://advisera.com/eugdpracademy/knowledgebase/contents-of-the-data-protection-policy-according-to-gdpr/ (Son Erişim Tarihi: 18.03.2019).

de Hert, Paul/Michal Czerniawski, "Expanding the European Data Protection Scope beyond Territory: Article 3 of the General Data Protection Regulation in its Wider Context", International Data Privacy Law, V. 6, No. 3, 2016.

Develioğlu, Hüseyin Murat, 6698 sayılı Kişisel Verilerin Korunması Kanunu ile Karşılaştırmalı Olarak Avrupa Birliği Genel Veri Koruma Tüzüğü Uyarınca Kişisel Verilerin Korunması Hukuku, On İki Levha Yayıncılık, İstanbul, 2017.

Dülger, Murat Volkan, Kişisel Verilerin Korunması Hukuku, Hukuk Akademisi, İstanbul, 2019.

Elliman, Dave, GDPR: It is time to rethink your approach to privacy, August 11, 2017, https://www.thoughtworks.com/insights/blog/gdpr-it-s-time-rethink-your-approach-privacy

Fernandes, Mário /Alberto Rodrigues da Silva/António Gonçalves, "Specification of Personal Data Protection Requirements: Analysis of Legal Requirements based on the GDPR Regulation", https://www.researchgate.net/profile/Mario_Fernandes14/ publication/ (Son erişim tarihi: 19.07.2019).

Fritz, Gernot/Nadja Paulus, "CJEU rules on joint controllership – what does this mean for companies?", Freshfields Bruckhaus Deringer LLP, https://digital.freshfields.com/post/102f0aw/cjeu-rules-on-joint-controllership-what-does-this-mean-for-companies, (Son erişim: 19.07.2019).

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

Guzman, Andrew T./Timothy L. Meyer, International Soft Law, Journal of Legal Analysis, Volume 2, Issue 1, Spring 2010.

Hintze, Mike/Khaled El Emam, "Comparing the benefits of pseudonymisation and anonymisation under the GDPR", Journal of Data Protection & Privacy, Volume 2, Number 2, Autumn 2018.

Kuner, Christopher, The European Commission's Proposed Data Protection Regulation: A Copernican Revolution in European Data Protection Law, Privacy and Security Law Report, June 2012, http://robertgrzeszczak.bio.wpia.uw.edu.pl/files/2012/12/Kuner_A-Copernican-Revolution-in-European-Data-Protection-Law.pdf (Son Erişim Tarihi: 10.02.2019).

Madge, Robert, Five Loopholes in the GDPR, August 27, 2017, https://medium.com/mydata/five-loopholes-in-the-gdpr-367443c4248b (Son Erişim Tarihi: 20.03.2019).

Markou, Christina, "The Right to Be Forgotten: Ten Reasons Why It Should Be Forgotten", Law, Governence and Technology Series 20: Reforming Data Protection Law, Springer, 2015.

Politou, Eugenia/Efthimios Alepis/Constantinos Patsakis, "Forgetting Personal Data and Revoking Consent under the GDPR: Challenges and Proposed Solutions", Journal of Cybersecurity, V. 4, I. 1, January 2018.

Ragep, F. Jamil, "Copernicus and His Islamic Predecessors: Some Historical Remarks", Mc. Gill University, History of Science Journal, N. XLV, 2007.

Soysal, Tamer, Tarımda Biyoteknoloji Uygulamaları ve Patent Hakları (Agricultural Biotech Patent Law), Adalet Yayınevi, 2019.

Tapan, Mehmet Nuri, "Avrupa Birliği (AB) Hukukunun Kaynakları ve Ulusal Hukuka Etkileri: Avrupa Adalet Divanı", Türkiye Barolar Birliği Dergisi, S. 3, Y. 1998.

Üzeltürk, Hakan, Avrupa Birliği Genel Veri Koruma Düzenlemesi, Yeditepe Üniversitesi Hukuk Fakültesi Dergisi, C. XV, S. 2, İstanbul, 2018.

Voigt, Paul /Axel von dem Bussche, The EU GDPR: A Practi cal Guide, Springer, Heidelberg, 2017.