T.C.
KIRIKKALE ÜNİVERSİTESİ
SOSYAL BİLİMLER ENSTİTÜSÜ
HUKUK ANABİLİM DALI
KAMU HUKUKU BİLİM DALI

Kişisel Verilerin KVKK ve GDPR Kapsamında Korunması
Yüksek Lisans Tezi

Hazırlayan

Yüksel TOLUN

Danışman

Doç. Dr. İslam Safa KAYA

Haziran - 2020
KIRIKKALE

T.C.
KIRIKKALE ÜNİVERSİTESİ
SOSYAL BİLİMLER ENSTİTÜSÜ
HUKUK ANABİLİM DALI
KAMU HUKUKU BİLİM DALI

Kişisel Verilerin KVKK ve GDPR Kapsamında Korunması

Yüksek Lisans Tezi

Hazırlayan

Yüksel TOLUN

Danışman

Doç. Dr. İslam Safa KAYA

Haziran - 2020
KIRIKKALE

KABUL-ONAY

Doç. Dr. İslam Safa Kaya danışmanlığında Yüksel Tolun tarafından hazırlanan “Kişisel Verilerin KVKK ve GDPR Kapsamında Korunması” adlı bu çalışma jürimiz tarafından Kırıkkale Üniversitesi Sosyal Bilimler Enstitüsü Hukuk Anabilim dalında yüksek lisans tezi olarak kabul edilmiştir.

../../2020

(Başkan)

Doç. Dr. Burak Adıgüzel

Doç. Dr. İslam Safa Kaya

Dr. Öğr. Üyesi Hamdi Gökçe Zabunoğlu

Yukarıdaki imzaların adı geçen öğretim üyelerine ait olduğunu onaylarım.

../../2020

Enstitü Müdürü

Yüksek Lisans Tezi olarak sunduğum “Kişisel Verilerin KVKK ve GDPR Kapsamında Korunması” adlı çalışmanın, tarafımdan bilimsel ahlak ve geleneklere aykırı düşecek bir yardıma başvurmaksızın yazıldığını ve faydalandığım eserlerin kaynakçada gösterilenlerden oluştuğunu, bunlara atıf yapılarak faydalanılmış olduğunu beyan ederim.

../../2020

Yüksel Tolun

ÖNSÖZ

Dijital dünyada harcadığımız zamanın giderek artması neticesinde temel hak ve özgürlüklerimizden olan kişilik hakkının ve özel hayatın gizliliğini talep etme haklarımızın internet üzerinde daha da önemli hale geldiğini görüyoruz. Zira özellikle otomatik sistemler ile yapılan kişisel veri işleme faaliyetleri zaman zaman bizleri fazlasıyla iyi tanıyarak alışveriş alışkanlıklarımıza etki edebilmektedir. Bu teknolojilerin kötüye kullanımı neticesinde doğabilecek kötü sonuçların ortaya çıkmasını engellemek ve kişilerin kişisel verileri üzerindeki hakimiyetlerini arttırmak için bazı koruyucu önlemler getirmek zaruri bir ihtiyaç haline gelmiştir.

Bu çalışmada kişisel verilerin korunması alanında ülkemizde en çok uygulama alanı bulacağına inandığımız 2 düzenlemenin içeriği ve aralarındaki farklara yönelik incelemeler yapılmıştır. Çalışmanın hazırlanmasında gerek yurt içinde gerek yurt dışında hem kişisel verilerin korunmasına yönelik düzenlemelere ilişkin danışmanlık ve temsil hizmetleri veren avukatlarla hem de kişisel veri işleme yaparak gelir sağlayan teknoloji firmalarının teknik elemanları ile istişare edilerek çalışmanın hem akademik açıdan hem de pragmatik açıdan faydalı olması hedeflenmiştir.

Hayatımın her döneminde olduğu gibi çalışmam hazırlanması esnasında da beni yalnız bırakmayan annem Elif Tolun ve babam Orhan Tolun'a verdikleri manevi destekten dolayı sevgi ve saygılarımı sunar, lisans yıllarından beri tanıdığım ve örnek aldığım Doç. Dr. İslam Safa Kaya'ya sorularımın hiçbirini cevapsız bırakmadığı ve sabırla bana destek verdiği için teşekkür ederim.

Yüksel Tolun

ÖZET

İnternetin günlük yaşantımızda kapladığı yerin her geçen gün artması ve kullanıcılar olarak sıklıkla kullandığımız yazılımlara ücretsiz biçimde erişmenin rahatlığına alışmamız sebebi ile kişisel verilerin korunması alanı giderek önem kazanmaktadır. Zira internetteki birçok hizmetin ücretsiz olarak sunulması ancak kullanıcıların yani bizlerin kişisel verilerinin, ürünün sahibi tarafından toplanması ve işlenmesi yoluyla gelir elde edilmesi ile mümkün olmaktadır. Her ne kadar burada iki tarafın da kabul ettiği bir anlaşma var gibi gözükse de aslında kullanıcıların kişisel verilerinin işlenmesine yönelik faaliyetlerden ciddi oranda zarar görmelerinin mümkün olması ve çoğunlukla kullanıcıların bu zararı öngöremeyecek olmaları sebebiyle kişisel verilerin işlenmesinin hukuk düzeni tarafından düzenlenmesi gerekmektedir. Bu bağlamda karşımıza çıkan en bilindik düzenleme, internetin küresel yapısının da etkisi ile oldukça geniş bir kapsama sahip olan GDPR'dir. Ülkemizde ise 6698 Sayılı Kişisel Verilerin Korunması Hakkındaki Kanun, bu alanı düzenlemekte ve vatandaşlarımızın kişisel verilerini korumaktadır. Bu iki düzenlemenin farkları ile beraber irdelenmesi, özellikle küresel boyutta veri işleme faaliyeti yapmak isteyen gerçek ve tüzel kişilere yol göstermesi bakımından önem arz etmektedir.

Anahtar Kelimeler: kişisel verilerin korunması, veri işlemenin düzenlenmesi, GDPR, Kişisel Verilerin Korunması Kanunu, özel hayatın gizliliği hakkı

ABSTRACT

Protection of personal data gains more and more importance as the internet occupies more of our daily lives and we, as users, get more accustomed to using our favorite software without a fee. Most of the free software online are only available because the company who makes the product collects and processes the personal information of their users to make profit. Even though it seems like there's a win-win agreement here, the users are often unaware of the risks that can occur due to their personal information being processed. That's why law needs to regulate the field of processing personal data. When it comes to personal data protecting regulations, the most famous one is European Union Global Data Protection Regulation. In Turkey, Personal Data Protection Law is currently regulating this field. Reviewing these two regulations together and focusing on their differences can guide any person who wants to process personal data on a global scale.

Keywords: personal data protection, regulations regarding data processing, European Union Global Data Protection Regulation, Personal Data Protection Law, right to privacy

KISALTMALAR

AB	Avrupa Birliği
ABAD	Avrupa Birliği Adalet Divanı
AEA	Avrupa Ekonomik Alanı
AİHM	Avrupa İnsan Hakları Mahkemesi
AİHS	Avrupa İnsan Hakları Sözleşmesi
BKK	Bağlayıcı Kurumsal Kurallar
BM	Birleşmiş Milletler
CNIL	Commission Nationale De L'informatique Et Des Libertés
CSV	Comma Separated Values
GDPR	Global Data Protection Regulation
JSON	JavaScript Object Notation
KEP	Kayıtlı E-posta Adresi
KVKK	Kişisel Verileri Koruma Kanunu
OECD	Organisation for Economic Co-operation and Development
SIS	Schengen Information System
TBK	Türk Borçlar Kanunu
TCK	Türk Ceza Kanunu
TMK	Türk Medeni Kanunu
XML	Extensible Markup Language

TABLOLAR

İÇİNDEKİLER

GİRİŞ

İnternetin hayatımızda her geçen gün daha fazla yer kaplaması ile beraber internet kullanıcılarının kişisel verileri işlenerek kar sağlanabilir hale gelmiştir. Daha önceleri edinmesi zor veya maliyetli olan kişisel verileri toplamayı ve işlemeyi kolaylaştıran araçların sayısının artması ile bu araçlar ucuz ve kolay biçimde elde edilebilir hale gelmişlerdir. Bunun doğal bir sonucu olarak bahse konu verilerin Türk vatandaşlarının kişilik haklarına zarar vermek için kullanılması da kolaylaşmıştır. Tüm dünyada olduğu gibi ülkemizde de kişilik haklarına zarar verme ihtimali olan gelişmeler ile bu gelişmelere karşı kişileri korumaya yönelik fikir ve önlemler eş zamanlı olarak ortaya çıkmıştır.[1]

Türkiye, Avrupa Konseyi, Birleşmiş Milletler (BM) ve Ekonomik Kalkınma ve İşbirliği Örgütü (OECD) de dahil olmak üzere çok sayıda uluslararası örgüte üyedir. Bu nedenle kişisel verilerin korunması için bir kanun çıkarılması yönünde ihtiyacın ortaya çıkmasında teknolojik gereksinimlerin yanı sıra uluslararası iş birliklerinin sürdürülmek istenmesinin de etkisi büyüktür. Zira gerek Avrupa Konseyi gerekse OECD, kişisel verilerin korunması konusunda düzenlemeler getirmiş ancak Türkiye bu uluslararası sözleşmelere imza atmasına karşın, bunları onaylayarak iç hukukunda yürürlüğe sokmamıştır.[2] Türkiye tarafından imzalanmasına rağmen iç hukukumuzda uygulama alanı bulmayan kişisel verilerin korunmasına ilişkin düzenlemeler şu şekildedir:

- 1981 – Kişisel Verilerin Otomatik İşlenmesine Karşı Bireylerin Korunması Sözleşmesi,
- 2001 – Kişisel Verilerin Otomatik İşlenmesine Karşı Bireylerin Korunması Sözleşmesine Ek Denetleyici Makamlar ve Sınıraşan Veri Aktarımına İlişkin Protokol

Bu durum 6698 Sayılı Kişisel Verilerin Korunması Kanunu'nun (KVKK) yürürlüğe girmesinden önce uluslararası arenada büyük bir eksiklik olarak nitelendirilmiş ve hatta Türkiye bu eksiklik sebebi ile bazı iş birliği fırsatlarından mahrum olmuştur. Örneğin 6698 sayılı KVKK öncesinde kişisel veriler korunmadığı gerekçesiyle Türkiye ile Avrupa Polis Teşkilatı (EUROPOL) ile operasyonel iş birliği anlaşması imzalanamamaktaydı. Benzer

[1] Gürsel, Esin, Düğmeci, Fatih, "Yapısal Anlamda Türkiye Kişisel Verileri Koruma Kurumu'na İlişkin Bir Değerlendirme", R&S - Research Studies Anatolia Journal, Cilt 1, Sayı 2, 2018, s. 319.

[2] Tekin, Nurullah, "Kişisel Verilerin Korunması İle İlgili Türkiye'deki Kanun Tasarısının Avrupa Birliği Veri Koruma Direktifi Işığında Değerlendirilmesi", Uyuşmazlık Mahkemesi Dergisi, Cilt 0, Sayı 4, 2014, s. 247.

şekilde Türkiye, kişisel verilerin korunmasına yönelik bir düzenleme olmaması sebebiyle çalıntı araçlar, pasaportlar, tutuklama kararları ve istenmeyen kişiler ile ilgili bilgiler içeren Schengen Bilgi Sistemi (SIS) gibi imkanlardan da faydalanamamıştır.[3]

Ülkemizde kişilerin verilerinin korunması yönündeki ihtiyacın başkaca bir yönü, Avrupa Birliği uyum sürecidir. Gerçekten; Birlik, kişisel verilerin korunması hakkında düzenlemeler ile bireylerin kişilik haklarını korumayı hedeflemektedir. Nitekim bu düzenlemeler üye ülkelerin mevzuatlarında da yer edinmektedir. Bunun doğal bir sonucu olarak Türkiye gibi aday ülke statüsünde olan ülkelerden de AB uyum süreci kapsamında kişisel verilerin korunması için düzenlemeler yapılması beklenmektedir. Üstelik AB mevzuatındaki birtakım maddeler, kişisel verilere ilişkin yeterli korumanın sağlanmadığı ülkelere veri aktarımını yasaklamak suretiyle Türkiye'nin e-ticaret anlamında Avrupa pazarında faaliyet göstermesini de engellemekteydi.[4]

Bu nedenle AB'nin kişisel verilerin işlenmesi alanında küresel bir etkiye de yol açan düzenlemesi olan GDPR'nin ve mevzuatımızda yürürlükte olan Kişisel Verilerin Korunması Kanunu'nun karşılaştırmalı bir incelemesi her iki düzenlemenin de uygulama alanında faaliyet göstermesi olası global teşebbüslere faydalı olacağı açıktır.

[3] Tekin, 2014: 248.

[4] Gürsel ve Düğmeci, 2018: 321.

I. BÖLÜM: KİŞİSEL VERİLERİN KORUNMASINA GENEL BİR BAKIŞ

A. KİŞİSEL VERİLERİN KORUNMASININ TARİHSEL GELİŞİMİ

1. Türk Hukukunda Kişisel Verilerin Korunmasına Yönelik Düzenlemeler

Hukukumuzda 6698 Sayılı KVKK'nın getirdiği yenilikleri ve bu yeniliklerin Avrupa'daki düzenlemeler ile benzerliklerini ve farklılıklarını incelemeden evvel, mevzuatımızda önceden beri var olan kişisel verilerin korunması düzenlemelerinin ve bunların tarihsel gelişiminin incelenmesi faydalı olacaktır.

Her ne kadar kişisel verileri toplanması, saklanması ve işlenmesi günümüzde yeni yeni önem kazanmakta gibi gözükse de mevzuatımızda bu alanı düzenleyen hükümler KVKK'dan çok daha eskiye dayanmaktadır. Zira kişisel verilerin korunması, hukuk devletlerinde korunması mecburi olan bazı değerlerle yakından ilişkilidir. Gerçekten; kişinin şerefinin, onurunun, hayat alanının, resminin, sesinin ve kişiye ait başka bir takım hassas verilerin kişilik hakkını oluşturan değerlerden sayıldığı açıktır.

Bu bağlamda, mevzuatımızda kişilik hakkını koruyan diğer hükümlerin incelenmesi, KVKK'ya zemin hazırlayan hukuki ortamın görülmesi bakımından önem arz etmektedir.

a. 1982 Anayasası'nda Kişilik Hakkı ve Kişisel Veriler

Anayasa, normlar hiyerarşisinin tepesinde yer aldığından doğaldır ki kişisel verilerin korunması alanındaki tüm diğer düzenlemelerin hukuki altyapısını oluşturmaktadır. 1982 Anayasasında; özel hayatın gizliliği hakkını düzenleyen 20. Madde başta olmak üzere konut dokunulmazlığını düzenleyen 21. Madde, haberleşmenin gizliliğini düzenleyen 22. Madde, dini ve vicdani kanaatleri açıklamaya zorlanamama hakkını düzenleyen 24. Madde ve düşünce ve kanaatleri açıklamaya zorlanamama hakkını düzenleyen 25. Madde kişisel verilerin

korunmasına yönelik düzenlemeler barındırmaktadırlar.[5] Bu bağlamda özel hayatın gizliliği hakkını düzenleyen 20. madde ön plana çıkmaktadır. Bu maddeye göre:

> *"Herkes, özel hayatına ve aile hayatına saygı gösterilmesini isteme hakkına sahiptir. Özel hayatın ve aile hayatının gizliliğine dokunulamaz.*
>
> *Millî güvenlik, kamu düzeni, suç işlenmesinin önlenmesi, genel sağlık ve genel ahlâkın korunması veya başkalarının hak ve özgürlüklerinin korunması sebeplerinden biri veya birkaçına bağlı olarak, usulüne göre verilmiş hâkim kararı olmadıkça; yine bu sebeplere bağlı olarak gecikmesinde sakınca bulunan hallerde de kanunla yetkili kılınmış merciin yazılı emri bulunmadıkça; kimsenin üstü, özel kâğıtları ve eşyası aranamaz ve bunlara el konulamaz. Yetkili merciin kararı yirmidört saat içinde görevli hâkimin onayına sunulur. Hâkim, kararını el koymadan itibaren kırksekiz saat içinde açıklar; aksi halde, el koyma kendiliğinden kalkar."*

Maddenin ilk fıkrası ile tüm vatandaşların kişilik hakkı kapsamında özel hayatının ve aile hayatının gizliliği güvence altına alınmıştır. Bahse konu hüküm, kişilik ve gizlilik haklarının hangi unsurları kapsadığını sınırlı sayıda saymamıştır. Bunun temelinde vatandaşların günlük hayattaki ihtiyaçlarının değişmesi ve/veya teknolojinin gelişmesi sonucunda kişilik hakkı kavramının ihtiva ettiği değerlerin değişecek olması yatmaktadır. Bu yüzden çerçeve hüküm olarak nitelendirilebilecek bu fıkra ile hem özel hayatın gizliliğini yakından ilgilendiren hem de gitgide daha fazla ekonomik değere haiz olmaya başlayan kişisel verilerimizin de korunduğu pek tabii söylenebilir.

2010 yılına gelindiğinde ise kişisel verilerin korunması alanında özel düzenlemelere ihtiyaç olacağı daha net bir biçimde görülmüştür. Yapılan Anayasa değişikliği ile 20. maddeye 3. bir fıkra eklenmiştir. Eklenen fıkraya göre göre;

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

Anayasa değişikliği teklifinde bu fıkra için gösterilen gerekçede;

[5] Kılınç, Doğan, "Anayasal Bir Hak Olarak Kişisel Verilerin Korunması", Ankara Üniversitesi Hukuk Fakültesi Dergisi, Cilt 61, Sayı 3, 2012, s. 1131.

"Anayasada kişisel verilerin korunmasına yönelik dolaylı hükümler bulunmakla birlikte yeterli değildir. Mukayeseli hukukta ve tarafı olduğumuz uluslararası belgelerde de kişisel verilerin korunması önemle vurgulanmaktadır. Maddeyle, herkesin, kendisiyle ilgili kişisel verilerin korunmasını isteme hakkı, anayasal bir hak olarak teminat altına alınmaktadır. Bu bağlamda, bireylerin kendilerini ilgilendiren kişisel veriler üzerinde hangi hak ve yetkilere sahip olduğu ve kişisel verilerin hangi hallerde işlenebileceği hükme bağlanırken, kişisel verilerin korunmasına ilişkin esas ve usullerin kanunla düzenleneceği öngörülmektedir."

İfadesine yer verilmiştir. 20. maddeye 2010 yılında eklenen bu fıkra ile hem kişisel verilerin korunması hakkı açık biçimde anayasada yer bulmuş hem de kişisel verilerin korunmasına ilişkin esaslar kanun ile belirlenir hükmüne yer verilmek suretiyle KVKK'nın hukuki temeli atılmıştır.[6]

b. 4721 Sayılı Türk Medeni Kanunu'nda Kişilik Hakkı

Kişisel verilerin korunmasını isteme hakkı, Anayasanın kişinin hak ve ödevlerini düzenleyen ikinci bölümünde ele alınmıştır. Bu sebeple bu hakkın kişilik hakkının bir uzantısı olduğunu söylemek yanlış olmayacaktır. Buradan hareketle Türk Medeni Kanunu'nun kişilik hakkını koruyan hükümleri, kişisel verilerin korunması için uygulama alanı bulacaktır.[7] Kişiliğin saldırılardan korunmasına yönelik düzenlemelere 4721 Sayılı Türk Medeni Kanunu'nun (TMK) 24. ve 25. maddeleri ile yer verilmiştir. 24. Maddeye göre:

"Hukuka aykırı olarak kişilik hakkına saldırılan kimse, hâkimden, saldırıda bulunanlara karşı korunmasını isteyebilir.

Kişilik hakkı zedelenen kimsenin rızası, daha üstün nitelikte özel veya kamusal yarar ya da kanunun verdiği yetkinin kullanılması sebeplerinden biriyle haklı kılınmadıkça, kişilik haklarına yapılan her saldırı hukuka aykırıdır."

Ve 25. Maddeye göre:

[6] Kişisel Verileri Koruma Kurumu, "Anayasal Bir Hak Olarak Kişisel Verilerin Korunmasını İsteme Hakkı", (Erişim) https://www.kvkk.gov.tr/SharedFolderServer/CMSFiles/cf706768-36ab-472c-bbd6-cb0b773405da.pdf, 23 Ocak 2020

[7] Çokmutlu, Metin, Türk Ceza Hukukunda Kişisel Verilerin Korunması, Yayımlanmamış Yüksek Lisans Tezi, Kocaeli Üniversitesi, Sosyal Biliimler Enstütüsü, Kocaeli, 2014, s. 125.

"Davacı, hâkimden saldırı tehlikesinin önlenmesini, sürmekte olan saldırıya son verilmesini, sona ermiş olsa bile etkileri devam eden saldırının hukuka aykırılığının tespitini isteyebilir.

Davacı bunlarla birlikte, düzeltmenin veya kararın üçüncü kişilere bildirilmesi ya da yayımlanması isteminde de bulunabilir. Davacının, maddî ve manevî tazminat istemleri ile hukuka aykırı saldırı dolayısıyla elde edilmiş olan kazancın vekâletsiz iş görme hükümlerine göre kendisine verilmesine ilişkin istemde bulunma hakkı saklıdır.

Manevî tazminat istemi, karşı tarafça kabul edilmiş olmadıkça devredilemez; mirasbırakan tarafından ileri sürülmüş olmadıkça mirasçılara geçmez."

Kişisel verilerinin gizliliğini ihlal edildiğini veya hukuka aykırı biçimde işlendiğini iddia eden kişi, 24 ve 25. Maddeler kapsamında dava açarak ihlalin tespitini, önlenmesini, durdurulmasını veya ihlal sebebi ile uğradığı zararların tazminini talep edebilir.[8]

Burada altı çizilmesi gerekli bir husus, 24. Maddede belirtilen hukuka uygunluk nedenleridir. Buna göre kişinin rızasının ya da daha üstün bir faydanın bulunması veya kanunun tanıdığı yetkinin kullanılması hallerinde kişilik haklarına bir saldırı olduğundan bahsedilemez. Bu düzenleme, KVKK ile getirilen kişisel verilerin işlenmesi şartlarına da paralel niteliktedir.

TMK, kişisel verilerin korunmasına ilişkin belirli bir seviyede koruma sağlamaktadır. Ancak Anayasa ile benzer şekilde, kişilik hakkının hangi değerleri koruduğuna ilişkin keskin sınırlar çizmekten kaçındığından ve kişisel verilerin korunmasına yönelik özel hükümlere yer vermediğinden tek başına yeterli bir koruma mekanizması değildir. Diğer bir deyişle TMK'da yer alan düzenlemeler, kişisel verilerin korunması alanının kendine özgü niteliği itibariyle kişisel verileri etkin biçimde korumak için yeterli değildirler.[9]

Tüm bunlara ek olarak, TMK kapsamında getirilen korumaların tamamı, kişisel verilerin gizliliği ihlal edildikten sonra yapılabilecek işlemlerden ibarettir. Bu düzenlemelerin kişisel verilerin korunmasını teşvik edici veya ihlalleri önleyici bir işlevi de bulunmamaktadır.[10]

[8] Çokmutlu, 2014: 124.
[9] Kılınç, 2012: 1132.
[10] Çokmutlu, 2014: 127.

c. 6098 Sayılı Türk Borçlar Kanunu'nda Kişilik Hakkı

TMK'ya paralel olarak, 6098 Sayılı Türk Borçlar Kanunu'nda da kişilik hakkının korunmasına yönelik hükümlere yer verilmiş olup, bu hükümler kişisel verilerin korunması bağlamında da uygulama alanı bulacaktır. Kişilik hakkının korunması bakımından Türk Borçlar Kanunu'nun (TBK) 27., 49. ve 58. Maddeleri öne çıkmaktadır.

TBK'nın 27. Maddesi; kişilik haklarına aykırı biçimde yapılan sözleşmelerin kesin hükümsüz olduğunu düzenlemektedir. Kanaatimizce bu hüküm, KVKK'da karşımıza çıkan rızanın geçerli olabilmesinin bazı şartlara bağlanması suretiyle rızaya rağmen kişinin verilerini korumaya yönelik düzenleme ile aynı doğrultudadır.

TBK'nın 49. Maddesi haksız fiil neticesinde ortaya çıkan zararların tazminine ilişkindir. Gerçekten, kişisel verilerin hukuka aykırı olarak işlenmesi bir haksız fiil niteliğinde olduğundan kişinin bu işlemler neticesinde uğradığı zararın tazminini isteme hakkı TBK ile düzenlenmiştir.[11]

Son olarak TBK 58. Madde ise; kişilik hakkı zarara uğrayan kimsenin uğradığı zararlarının tazminini talep etmesine ilişkindir. Özellikle internet ortamında kişilik haklarının ihlalinin ve kişinin şerefine yahut özel hayatına karşı suçların işlenmesinin daha kolay olduğu göz önünde bulundurulduğunda 58. Maddenin her geçen gün daha sık uygulandığını söylemek yanlış olmayacaktır.

Borçlar Kanunu da Medeni Kanun gibi kişisel verilerin korunmasını ayrıca ve detaylı biçimde düzenlemek yerine, hak ihlali gerçekleştikten sonra uygulanabilecek genel hükümlere yer verdiğinden kişisel verilerin korunması bağlamında yeterli değildir.

d. 5237 Sayılı Türk Ceza Kanunu'nda Kişilik Hakkı

Özel hayatın gizliliği hakkının ihlali neticesinde oluşan suçların tanımları, 5237 Sayılı Türk Ceza Kanunu'nun (TCK) 132. ve devam maddeleriyle yapılmış ve bu suçların oluşması halinde verilecek cezalar belirlenmiştir.

KVKK perspektifinden bakıldığında üzerinde durulması gereken Türk Ceza Kanunu Maddeleri; özel hayatın gizliliğini ihlal suçunu düzenleyen m.134, kişisel verilerin

[11] Çokmutlu, 2014: 127.

kaydedilmesi suçunu düzenleyen m.135, verileri hukuka aykırı olarak verme veya ele geçirme suçunu düzenleyen m.136 ve verileri yok etmeme suçunu düzenleyen m.138'dir. Nitekim bu suçların maddi unsurunu oluşturan fiiller aynı zamanda KVKK'yı da ihlal etmektedirler.

Özel hayatın gizliliğini ihlal suçunu tanımlayan m.134'e göre;

> *"Kişilerin özel hayatının gizliliğini ihlal eden kimse, bir yıldan üç yıla kadar hapis cezası ile cezalandırılır. Gizliliğin görüntü veya seslerin kayda alınması suretiyle ihlal edilmesi halinde, verilecek ceza bir kat artırılır.*
>
> *Kişilerin özel hayatına ilişkin görüntü veya sesleri hukuka aykırı olarak ifşa eden kimse iki yıldan beş yıla kadar hapis cezası ile cezalandırılır. İfşa edilen bu verilerin basın ve yayın yoluyla yayımlanması halinde de aynı cezaya hükmolunur."*

Görüldüğü üzere KVKK kapsamında ihlal olarak nitelendirilebilecek olan özel hayata ilişkin görüntü veya ses kaydı ile bu kayıtların alenileştirilmesi eylemleri, aynı zamanda TCK m.134 kapsamında suç teşkil etmektedir.

Veri kaydına ilişkin bir düğer suç ise TCK'nın 135. Maddesi ile düzenlenen kişisel verilerin kaydedilmesi suçudur ve bu suç; TCK'daki KVKK ile en yakından ilişkili olan suçtur. 135. maddenin birinci fıkrasına göre:

> *"Hukuka aykırı olarak kişisel verileri kaydeden kimseye bir yıldan üç yıla kadar hapis cezası verilir."*

Yine KVKK'ya paralel olarak, aynı maddenin 2. Fıkrası ile KVKK'nın özel nitelikli kişisel veri saydığı bilgilerin kaydedilmesi de cezayı artırıcı sebep olarak belirlenmiştir:

> *"Kişisel verinin, kişilerin siyasi, felsefi veya dini görüşlerine, ırki kökenlerine; hukuka aykırı olarak ahlaki eğilimlerine, cinsel yaşamlarına, sağlık durumlarına veya sendikal bağlantılarına ilişkin olması durumunda birinci fıkra uyarınca verilecek ceza yarı oranında artırılır."*

Ancak m.135'in birinci fıkrasında kişisel verinin tanımının yapılmaksızın kaydedilmelerinin yasaklanması, maddenin suçta ve cezada kanunilik ilkesine aykırı

olduğundan hareketle eleştirilmesine sebep olmuştur.[12] Ancak bu hususta Yargıtay'ın, TCK'nın 135. Maddesinin gerekçesinde yer alan

> *"Gerçek kişiyle ilgili her türlü bilgi, kişisel veri olarak kabul edilmelidir. Söz konusu suç tanımında kişisel verilerin bilgisayar ortamında veya kağıt üzerinde kayda alınması arasında bir ayırım gözetilmemiştir"*

hükmüne uygun olarak içtihatlar oluşturduğunu görmekteyiz. Nitekim Yargıtay Ceza Genel Kurulu, 2012/1510E. ve 2014/331K. sayılı kararında da;

> *"TCK'nun 135 ve 136. maddelerindeki kişisel verilerin korunmasına ilişkin düzenlemelerde sadece sır niteliğinde kişisel verilerin korunacağına ilişkin bir hükmün bulunmaması ve aksine 135. maddenin gerekçesinde gerçek kişiyle ilgili her türlü bilginin kişisel veri olarak kabul edilmesi gerektiğinin belirtilmesi karşısında, her türlü kişisel verinin hukuka aykırı olarak başkasına verilmesi, yayılması ve ele geçirilmesi fiillerinin kanunun 136. maddesindeki suçu oluşturduğu kabul edilmelidir."*

şeklinde değerlendirmede bulunarak gerçek kişiye ait her türlü bilginin kişisel veri sayılacağını kabul etmiştir.

TCK ile kişisel verilerin kaydedilmesinin yanı sıra, hukuka aykırı olarak ele geçirilmesi ve üçüncü kişiler ile paylaşılması da suç olarak tanımlanmıştır. Verileri hukuka aykırı olarak verme veya ele geçirme kenar başlıklı TCK'nın 136. maddesine göre:

> *"Kişisel verileri, hukuka aykırı olarak bir başkasına veren, yayan veya ele geçiren kişi, iki yıldan dört yıla kadar hapis cezası ile cezalandırılır."*

Bu maddeye göre suç oluşabilmesi için, kişinin verileri yetkisiz olarak ele geçirmiş olması gereklidir. Bu konuda bir banka çalışanının müşterilerin bilgilerini kendi e-posta adresine göndermesine yönelik Yargıtay 12. Ceza Dairesi'nin 2015/4348E. ve 2015/4865K. sayılı kararı emsal teşkil etmektedir. Bu karara göre;

> *"...sanığın çalıştığı bankada yetkisiz üçüncü kişi konumunda bulunmadığı, kendisine verilen yetki kapsamında, şahsi mail hesabına gönderdiği bilgilere erişebildiği gibi, sanık dışında diğer çalışanlar tarafından da, bu bilgiler şahsi mail hesabına gönderilerek kullanıldığı ve sanığın bu bilgileri başka bankalara dağıttığına ilişkin dosya kapsamından*

[12] Çokmutlu, 2014: 174.

hiçbir delil bulunmadığı anlaşılmakla, sanık hakkında beraat kararı verilmesinde isabetsizlik görülmemiştir."

136. maddeyi önemli kılan bir nokta; kişinin özel hayatının gizliliğinin yanı sıra kişisel verilerinin yayılması sebebi ile toplum içinde itibarını kaybetme, şantaja maruz kalma gibi daha büyük tehlikelere karşı da kişiyi korumaya yönelik bir düzenleme olmasıdır.[13] Öyle ki, Yargıtay Ceza Genel Kurulu bir şikayete delil oluşturması bakımından dahi kişisel verilerin ele geçirilmesinin hukuka uygun olduğunu kabul etmemektedir. Gerçekten, Yargıtay Ceza Genel Kurulu tarafından verilen 2012/1514E. ve 2014/312K. sayılı karara göre;

"Kendisi ve eşi de memur olan sanığın, yapacakları şikayete konu olmak üzere eşi ile aynı işyerinde ebe olarak çalışan katılanın doğum belgesini hastaneden alarak, il sağlık müdürlüğüne verdikleri şikayet dilekçesinin ekinde sunmaları şeklinde gerçekleşen somut olayda, katılana ait doğum belgesinin kişisel veri olması, memur olarak çalışan sanığın başkasına ait bilgileri içeren bir belgeyi velevki yapacağı şikayet başvurusuna konu olsa dahi almasının hukuka aykırı olacağını bilebilecek durumda bulunması, suça konu doğum belgesini şikayet dilekçesine eklemek suretiyle burada yer alan ve kişisel veri niteliğinde bulunan bilgilerin katılanın rızası dışında başkalarınca öğrenilmesine neden olunması hususları birlikte değerlendirildiğinde, sanığın eylemi TCK'nun 136. maddesinde düzenlenen kişisel verileri hukuka aykırı olarak ele geçirme ve yayma suçunu oluşturmaktadır."

Benzer şekilde, şayet bilgiler elde edildiği anda veri sahibinin rızası olmuş olsa bile daha sonra rızanın ortadan kalkması halinde bilgilerin yayılmaya devam etmesi de TCK m. 136. Bakımından suç olarak kabul edilmektedir. Buna ilişkin olarak Yargıtay 12. Ceza Dairesi'nin 2017/150E. ve 2017/6231K. sayılı içtihadında, ayrıldığı sevgilisinin fotoğrafını Facebook profilinden silmeyen sanık hakkında;

"İddiaya konu sanıkla mağdur arasındaki ilişkinin varlığını ve boyutunu gösteren fotoğrafların, daha önce mağdurun rızasına uygun olarak facebook adlı sosyal paylaşım sitesinde yayımlanmış olması karşısında, bu fotoğraflar, mağdurun özel yaşam alanına ilişkin ve özel hayatının gizliliğini ihlal edecek nitelikte görüntüler olarak kabul edilemeyeceğinden, sanığın, mağdura ait kişisel veri niteliğindeki fotoğrafları, mağdurun rızasına aykırı şekilde yayımlamaya devam etmesi biçiminde sübut bulan eyleminden dolayı TCK'nın 136/1. maddesindeki verileri hukuka aykırı olarak verme veya ele geçirme suçundan mahkumiyet kararı verilmesi gerektiği gözetilmeksizin,

[13] Çokmutlu, 2014: 214.

yasal ve yeterli olmayan yazılı gerekçelerle sanık hakkında CMK'nın 223/2-a maddesi gereğince beraat kararı verilmesi kanuna aykırı olup…"

Şeklinde tespitte bulunulmuştur. İçtihat olarak yerleşmiş olan bu uygulama, çalışmanın devamında irdeleyeceğimiz verilerin işlenmesi yönündeki açık rızanın her zaman geri çekilebileceği yönündeki KVKK düzenlemesine de paraleldir.

Ancak 136. maddenin lafzı; maddenin içeriğinde "yayma" eylemine yer verilmişken, madde kenar başlığında bu eyleme yer verilmemesi ve madde içeriğinde "kişisel veri" ibaresine yer verilmişken kenar başlığında "veri" kavramının kullanılmış olmasının tutarsızlıklara sebebiyet verdiği noktasında eleştirilmektedir.[14]

Son olarak TCK m. 138 ile verileri yok etmeme suçu tanımlanmıştır:

"Kanunların belirlediği sürelerin geçmiş olmasına karşın verileri sistem içinde yok etmekle yükümlü olanlara görevlerini yerine getirmediklerinde bir yıldan iki yıla kadar hapis cezası verilir."

Verileri yok etmeme suçu, özellikle son yıllarda dijital izlerimizin artması ile gündeme gelen ve bu çalışmanın da konusunu oluşturan GDPR'de "Unutulma Hakkı" olarak yer bulan hakkın TCK'daki izdüşümü olarak değerlendirilebilir. Buna ek olarak, verilerin zamanında silinmemesi/yok edilmemesi yine KVKK anlamında da ihlal teşkil etmektedir.

Yukarıda sayılan kanunlara ek olarak; İş Kanunu'ndaki işçinin özlük dosyası hakkındaki hükümler, Banka Kartları ve Kredi Kartları Kanunu'nda yer alan özellikle bilgileri saklamaya yönelik hükümler de kişisel verilerin korunması anlamında ikincil mevzuat olarak kabul edilebilir. Yine Adli Sicil Kanun'unda ve Türk Ticaret Kanunu'nda da kişisel verilerin korunması yönünde bazı düzenlemelere yer verilmiştir.[15]

Görüldüğü üzere KVKK'nın yürürlüğe girmesinden önce de hukukumuzda kişilik haklarının ve devamında kişisel verilerin korunması için düzenlemeler bulunmaktaydı. Bu düzenlemeler, KVKK ile aynı anda uygulanmaya da devam edecekler.

[14] Çokmutlu, 2014: 214.

[15] Kartal, Mustafa Tevfik, "Kişisel Verilerin Korunması: Türk Bankacılık Sektörü Üzerine Kavramsal Bir Değerlendirme", Uluslararası Ekonomi ve Yenilik Dergisi, Cilt 4, Sayı 1, 2018, s. 10,11.

e. 5809 Sayılı Elektronik Haberleşme Kanunu

2008 yılında yürürlüğe giren Elektronik Haberleşme Kanunu'nu; elektronik haberleşme hizmeti sunan işletmelere 4. maddesi ile bilgi güvenliği ve haberleşme gizliliğinin korunması sorumluluğunu yüklemiş ve 12. maddesi ile kişisel veri gizliliğinin korunmasına yönelik ek yükümlülükler getirilebileceğini ifade etmiştir.

Aynı kanunun kişisel verilerin işlenmesi ve korunması kenar başlıklı 51. Maddesinde kişisel verilerin işlenmesinde uyulacak ilkeler sayılmıştır. Bu ilkeler, KVKK'daki ilkeler ile aynı olup, çalışmanın devamında detaylı biçimde inceleneceklerdir. Yine 51. Madde, verilerin yurt dışına aktarımı, işlemenin hukuka uygunluğu gibi daha sonra KVKK'da da yer bulan birçok hükme yer vermiştir.

f. 6698 Sayılı Kişisel Verilerin Korunması Kanunu

6698 Sayılı KVKK'nın ikinci maddesine göre Kanun; kişisel verileri işlenen gerçek kişileri ve bu verileri işleyen gerçek ve tüzel kişilere uygulanır. Aynı maddeye göre KVKK'nın uygulanması için kişisel verileri işleme faaliyetlerinin kısmen veya otomatik olması yahut otomatik olmasa bile bir veri kayıt sisteminin parçası olması gereklidir. Zıt kanaati ile ifade etmek gerekirse KVKK, otomatik olmayan ve herhangi bir veri kayıt sisteminin parçası olmayan yollarla işlenen kişisel veriler ve bu verileri işleyenler bakımından uygulama alanı bulmayacaktır.

2. Avrupa Birliği'nde Kişisel Kişisel Verilerin Korunmasına Yönelik Düzenlemeler

Veri gizliliğinin ortaya çıkışının, kanunlarda da yer edinmesinden çok önce iş dünyasında olduğu bilinmektedir. Örneğin avukat-müvekkil gizliliği ya da hukukumuzdaki ismi ile avukatın sır saklama yükümlülüğünün, avukat ile müvekkili arasında bir sözleşme olarak başladığı ve daha sonra kanunlaştığı düşünülmektedir. Böylelikle müvekkilin yasal yaptırımlardan korkmaksızın avukatı tarafından bilgilendirilmesi, avukatın da müvekkilin çıkarlarını koruyabilmesi mümkün olmuştur. Benzer şekilde, sağlık kayıtlarının doktorun

güvencesinde olması da sağlık verilerinin korunmasına ilişkin yasalardan onlarca yıl önce ortaya çıkmıştır.[16]

Bu çalışma kapsamında GDPR'nin incelenmesine geçilmeden önce GDPR'den önce Birlik hukukunda kişisel verilerin korunmasını amaçlayan düzenlemelerin incelenmesi, hem GDPR'ye ihtiyaç duyulmasının sebeplerinin hem de GDPR'de yer alan düzenlemelerin temellerinin anlaşılması bakımından önem arz etmektedir.

a. Avrupa İnsan Hakları Sözleşmesi

Avrupa Konseyi, İkinci Dünya Savaşı'ndan sonra Avrupa'daki ülkeleri hukukun, demokrasinin, insan haklarının ve sosyal gelişimin öne çıkarıldığı bir amaç etrafında toplamak üzere kurulmuştur. Bu amaca yönelik olarak 1950 yılında kabul edilen Avrupa İnsan Hakları Sözleşmesi (AİHS), 1953 yılında yürürlüğe girmiştir.[17] AİHS hükümleri, taraf devletler için bağlayıcı niteliktedirler. Avrupa Konseyi ülkelerinin tamamı günümüze dek ya AİHS'i kendi ulusal hukuklarının bir parçası haline getirmiş ya da sözleşmeyi ulusal hukuklarında etki gösterecek biçimde tanımışlardır. Başka bir ifadeyle günümüzde sözleşmeye uygun hareket etme yükümlülüğü altındadırlar. Taraf devletler, yetkilerini ve güçlerini kullanırken sözleşme ile sağlanmış haklara saygı göstermek zorundadırlar. Buna ulusal güvenlik sebebiyle kullanılan yetkiler de dahildir. Nitekim Avrupa İnsan Hakları Mahkemesinin (AİHM) bazı emsal kararları, devletlerin hassas ulusal güvenlik meselelerini korumak üzere icra ettikleri bazı faaliyetlerini de kapsamaktadır.[18]

Kişisel verilerin korunması hakkı, kaynağını AİHS'in 8. maddesi ile düzenlen aile ve özel yaşamına saygı duyulmasını isteme hakkından almaktadır.[19] Bunun bir sonucu olarak AİHM, kişisel verilerin gizliliğinin ihlali iddiasıyla önüne gelen uyuşmazlıkları, AİHS'in 8. maddesine göre çözümlenmektedir. Mahkeme, öncelikle 8. Maddede düzenlenen "özel alan" kavramını somutlaştırmakta ve aynı maddenin ikinci fıkrası kapsamında bu alana yapılan müdahaleleri incelemektedir. Başka bir ifade ile AİHM, 8. Maddenin birinci fıkrası ile öngörülen özel alanının sınırlarını, maddenin ikinci fıkrasını yorumlamak suretiyle çizmekte

[16] Calder, Alan, EU GDPR A Pocket Guide, IT Governance Publishing, Cambridgeshire, 2016, s.11.
[17] European Union Agency for Fundamental Rights and Council of Europe, Handbook on European Data Protection Law, Imprimerie Centrale, Luxembourg, 2018, 22.
[18] European Union Agency for Fundamental Rights and Council of Europe, 2018: 23.
[19] European Union Agency for Fundamental Rights and Council of Europe, 2018: 23.

ve buradan hareketle somut olayda özel alana yapılan müdahalenin meşruluk kazanıp kazanmadığını değerlendirmektedir.[20]

AİHM bu yöntem ile iletişimin dinlenmesi, özel veya kamu kuruluşları tarafından gerçekleştirilen çeşitli izleme yöntemleri, kamu otoriteleri tarafından kişisel verilerin depolanması da dahil olmak üzere veri güvenliğini ilgilendiren birçok duruma ilişkin karar vermiştir. Belirtmek gerekir ki özel hayatın gizliliğine saygı duyulmasını isteme hakkı, mutlak bir hak değildir. Zira bu hakkın kullanımı ifade özgürlüğü veya bilgiye erişim hakkı gibi diğer bazı hakların kullanılmasına engel olabilir. Bu sebeple mahkeme somut olayda yarışan haklar arasında bir denge bulmayı amaçlamaktadır. Buna ek olarak AİHM'in verdiği kararlarda devletlere yalnızca bu hakkı ihlal edebilecek davranışlardan kaçınmak yükümlülüğü vermediğini, aynı zamanda bazı durumlarda bu hakkı güvence altına almak üzere aktif çaba gösterme görevi yüklediğini de görmekteyiz.[21]

Avrupa İnsan Hakları Sözleşmesinde yer alan düzenlemenin yoruma açık olmasından bahisle, kimilerince kötüye kullanılabileceği de dile getirilmiştir. Yukarıda ifade edildiği üzere hakkın kullanımı bazı diğer haklarının kısıtlanması anlamına gelmektedir. Bu durum hakkın kötüye kullanımının önünü açtığı gibi, yine 8. maddeye dayanarak yapılacak yasal veya idari düzenlemeler neticesinde bazı kurum veya kuruluşlara adaletsiz yükler getirilmesi veya bu maddeye dayalı kapsamlı davalar açmak yoluyla AİHM'in devletler üzerinde sahip olduğu gücü kullanarak devletlerin egemenliğinin sınırlanması gibi problemlerin ortaya çıkabileceği söylenmiştir. Ne var ki düzenlemenin, her iki cepheden de eleştiriler almasına rağmen bugüne dek tüm tarafların çıkarlarını gözetecek şekilde dengede kaldığı da söylenebilir. Bu yüzdendir ki AİHS'nin özel hayatın gizliliği hakkına ilişkin ortaya koyduğu emsal, modern yasal düzenlemelerimizi dahi etkileyecek kadar uzun bir süredir etkisini sürdürmektedir.[22]

b. Kişisel Verilerin Otomatik İşleme Tabi Tutulması Karşısında Bireylerin Korunması Sözleşmesi (108 No'lu Sözleşme)

Bugün 108 numaralı sözleşme olarak da bilinen Kişisel Verilerin Otomatik İşleme Tabi Tutulması Karşısında Bireylerin Korunması Sözleşmesi; 1960'lardan sonra teknolojide

[20] Solmaz, Eren, "Avrupa İnsan Hakları Mahkemesi Kararları'nın "Kişisel Verilerin Korunması"na Katkısı", İdare Hukuku ve İlimleri Dergisi, Cilt 18, Sayı 1, 2019, s. 64.
[21] European Union Agency for Fundamental Rights and Council of Europe, 2018: 24.
[22] Calder, 2016: 13.

yaşanan gelişmeler neticesinde ülkelerin ve uluslararası kuruluşların kişisel verilerin gizliliği ve korunması kavramlarıyla tanışmaları neticesinde ortaya çıkmıştır. Avrupa Konseyi, 108 No'lu sözleşmeyi 1985 yılında kabul etmiştir. Bu sözleşme, özel olarak kişisel verilerin toplanması ve işlenmesine karşı yapılan bağlayıcı nitelikteki ilk uluslararası sözleşmedir.

Aynı zamanda ilk kez bu sözleşme ile kişilerin ırkı, siyasi görüşü, dini ve adli kayıtları gibi hassas verilerinin işlenmesi hukuka aykırı kabul edilmiştir. Bu sözleşme gerek özel sektör tarafından toplanan gerekse yargı ve kolluk unsurları gibi kamu araçlarınca toplanan ve işlenen tüm verileri kapsamaktadır. 108 No'lu sözleşme vatandaşları yetkisiz veri toplanması ve işlenmesi gibi kötüye kullanımlara karşı korumakta ve sınır dışına veri aktarımını düzenlemektedir. 108 No'lu sözleşme kişisel veriyi; kimliği belirli veya belirlenebilir bir kişiye ait olan veri olarak tanımlandığından doğru biçimde anonimleştirilmiş edilmiş veriler, 108 No'lu sözleşme kapsamında değillerdir.[23]

108 No'lu sözleşmenin kişilerin verilerin hukuka aykırı bir şekilde toplanması ve işlenmesi neticesinde zarara uğramasını engellemek için asgari bazı standartlar koyduğunu söylemek yanlış olmayacaktır. Sözleşmenin diğer bir görevi, kişisel verilerin sınır ötesi akışının düzenlenmiş olmasıdır. Bu sözleşmenin yapılması ile aynı tarihlerde OECD, Özel Yaşamın Korunması Ve Kişisel Verilerin Sınır Ötesi Akışına İlişkin Rehber İlkeleri yayınlamıştır. Avrupa Konseyi'nin ve OECD'nin çalışmaları, birçok Avrupa ülkesinin harekete geçmesine ve kişilerin veri güvenliği hakları ile kamu otoriteleri ve işverenler gibi veri toplama ve işleme ihtiyacı duyanların bu ihtiyaçları arasında dengeleyici ulusal düzenlemeler yapmalarına sebep olmuştur.[24]

108 No'lu sözleşme, kendisinden sonra gelecek olan Avrupa Birliği 95/46/EC Kişisel Verilerin İşlenmesi Ve Bu Tür Verilerin Serbest Dolaşımına Dair Bireylerin Korunması Direktifin'in temelini oluşturmuştur.[25]

[23] Güner, Oğuz, Günar, Altuğ, "Protection of Personal Data in the European Union-turkey Relations: Effect of Visa Liberalisation Dialogue", Yönetim ve Ekonomi Araştırmaları Dergisi, Cilt 17, Sayı 4, 2019, s. 39.

[24] Tikkinen-Piri, Christina, Rohunen, Anna, Markkula, Jouni, "EU General Data Protection Regulation: Changes and implications for personal data collecting companies", Computer Law & Security Review, Cilt 34, Sayı 1, 2018, s. 136.

[25] Kierkegaard, Sylvia, Waters, Nigel, Greenleaf, Graham, Bygrave, Lee A., Lloyd, Ian, Saxby, Steve, "30 years on – The review of the Council of Europe Data Protection Convention 108", Computer Law & Security Report, Cilt 27, Sayı 3, 2011, s. 223

c. 95/46/EC Kişisel Verilerin İşlenmesi Ve Bu Tür Verilerin Serbest Dolaşımına Dair Bireylerin Korunması Direktifi

1990'ların başında Birlik içerisinde kişisel verilerin işlenmesine dair düzenlemelerin birbirleri ile uyumlu olması için Avrupa Birliği çapında bir çalışma başlatılmıştır. 108 No'lu sözleşmeyi temel alan bu çalışma neticesinde Direktif, üye devletlerin ulusal yasama işlemleri yoluyla uygulanmak üzere 1995 yılında kabul edilmiştir. Bu direktif bireylerin kişisel verilerinin işlenmesi faaliyetlerine karşı korunmasının ve bu verilerin Avrupa Birliği içerisindeki akışının düzenlenmesini kapsamaktadır.[26] Direktif, ilerleyen süreçte kişisel verilerin korunmasına ilişkin Avrupa standardının oluşmasında büyük rol oynadığından, mercek altına alınmasında fayda vardır.[27]

Direktif'in temelinde yatan ana kavram; kişisel verilerin işlenmesidir. Kendisinden önce gelen düzenlemeler genelde kişisel verilerin depolanmasına yönelik kurallar getirmişken Direktif, depolamadan daha geniş bir işleme kavramını benimsemiştir. Direktif'e göre kişisel verilerin depolanması, veri işlemenin yalnızca bir çeşidi olarak görülmüştür.[28]

d. Kişisel Verilerin Otomatik İşleme Tabi Tutulması Karşısında Bireylerin Korunması Sözleşmesine Ek Denetleyici Makamlar Ve Sınıraşan Veri Akışına İlişkin Protokol (181 Sayılı Ek Protokol)

108 No'lu sözleşmenin kabul edilişinden sonra yaşanan teknolojik gelişmelerin beraberinde getirdiği sosyolojik değişiklikler 108 No'lu Sözleşme'nin gözden geçirilmesi ihtiyacını doğurmuştur. 1990'larda internetin ortaya çıkması ve ardından Web 2.0 ile bilginin evrensel ölçekte paylaşılması ve aktarılmasının mümkün kılındığı interaktif bir ortam sağlanması neticesinde kişisel verilerin gizliliği ve korunması konularında bazı yeni ihtiyaçlar doğmuştur. Google ve Wikipedia gibi bilginin paylaşılmasına olanak sağlayan araçlar ile ortaya çıkan bu ihtiyaç; yer belirleme teknolojileri, güvenlik kameraları, nesnelerin interneti ve

[26] Tikkinen-Piri, Rohunen ve Markkula, 2018: 136.
[27] Elgesem, Dag, "The structure of rights in Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and the free movement of such data", Ethics and Information Technology, 1999, s. 283.
[28] Elgesem, 1999: 284.

biyometrik verileri gibi hayatımıza giren yeni teknolojik kavramlar ile de katlanarak artmaktadır. [29]

Yeni ihtiyaçlar doğrultusunda sözleşmenin uyarlanması 2001 yılında Kişisel Verilerin Otomatik İşleme Tabi Tutulması Karşısında Bireylerin Korunması Sözleşmesine Ek Denetleyici Makamlar Ve Sınıraşan Veri Akışına İlişkin Protokol (181 Sayılı Ek Protokol) ile gerçekleşmiştir. Protokolün amacı sözleşme ile belirlenmiş prensiplerin uygulanabilirliğini arttırmak ve bazen düzenlemeler eklemektir.[30]

108 No'lu sözleşme de Direktif de kabul edilişlerinin üzerinden sırasıyla 30 ve 20 yıldan fazla zaman geçmiş olmasına rağmen ortak amaçları olan Avrupa Birliği üye devletlerindeki kişisel verilerin korunması düzenlemelerinde tutarlılığı ve uyumluluğu yakalama hedefine ulaşamamışlardır. Bunun üzerine Avrupa Komisyonu; Avrupa Birliği'nin veri korunmasına ilişkin sistemini reform etmiştir. Bu reform neticesinde işbu çalışmanın temel konusu olan GDPR ortaya çıkmıştır.

e. 2002/58/EC Sayılı Elektronik Haberleşme ve Gizlilik Direktifi

E-Gizlilik Direktifi olarak da bilinen 2002/58/EC Sayılı Elektronik Haberleşme ve Gizlilik Direktifi, Birlik'te yürürlükte olan veri gizliliği hükümlerine ek olarak, elektronik haberleşme alanında gizliliği düzenlememektedir.[31]

GDPR'nin 95. Maddesi ile, elektronik haberleşme alanında gösterdiği faaliyetler sebebi ile 2002/58/EC Sayılı Direktif'e tabi olan ve bu konuda yükümlülük altında bulunan gerçek ve tüzel kişilere ek yükümlülük getirmeyeceği düzenlenmiştir.

f. General Data Protection Regulation

GDPR'nin kapsamını düzenleyen ikinci maddesine göre; GDPR, kişisel verilerin tamamen ya da kısmen otomatik araçlarla yahut dosyalama sisteminin parçasını oluşturan veya bir dosyalama sisteminin parçası olması amaçlanan araçlarla işlenmesine uygulanır.

---

[29] De Terwangne, Cécile, "The work of revision of the Council of Europe Convention 108 for the protection of individuals as regards the automatic processing of personal data", International Review of Law, Computers & Technology, Cilt 28, Sayı 2, 2014, s. 118

[30] De Terwangne, 2014: 118,119.

[31] Information Comissioner's Office, "Guide to the Privacy and Electronic Communications Regulations", (Erişim) https://ico.org.uk/media/for-organisations/guide-to-pecr-2-4.pdf, 24 Aralık 2019

İkinci maddenin devamında, GDPR'nin uygulama alanı bulmayacağı istisnai haller sayılmıştır. GDPR; birlik hukuku kapsamına girmeyen faaliyetlerde, üye devletler tarafından Avrupa Birliği Anlaşması'na uygun olarak dış güvenlik politikasına ilişkin hükümler uygulanırken, tamamen kişisel veya ev faaliyet esnasında bir gerçek kişi tarafından, kamu güvenliğine yönelik tehditlere karşı güvence sağlanması ve bu tehditlerin önemlisi de dahil olmak üzere suçların önlenmesi, soruşturulması, tespiti ve kovuşturulması ya da cezaların infaz edilmesi ile ilgili olarak yetkili makamlar tarafından kişisel verilerin işlenmesi durumlarında uygulanmaz.

İkinci madde ile düzenlenen durumlar GDPR'nin maddi kapsamını belirlerken, GDPR'nin bölgesel kapsamı 3. Madde ile belirlenmiştir. Buna göre GDPR, işleme faaliyetinin Birlik içerisinde gerçekleşip gerçekleşmemesine bakılmaksızın Birlik içerisindeki bir kontrolör veya işleyicinin işletmesinin faaliyetleri bağlamında kişisel verilerin işlenmesi halinde uygulanır. Devamla yine 3. maddeye göre GDPR işleme faaliyetlerinin;

- Veri sahibine ödeme yapılıp yapılmadığına bakılmaksızın, Birlik içerisindeki veri sahibine mal veya hizmet sunulması veya
- Veri sahibinin davranışları Birlik içerisinde gerçekleştiği ölçüde davranışlarının izlenmesi

Hususlarından herhangi biriyle alakalı olması durumunda, Birlik içerisinde bulunan veri sahiplerinin kişisel verilerinin Birlik içerisinde olmayan bir kontrolör veya işleyici tarafından işlenmesinde de uygulanacaktır.

Görüldüğü üzere GDPR; Avrupa Birliği tabanlı kontrolör ve işleyicilere uygulandığı gibi, Avrupa Birliği içerisinde yer alan veri sahibinden mal veya hizmet sunulması yahut veri sahibinin davranışların izlenmesi durumlarında, veri işleme işleminin nerede gerçekleştiğine bakılmaksızın, uygulanmaktadır. Diğer bir deyişle GDPR, genişletilmiş bir bölgesel kapsam benimsemiştir.[32]

Yine dikkat edilmesi gereken diğer bir nokta, her ne kadar GDPR'nin yalnızca Avrupa Birliği vatandaşlarına uygulandığı ile ilgili bazı yanlış algılar olsa da GDPR, Birlik içerisinde yaşayan ancak vatandaş olmayan göçmenler, çalışma ve turist vizesi ile Birlik sınırları içerisinde bulunanlar, yaşama izni olanlar gibi Birlik içerisinde yer alan tüm kişileri kapsamaktadır. Buna ek olarak kişisel verisi Avrupa Birliği sınırları içerisinde depolanan yahut işlenen kişiler, Avrupa Birliği vatandaşı olmasalar veya Avrupa Birliği sınırları içerisinde

[32] Tikkinen-Piri, Rohunen ve Markkula, 2018: 138.

yaşamasalar dahi GDPR'nin korumasından faydalanabileceklerdir. Zira Birlik içerisinde yer alan kurum ve kuruluşlar, yürüttükleri veri işleme faaliyetleri bakımından veri sahibinin nerede olduğuna bakılmaksızın GDPR ile bağlılardır.[33]

B. KİŞİSEL VERİLERİN KORUNMASI HUKUKUNDA TANIMLAR

1. KVKK'da Yer Alan Tanımlar

a. Açık Rıza Kavramı

Rıza ve açık rıza, KVKK'nın birçok noktasında işleme faaliyetinin gerçekleştirilebilmesi için hukuka uygunluk şartı olarak öngörüldüğünden üzerinde durulması gereken kavramlardandır. Kanun, açık rızayı *"Belirli bir konuya ilişkin, bilgilendirilmeye dayanan ve özgür iradeyle açıklanan rıza"* olarak tanımlamıştır. Buna göre, ilgili kişinin rızasının açık rıza sayılabilmesi için gerekli şartlar;

- Rızanın belirli bir konuya ilişkin olarak verilmesi
- Bilgilendirmenin usulüne uygun biçimde yapılması ve
- Rızanın özgür irade ile alınmasıdır.

Çalışmanın devamında da sıklıkla değinileceği üzere, kişisel verilerin korunmasına yönelik düzenlemelerin amacı kişinin verileri üzerindeki hakimiyetini kuvvetlendirmek ve kişisel veri işleme faaliyetleri hakkındaki şeffaflığı artırmaktır.[34] Bu bağlamda kişinin verdiği rızanın gelecekteki tüm işleme faaliyetlerini kapsayan, genel nitelikli bir rıza olması kabul edilemez.[35] Açık rızanın geçerli olabilmesi için, kişinin verdiği rızanın hangi işleme faaliyetlerine ilişkin olarak rıza gösterdiğinin net biçimde anlaşılması gerekir.

Yine kişinin verileri üzerinde hakimiyet sahibi olabilmesi için işleme faaliyetlerine rıza vermeden evvel kişisel verilerinin hangi amaçla, ne kadar süre ile, hangi nitelik ile işleneceği ve hangi amaçlarla kullanılacağı konusunda bilgilendirilmesi gerekir.[36] Nitekim KVKK,

---

[33] Calder, 2016: 36.

[34] Anı, Nevzat Ali, Kişisel Verilerin İşlenmesi ve Açık Rıza, Yayımlanmamış Yüksek Lisans Tezi, İstanbul Üniversitesi, Sosyal Bilimler Enstitüsü, İstanbul, 2018, s. 131.

[35] Anı, 2018: 131.

[36] Korkmaz, İbrahim, "Kişisel Verilerin Korunması Kanunu Hakkında Bir Değerlendirme", Türkiye Barolar Birliği Dergisi, Cilt 29, Sayı 124, 2016, s. 108.

bilgilendirme konusuna verdiği önemi 10. Madde ile veri sorumlusuna aydınlatma yükümlülüğü getirmek suretiyle vurgulamış ve veri sorumlusunu bu hususta doğrudan sorumlu kılmıştır.[37]

Son olarak kişinin iradesini sakatlayacak cebir, tehdit, hata ve hile gibi durumların varlığında verilen rızanın açık rıza niteliğinde olduğundan bahsetmek mümkün olmayacaktır. Zira açık rızanın özgür irade ile verilmiş olması gerekliliği düzenlenmiştir. Tarafların eşit durumda olmadıkları (Örneğin işçi-işveren ilişkisi gibi), yahut bir ürün veya hizmetin sunulması için rızanın ön şart olduğu hallerde verilen rızanın özgür iradeye dayandığı kabul edilemez.[38]

b. Anonim Hale Getirme Kavramı

Kişisel verilerin işlenmesi, şüphesiz günlük yaşantımıza dahi etki eden büyük faydalar sağlamaktadır. Kişisel verilerin korunmasına yönelik düzenlemeler, işte bu faydalar ve kişilerin temel hal ve özgürlükleri arasında bir denge bulmayı amaçlar. Bu çerçevede, kişisel verilerin anonim hale getirilerek işlenmesi verilerinden faydalanmasını engellemeden gizliliği koruduğu için bu dengenin sağlanmasında büyük önem arz etmektedir.[39]

Anonim hale getirme kavramı; KVKK'da *"Kişisel verilerin, başka verilerle eşleştirilerek dahi hiçbir surette kimliği belirli veya belirlenebilir bir gerçek kişiyle ilişkilendirilemeyecek hâle getirilmesi"* şeklinde tanımlanmıştır. Görüldüğü üzere ana kriter, anonimleştirilen kişisel verilerin bir kişi ile ilişkilendirilip ilişkilendirilemeyeceği hususudur.[40] Bu noktada anonim hale getirme işleminin, kişinin adı yerine takma isim kullanılması veya her bir kişi için numara belirlenmesinden ibaret bir faaliyet olmadığı vurgulanmalıdır. Zira zaman zaman kişilere takma ad veya numara atanmış olsa bile kişinin kimliğinin tespiti mümkün olabilmektedir. Bu sebeple de veri, kişisel veri niteliğini kaybetmemektedir. Anonim hale

[37] Anı, 2018: 133.
[38] Kişisel Verileri Koruma Kurumu, "Açık Rıza", (Erişim) https://www.kvkk.gov.tr/SharedFolderServer/CMSFiles/66b2e9c4-223a-4230-b745-568f096fd7de.pdf, 24 Ocak 2020
[39] Gözüküçük, Merve, Veri işleme Süreçlerinde Tartışmalı Bir Çözüm: Veri Anonimleştirilmesi, Yayımlanmamış Yüksek Lisans Tezi, İstanbul Bilgi Üniversitei, Sosyal Bilimler Enstitüsü, İstanbul, 2014, s. 42.
[40] Gözüküçük, 2014: 45.

getirme kavramından anlamamız gereken şey; hiçbir surette kişinin kimliğini açık etmeyecek şekilde verilerin saklanmasıdır.[41]

Verilerin yanlış biçimde anonim hale getirilmesi sebebi ile kişilerin kimlik bilgilerinin tespit edilebilmesi konusunda Netflix'in yakın zamanda yaptığı hata örnek olarak gösterilebilir. İnternet medya devi, kullanıcılarının verilerini anonim hale getirdiğini iddia etmiş ve ardından bu verileri halka açık şekilde paylaşmıştır. Ancak paylaşılan verinin büyüklüğü sebebiyle, kişilerin kimlikleri uzmanlar tarafından saptanabilmiştir.[42] Bu gibi örnekler bizlere anonim hale getirme işleminin veri güvenliği bakımından önemli olduğu kadar, teknik olarak zor bir işlem olduğunu da göstermektedir.

Anonimleştirme, yukarıda izah edilen fayda/gizlilik dengesinin sağlanması bakımından güçlü bir silah olduğundan hem anonimleştirme işleminin güvenilirliğinin artırılması hem de anonimleştirme sürecine olan güvenin korunması için disiplinlerarası bir yaklaşım benimsenmeli ve hukuki altyapı, teknik metotlar ile desteklenmelidir.[43]

c. İlgili Kişi Kavramı

Kanun, "ilgili kişi"yi *"Kişisel verisi işlenen gerçek kişi"* olarak tanımlamıştır. Kanun'un lafzında da açıkça görüldüğü üzere, kişisel veri kavramı hukukumuzda yalnızca gerçek kişilerin verilerini kapsamaktadır. Diğer bir deyişle tüzel kişilerin ilgili kişi sıfatına haiz olmaları mümkün değildir. Eğer bir veri, tüzel kişiye ait olmasına rağmen herhangi bir gerçek kişinin kimliğinin belirlenebilmesi sonucunu doğuruyorsa bahse konu veri kişisel veri niteliğinde kabul edilir. Fakat bu durum, biraz önce ifade ettiğimiz tüzel kişilerin ilgili kişi olamayacağı kuralının istisnası değildir. Zira bu halde ilgili kişi veriye sahip olan tüzel kişi değil, veri aracılığı ile kimliği belirlenebilen gerçek kişidir.[44]

Kişisel verilerin çoğunlukla kişinin manevi varlığı ile ilgili olması ve tüzel kişilerin manevi tazminat talep etme haklarının tartışmalı olması sebepleri ile tüzel kişiler kapsam

---

[41] Henkoğlu, Türkay, "Kişisel Verileriniz Ne Kadar Güvende? Bilgi Güvenliği Kapsamında Bir Değerlendirme", Arşiv Dünyası Dergisi, Sayı 17-18, 2017, s. 53.

[42] Çekin, Mesut, "6698 Sayılı Kişisel Verilerin Korunması Hakkında Kanun'un Big Data (Büyük Veri) Ve İrade Serbestisi Açısından Değerlendirilmesi", İstanbul Ünversitesi Hukuk Fakültesi Mecmuası, Cilt 74, Sayı 2, 2016, s. 636. Ve Singel, Ryan, "Netflix Spilled Your Brokeback Mountain Secret, Lawsuit Claims", (Erişim) https://www.wired.com/2009/12/netflix-privacy-lawsuit/, 22 Kasım 2019

[43] Gözüküçük, 2014: 110.

[44] Kişisel Verileri Koruma Kurumu, 100 Soruda Kişisel Verilerin Korunması Kanunu, KVKK Yayınları, Ankara, 2018, s. 21.

dışında bırakılmıştır. Bu yüzden verilerinin hukuka aykırı biçimde kişilik haklarını ihlal edecek şekilde depolanması ve işlenmesi sonucunda zarara uğrayan tüzel kişiler, önceki bölümde bahsedilen ikincil kanun hükümleri çerçevesinde haklarını arayacaklardır.

Gerçek kişi sınırlaması, kişisel verilerin korunmasının, Türk Medeni Kanunu'na uygun olarak sağ ve tam doğum ile başladığı ve kişinin ölümü ile son bulduğu anlamına gelmektedir.[45] Türk Medeni Kanunu'na göre kişinin ölümü ile kişiliği de son bulacağından, ölülerin de ilgili kişi olarak değerlendirilmeleri mümkün değildir.

TMK'ya göre kişiliğin sağ ve tam doğum ile kazanılması, bazı durumlarda ilgili kişinin kim olduğuna ilişkin belirsizlik oluşturabilmektedir. Örneğin bebeğin doğumundan önce bebeğe ilişkin elde edilmiş tıbbi verileri ile ultrason gibi yöntemlerle elde edilmiş görüntüleri Kanun'a göre kişisel veri kapsamında değerlendirilebilir mi? Şayet bunların kişisel veri olduklarını kabul edersek, o halde ilgili kişi tam ve sağ doğumdan itibaren kişiliğini kazanan bebek mi olacaktır? Yoksa veriler elde edildiğinde bebek ilgili kişi sıfatına haiz olamadığından, bu verilerin korunması bakımından ilgili kişi bebeğin annesi mi kabul edilecektir? Her ne kadar çocukların kişisel verilerinin korunacağı konusunda herhangi bir muallak bulunmasa da açıklanan durumda ilgili kişinin kim olacağı hakkında mevzuatımızda bir netlik yoktur.

d. Kişisel Veri Kavramı

KVKK'nın 3. Maddesinin 1. Fıkrasının d bendine göre *"Kimliği belirli veya belirlenebilir gerçek kişiye ilişkin her türlü bilgiyi"* kişisel veri niteliğindedir. Yukarıda da izah edildiği üzere bu madde ile Kanun'da kişisel veri kavramının kapsamı, gerçek kişiler ile sınırlandırıldığından Kanun, tüzel kişilerin verileri bakımından uygulama alanı bulmaz. Konu bakımından ise bir verinin kişisel veri sayılabilmesi için ilgili kişiyi belirlenebilir kılması gerekmektedir.

KVKK, kişiye ait hangi bilgilerin kişisel veri niteliğinde olduğunun sınırlı sayıda sayılmayıp, kişinin kimliğini belirlenebilir kılan her türlü bilgiyi kişisel veri olarak kabul ederek, bir verinin kişisel veri niteliğinde olup olmadığının somut olaya göre değerlendirilmesini Kanun uygulayıcıya bırakılmıştır.[46] Bazı durumlarda bir veri; tek başına kişinin kimliğini belirlenebilir kılmazken, birtakım ek bilgiler ile kişinin kimliğinin ifşa

[45] Yücedağ, Medeni Hukuk Açısından Kişisel Verilerin Korunması Kanunu'nun Uygulama Alanı Ve Genel Hukuka Uygunluk Sebepleri, 2017: 766.
[46] Kişisel Verileri Koruma Kurumu, 2018: 18.

edilmesine sebep olabilir. Bu durumda verinin kişisel veri niteliğinde olup olmayacağı tartışmalıdır. [47]

Her ne kadar bazı belirsizliklere yol açsa da kişisel verilere ilişkin toplama, depolama ve işleme faaliyetlerinin tamamına yakınının bilişim teknolojileri kullanılarak icra edildiği ve bu teknolojilerin çok hızlı bir biçimde geliştiği düşünüldüğünde, KVKK'da kişisel veri kalemlerinin tek tek sayılmasındansa bu şekilde çerçeve hüküm kurulması kanaatimizce yerinde olmuştur.

e. Kişisel Verilerin İşlenmesi

Kişisel verilerin işlenmesi kavramı; KVKK'nın m 3./1-e ile tanımlanmıştır. Buna göre:

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

Kişisel veri kavramının tanımına benzer şekilde, kişisel verilerin işlenmesi kavramı da sınırlı sayıda işlemlerin yazılması yoluyla tanımlanmak yerine her somut olayda baştan değerlendirilmek üzere geniş ve yoruma açık olarak yapılmıştır. Bu sebeple kişisel verilerin ilk elde edilmesinden başlayarak veriler üzerinde gerçekleşen tüm işlemler "kişisel verilerin işlenmesi" olarak değerlendirilir. Tanımda açıkça belirtildiği gibi; verilerin yalnızca kaydedilmesi dahi kişisel verilerin işlenmesi olarak değerlendirilir. Bu nedenle kişisel verilerin sadece depolanması, bu veriler herhangi bir işleme tabi tutulmasalar da bir veri işleme faaliyetidir.[48]

Kanundaki tanımda kişisel verilerin işlenmesi konusunda otomatik yollarla işleme ve otomatik olmayan yollarla işleme olmak üzere ikili bir ayrıma gidildiği görülmektedir. Kanun metninde otomatik yollarla kişisel verilerin işlenmesi kavramının tanımı yapılmamış olmasına karşın Kanun'un gerekçesine bakıldığında otomatik yollarla işleme kavramının, *"verilerin*

[47] Yücedağ, Nafiye, "Medeni Hukuk Açısından Kişisel Verilerin Korunması Kanunu'nun Uygulama Alanı Ve Genel Hukuka Uygunluk Sebepleri", İstanbul Üniversitesi Hukuk Fakültesi Mecmuası, Cilt 72, Sayı 2, 2017, s. 767,768.
[48] Kişisel Verileri Koruma Kurumu, 2018: 18,22.

bilişim sistemleri aracılığıyla işlenmesini" ifade ettiği görülebilir. Kanun otomatik yollarla yapılan tüm işlemeleri kapsamaktayken, verilerin otomatik olmayan yollarla işlenmesini yalnızca bu faaliyetlerin bir veri kayıt sistemi aracılığıyla yapılması hallerinde kapsar. Burada veri kayıt sistemi, elektronik veya fiziki ortamda oluşturulan ve verilerin sınıflandırılabildiği her türlü sistemi kapsar. Örneğin bir kâğıtta kişilerin isim ve soy isimlerinin yazılı olması tek başına kanun kapsamında değerlendirilmezken, kâğıttaki bu listenin herhangi bir kıstas göz önünde bulundurularak hazırlandığı tespit edilirse o zaman kanun kapsamına girecektir.[49]

Verinin yalnızca depolanmasının dahi veri işleme sayılması, sayılan işleme faaliyetlerinin sınırlayıcı olmadığının açıkça belirtilmesi ve veri üzerinde gerçekleştirilecek her türlü faaliyetin veri işleme kavramına dâhil edilmesi, kavramın kapsamını oldukça geniş tutmaktadır. Kişisel veri kavramına benzer şekilde, kanun uygulayıcılara büyük sorumluluk düşmekteyse de teknolojinin gelişme hızı ve her geçen gün veri işlemenin yeni yollarının keşfedildiği göz önünde bulundurulduğunda bu tanımın da çerçeve olarak yapılması yerindedir.

f. Kurum

KVKK, 19. ve devam maddeleri ile idari ve mali özerkliğe sahip bir veri koruma otoritesi kurmaktadır. KVKK'ya göre; Kişisel Verileri Koruma Kurumu, yani Kurum, merkezi Ankara olan, kamu tüzel kişiliğine haiz ve Cumhurbaşkanının görevlendireceği bakan ile ilişkili olan bir kamu tüzel kişiliğidir.

Kurum, 27.09.1984 tarihli ve 3046 sayılı Bakan Yardımcılarının Mali Hakları ve Bazı Düzenlemeler Hakkında Kanun kapsamında "ilişkili kuruluş" olarak değerlendirilmektedir. Buna göre Kurum'un bakanlık ile hiyerarşik bir bağı yoktur ancak bakanlığın idari vesayet denetimine sınırlı şekilde tabiidir.[50] 15 Temmuz 2018 tarihli ve 30479 sayılı Resmi Gazetede yayımlanan "Bakanlıklara Bağlı, İlgili ve İlişkili Kurum ve Kuruluşlar ile İlgili 2018/1 Sayılı Cumhurbaşkanlığı Genelgesi" ile Kurum Adalet Bakanlığı ile ilişkilendirilmiştir.

Kurumun KVKK'nın 20. Maddesi ile belirlenen görevleri, görev alanı ile ilgili ulusal ve uluslararası gelişmeleri takip etmek, iş birlikleri kurmak, yıllık faaliyet raporu sunmak ve kanunlarla verilen diğer görevleri yerine getirmek olarak özetlenebilir. Diğer bir deyişle

[49] Kişisel Verileri Koruma Kurumu, 2018: 25.
[50] Gürsel ve Düğmeci, 2018: 323.

Kurum; kişisel verilerin korunması alanına ilişkin olarak düzenleme, denetim, uyuşmazlık çözme, yaptırım uygulama ve görüş bildirme görevlerini yerine getirir.[51]

Kurum; Kurul ve Başkanlıktan oluşur.

g. Kurul

Kurul, Kişisel Verileri Koruma Kurumunun dokuz üyeden oluşan bağımsız karar organıdır. Kurul;

- Kişisel verilerin, temel hak ve özgürlüklere uygun şekilde işlenmesini sağlamaktan,
- Kişisel verilerle ilgili haklarının ihlal edildiğini ileri sürenlerin şikâyetlerini karara bağlamaktan,
- Şikâyet üzerine veya ihlal iddiasını öğrenmesi durumunda resen görev alanına giren konularda kişisel verilerin kanunlara uygun olarak işlenip işlenmediğini incelemek ve gerektiğinde bu konuda geçici önlemler almaktan,
- Özel nitelikli kişisel verilerin işlenmesi için aranan yeterli önlemleri belirlemekten,
- Veri Sorumluları Sicilinin tutulmasını sağlamaktan,
- Kurulun görev alanı ile Kurumun işleyişine ilişkin konularda gerekli düzenleyici işlemleri yapmaktan,
- Veri güvenliğine ilişkin yükümlülükleri belirlemek amacıyla düzenleyici işlem yapmaktan,
- Veri sorumlusunun ve temsilcisinin görev, yetki ve sorumluluklarına ilişkin düzenleyici işlem yapmaktan,
- KVKK'da öngörülen idari yaptırımlara karar vermekten,
- Diğer kurum ve kuruluşlarca hazırlanan ve kişisel verilere ilişkin hüküm içeren mevzuat taslakları hakkında görüş bildirmekten,
- Kurumun; stratejik planını karara bağlamak, amaç ve hedeflerini, hizmet kalite standartlarını ve performans kriterlerini belirlemekten,
- Kurumun stratejik planı ile amaç ve hedeflerine uygun olarak hazırlanan bütçe teklifini görüşmek ve karara bağlamaktan
- Kurumun performansı, mali durumu, yıllık faaliyetleri ve ihtiyaç duyulan konulardan hakkında hazırlanan rapor taslaklarını onaylamaktan ve yayımlamaktan,
- Taşınmaz alımı, satımı ve kiralanması konularındaki önerileri görüşüp karara bağlamaktan,
- Kanunlarla verilen diğer görevleri yerine getirmekten

Sorumludur. Kurul içeresindeki toplantılar aksi kararlaştırılmadıkça gizlidir.

[51] Gürsel ve Düğmeci, 2018: 323,324.

İdarenin kanuniliği ilkesi gereği, Kurul'un Kurum adına alacağı kararlara ve yapacağı işlemlere karşı yargı denetimi yolu açıktır. Kurul'un verdiği idari para cezaları hariç diğer işlemlerine karşı İdari Yargılama Usul Kanundaki esaslara göre İdari dava açmak mümkündür. Kurulca kesilen idari para cezalarına ise 5326 sayılı Kabahatler Kanunu hükümlerine göre itiraz edilebilir.[52]

h. Başkan

KVKK'nın 24. Maddesine göre Kurul ve Kurumun Başkanı, Kurumun en üst amiridir ve kurum hizmetlerinin mevzuata ve kuru stratejine uygun olarak yürütülmesini sağlar. Başkan aynı zamanda, kurul toplantılarını idare eder, kurul kararlarının kamuoyuna duyurularını sağlar, kurumun yönetim ve işleyişine ilişkin bütçe ve personel atamaları dahil olmak üzere idari görevleri yerine getirir.

i. Veri Sorumlusu Kavramı

Kişisel verilerin hangi amaçlarla ve araçlarla işleme tabi tutulacağının kararını veren, verilerin kaydı için sistemlerin kurulmasından ve yönetilmesinden sorumlu olan kişi, "veri sorumlusu"dur. Burada kişi; özel hukuk tüzel kişisi de kamu tüzel kişisi de olabilir. Altı çizilmesi gerekli başka bir husus; veriler bir tüzel kişi tarafından işleme tabi tutulduğunda, veri sorumlusunun o tüzel kişinin çalışanları değil, bizzat tüzel kişiliğin kendisi olduğudur.[53]

Kanun'un lafzında veri sorumlusunun, kişisel verilerin işlenmesine dair kararları vermesinin yanı sıra veri kayıt sisteminin kurulmasından ve yönetilmesinden de sorumluğu olduğunun belirtilmesi; kişinin yalnızca bu iki şartı aynı anda sağlaması halinde mi veri sorumlusu sıfatına haiz olabileceği yönünde bazı tartışmalara sebebiyet vermiştir. Ancak doktrinde bunun zorunlu değil tanımlayıcı bir etken olduğu, bu yüzden kişisel verilerin işleme ve araçlarını belirleyen kişinin veri sorumlusu olduğu yönündedir.[54] Bu bağlamda veri sorumlusunun belirlenmesinde temel kıstas işlevi yani verilerin işleme tabi tutulacağı amaçlar

[52] Gürsel ve Düğmeci, 2018: 327.
[53] Kişisel Verileri Koruma Kurumu, 2018: 30.
[54] Pekmez, Cüneyt, "Overview of the Definitons of Data Controller and Data Processor within the Scope of The Turkish Code of Personal Data Protection (TCDP)", Annales de la Faculté de Droit d'Istanbul, Sayı 67, 2019, s. 63.

ve hangi yöntemler ile bu işleme faaliyetlerinin yürütüleceğine karar vermek konusunda yetkili olmasıdır.

İşlev odaklı yapılan tanım sebebiyle veriye sahip olan herkes veri sorumlusu sayılmayacaktır olamaz. Örneğin bir şirket verilerini saklamak ve depolamak için bir başka şirketten hizmet satın alıyorsa, depolama hizmetini veren şirket veriye sahip olduğu halde verinin kimlerle ne şekilde paylaşılacağını veya ne şekilde işleneceğini belirleyen otorite olmadığından veri sorumlusu olarak değerlendirilmeyecektir. Bunun en güzel örneği, verilerin saklanması için bir bulut depolama çözümü tercih edildiğinde şayet bulut altyapısını sunan şirket ile ayrıca bir veri işleme anlaşması yapılmazsa, bu şirketin veri sorumlusu olmayacağıdır.

Veri sorumlusu, KVKK ile kendisine yüklenen sorumlulukları getirmekle mükellef olup, bunlara aykırı hareket etmesi yahut kişisel verilerin işlenmesi ilkelerini ihlal etmesi hallerinde hem oluşan zararın tazmininden hem de kurul tarafından verilecek kararın yerine getirilmesinden sorumludur.[55]

j. Veri İşleyen Kavramı

Yine 6988 Sayılı KVKK'nın m. 3/1-ğ'ye göre veri işleyen kavramı; *"veri sorumlusunun verdiği yetkiye dayanarak onun adına kişisel verileri işleyen gerçek veya tüzel kişiyi"* anlatmakta kullanılır. Burada önemli olan kıstas; veri işleyenin faaliyetlerini, veri sorumlusunun talimatına bağlı olarak gerçekleştirmesidir. Bu nedenle veri işleyenin görevinin daha çok teknik kısımlar ile ilgili olduğunu söylemek yanlış olmayacaktır. Ancak veri sorumlusu ve veri işleyen kavramlarının tanımları, kişiye göre değil icra edilen faaliyetlerin niteliğine göre yapıldığından, aynı kişi farklı faaliyetleri ile hem veri sorumlusu hem de veri işleyen olabilir.[56]

Yukarıda verilen bulut bilişim sistemleri örneğinden devam etmek gerekirse, günümüzde birçok bulut depolama hizmeti sağlayıcısının aynı zamanda depolanan verilerin anlamlı biçimde işlenebilmesi ve analiz edilebilmesi için çeşitli araçlar da sağladığı görülmektedir. Veri sorumlusu tarafından bir bulut hizmet sağlayıcısından hizmet almak yoluyla verilerin işlenmesi halinde bu bulut sağlayıcısı da veri işleyen sıfatında olacaktır.

---

[55] Memiş, Tekin, "Veri Sorumlusu ve Veri İşleyen Arasındaki İlişkiler ve Sorumluluk Düzeni", Beykent Üniversitesi Hukuk Fakültesi Dergisi, Cilt 3, Sayı 6, 2017, s. 11.
[56] Kişisel Verileri Koruma Kurumu, 2018: 31.

Veri işleyen kavramının en önemli özelliği veriyi, veri sorumlusunun talimatları doğrultusunda işlemesidir. Veri İşleyen, veri sorumlusunun talimatları ile bağlı olduğundan veri işlenmesine ilişkin yükümlülüklerin yerine getirilmesinde asıl sorumlu veri sorumlusu olacaktır.[57] Veri sorumlusunun talimatlarının aşılması durumunda veri işleyenin sorumluluğu doğacaktır ve o aşamada veri işleyen "de facto"[58] veri sorumlusu kabul edilecektir.[59] Diğer bir deyişle talimatları aşan veri işleyen de veri sorumlusuymuş gibi değerlendirilerek ortaya çıkan zarardan sorumlu tutulacaktır.

k. Veri Kayıt Sistemi

KVKK m.3'e göre veri kayıt sistemi, kişisel verilerin belirli kriterlere göre yapılandırılarak işlendiği kayıt sistemini ifade eder. Dikkat edilmesi gereken nokta, kanun özel olarak bir belirleme yapmadığından sistemin elektronik ortamda bulunması şart değildir.

l. Veri Sorumluları Sicili

Kişisel verileri işleyen gerçek ve tüzel kişilerce veri işlemeye başlanmadan önce kayıt olması gereken, Kurulun gözetiminde Başkanlık tarafından kamuya açık olarak tutulan sicildir. Kural olarak veri işleme faaliyeti icra edecek olan herkesin sicile kaydolması gereklidir ancak Kurul kaydolma zorunluluğuna istisnalar getirebilir.

2. GDPR'de Yer Alan Kavramlar

GDPR'nin gerek kapsamını gerek uygulanabilirliğini doğru şekilde belirleyebilmek için, GDPR'de geçen kavramların doğru anlaşılması ve yorumlanması gerektiği izahtan varestedir. Bu sebeple GDPR'nin 4. Maddesinde kişisel verilerin korunmasına ilişkin bazı terimlerin tanımlarına yer verilmiştir. Bu çalışma kapsamında da kavramların hem GDPR metninde açıklandığı şekillerinin hem de doktrinde ve uygulamada nasıl yorumlandıklarının incelenmesi, GDPR ve 6698 Sayılı Kanun arasındaki farklıların belirlenmesi açısından önemlidir.

[57] Kişisel Verileri Koruma Kurumu, 2018: 31.
[58] Fiilen
[59] Pekmez, 2019: 67.

a. Kişisel Veri

GDPR'ye göre Kişisel Veri, tanımlanmış veya tanımlanabilir bir gerçek kişiye ilişkin her türlü bilgidir. Buna göre GDPR'deki kişisel veri kavramı da tüzel kişilerin verilerini kapsamaması bakımından 6698 Sayılı Kanun'daki tanım ile benzerlik göstermektedir.

Dikkat edilmesi gereken nokta yine bir verinin kişisel veri olup olmadığının işleme faaliyetinin niteliğine göre göreceli olabileceğidir. Örneğin bir evin finansal değeri; normal şartlar altında kişisel veri olarak kabul edilmez. Ancak ev; mülkiyet sahibinin bazı hukuki yükümlülükler altına girmesine sebep olabileceğinden, örneğin evin malikinin vergi yükümlülüğüne ilişkin bir veri işlemesi yapılırken evin finansal değerinin de kişisel veri olarak kabul edilmesi gerekir.[60]

Özellikle internet kullanımının hızla arttığı bu günlerde, internette paylaşılan bilgilerin tek başına kişisel verilerin gizliliğini ihlal edip etmeyeceği netleştirilmelidir. Buna ilişkin olarak Avrupa Birliği Adalet Divanının (ABAD) Lindqvist kararı, her ne kadar Direktif'in yürürlükte olduğu zaman verilen bir karar olsa da, GDPR'nin kişisel veri kavramını tanımlama biçimi Direktif ile aynı olduğundan, emsal teşkil edebilir. İsveç'te yaşayan Bodil Lindqvis, kilisesi için bir web sitesi hazırlarken, kilisede görevli olan arkadaşlarının isimlerinin, telefon numaralarının, işlerinin ve hobilerinin yer aldığı bazı sayfalar da hazırlamıştır. Lindqvis, İsveç veri koruma otoritesini (Datainspektion) bilgilendirmeksizin kişisel verileri otomatik yollarla işleme tabii tuttuğu gerekçesi ile para cezasına çarptırılmıştır. Bir internet sitesinde birinden ismi ile bahsetmenin kişisel veri işleme faaliyeti sayılamayacağını savunan Lindqvist, karara itiraz etmiş ve temyiz mahkemesi ABAD'ın görüşünü istemiştir.[61] ABAD kararında, bir internet sayfasında adıyla veya başka bir şekilde tanımlanan bir kişinin; telefon numarası, hobileri gibi bilgilerinin paylaşılmasının Direktif kapsamında kişisel veri olduğunu ifade etmiş ve bunun Direktif'te de GDPR'de de yer alan "evsel amaçlar için kullanma" istinası kapsamında korunmadan muaf olmadığını belirtmiştir.[62]

---

[60] Torre, Lydia F de la, "What is 'personal data' under EU data protection law?", (Erişim) https://medium.com/golden-data/what-is-personal-data-under-eu-data-protection-law-a9983fb2e483, 27 Şubat 2020

[61] Pinsent Masons, "Identifying people on-line violates Data Protection laws, says European Court", (Erişim) https://www.pinsentmasons.com/out-law/news/identifying-people-on-line-violates-data-protection-laws-says-european-court, 13 Ocak 2020

[62] Avrupa Birliği Adalet Divanı 6 Kasım 2003 tarih ve C-101/01 sayılı kararı, 2003.

b. Veri Sahibi

GDPR, veri sahibini verileri toplanan veya işlenen ve doğrudan veya dolaylı olarak tanımlanabilen gerçek kişi olarak tanımlamıştır. Buna ek olarak veri sahibinin kimliğinin belirlenmesinde kullanılabilecek bazı tanımlayıcıları da sınırlı sayıda olmamak kaydıyla saymıştır. GDPR'de geçen örnek tanımlayıcılar; kimlik numarası, konum verileri, çevrim içi tanımlayıcı ya da söz konusu gerçek kişinin fiziksel, fizyolojik, genetik, ruhsal, ekonomik, kültürel veya toplumsal kimliğine özgü faktörlerdir.

GDPR'ye göre yalnızca gerçek ve hayatta[63] olan kişiler veri sahibi olabilirler. Ancak GDPR'nin gerekçesinin 27. Maddesine göre üye devletler ölülerin verilerinin işlenmesine ilişkin düzenlemeler de getirebilirler.

Veri sahibinin kimliğinin "belirlenebilir" olmasına yol açacak tanımlayıcıların neler olduğu sınırlı sayıda sayılmadığından, bazı durumlarda verinin kişisel veri niteliğinde olup olmadığının ayrımına varmak güç olabilmektedir. Bazı hallerde bir veri parçası tek başına bir kişinin kimliğini belirlenebilir kılmazken başka bazı veriler ile birleştirildiğinde tanımlayıcı hale gelebilir. Veya tam tersi bazı hallerde de kesin olarak tanımlayıcı nitelikte olacağını düşündüğümüz verilerin kişisel veri olmaması mümkündür. Örneğin kişinin ismi, ülkede çok insanın kullandığı yaygın bir isimden söz edildiğinde kişisel veri niteliğinde değerlendirilmeyecektir.[64]

c. İşleme Faaliyeti

4. Madde ile İşleme Faaliyeti kavramının kapsamı oldukça geniş tutulmuş, kişisel veriler veya veri setleri üzerinde gerçekleştirilen:

- toplama,
- kaydetme,
- düzenleme,
- yapılandırma,
- saklama,
- uyarlama veya değiştirme,
- elde etme,
- danışma,
- kullanma,

[63] European Union Agency for Fundamental Rights and Council of Europe, 2018: 84.

[64] Kersten, Jenna, "What is GDPR Personal Data and Who is a GDPR Data Subject?", (Erişim) https://kirkpatrickprice.com/blog/what-is-gdpr-personal-data-and-who-is-a-gdpr-data-subject/, 20 Ocak 2020

- iletim yoluyla açıklama,
- yayma veya kullanıma sunma,
- uyumlaştırma ya da birleştirme,
- kısıtlama,
- silme veya imha

gibi tüm işlem ve işlem dizileri, Otomatik veya otomatik olmayan yollarla gerçekleştirip gerçekleştiremediklerinin bakılmaksızın işleme faaliyeti olarak kabul edilmiştir.

Burada dikkat çekilmesi gereken bir husus, GDPR'nin kendisinden önce gelen Direktif ile benzer bir yol izleyerek, verilerin işlenmesi kavramını geniş tutmuş ve düzenlemenin merkezine almış olmasıdır. GDPR, halefi ile benzer biçimde kişisel verilerin depolanmasını işleme faaliyetinin yalnızca bir türü olarak kabul etmiştir.

d. İşleme Kısıtlaması

GDPR ile bir takım kişisel veriler üzerindeki işleme faaliyetlerinin kısıtlanması hakkı veri sahibine tanınmıştır. Veri sahibinin bu hakkı kullanması halinde veri işaretlenir ve üzerinde depolama dışında hiçbir işleme faaliyeti gerçekleştirilemez.[65] Bu hakkın kullanımına ilişkin detaylara çalışmanın ilerleyen bölümlerinde değinilecektir.

e. Profil Çıkarma

Profil çıkarma; özellikle son dönemde gelişen teknolojiler sayesinde, kişinin verileri üzerinde yapılan birtakım hesaplamalar neticesinde kişiye özgü bazı raporlamaların oluşturulması işlemini ifade etmektedir. GDPR, profil çıkarma işlemini *"bir gerçek kişinin işteki performansı, ekonomik durumu, sağlığı, kişisel tercihleri, ilgi alanları, güvenilirliği, davranışları, konumu veya hareketlerine ilişkin hususların analiz edilmesi veya tahmin edilmesi başta olmak üzere söz konusu gerçek kişiye ilişkin belirli kişisel özelliklerin değerlendirilmesi için kişisel verilerin kullanımını ihtiva eden her türlü otomatik kişisel veri işleme biçimidir"* Şeklinde tanımlamak suretiyle hem sınırlı sayıda olmamak kaydı ile bir dizi örneğe yer vermiş hem de var olan verilere dayanarak yapılacak davranış tahminlerini de profil çıkarma işleminin kapsamında değerlendirilmiştir.

[65] Torre, Lydia F de la, "The right to restrict processing under EU data protection law", (Erişim) https://medium.com/golden-data/what-is-the-right-to-restrict-processing-under-eu-data-b6627db1319f, 2020 Ocak 3

f. Takma Ad Kullanımı

GDPR, takma ad kullanımını kişisel verilerin tek başlarına tanımlanmış veya tanımlanabilir bir gerçek kişiyle ilişkilendirilemeyecek şekilde işlenmesi olarak tanımlanmıştır. Bu bağlamda, takma ad kullanılan veriler ile birleştirildiğinde veri sahibinin kimliğinin belirlenmesini sağlayabilecek veriler ek bilgi olarak nitelendirilmiş ve takma ad kullanımı faaliyetlerinde ek bilgilerin ayrı tutulması ile ilgili teknik düzenlemelerin yapılması gibi bazı tedbirler alınması şart koşulmuştur.

Her ne kadar anlamsal olarak yakın olsalar da takma ad kullanarak (pseudonymous) işlenen veri ile anonimleştirilmiş(anonymous) veri arasında GDPR'nin uygulanması bakımından ciddi farklar vardır. Anonimleştirilmiş veri, bir gerçek kişi ile hiçbir şekilde ilişkilendiremez niteliktedir ve bu sebeple GDPR kapsamında kişisel veri sayılmaz. Takma ad kullanarak işlenen veriler ise bir gerçek kişi ile ilişkilendirilebilirler[66] ve bu yüzden GDPR kapsamında kişisel veri olarak değerlendirilirler.[67] Bu sebeple veriyi anonimleştirmek, veri sahibinin kimliğini tamamen gizlemekteyken takma ad kullanarak işlemek yalnızca veri sahibinin tanımlanma riskini azaltmaktadır.[68]

g. Dosyalama Sistemi

İşlevsel veya coğrafi bir temelde merkezi, ademi-merkezi veya dağınık olarak spesifik kriterlere göre erişilebilen yapılandırılmış herhangi bir kişisel veri dizisi GDPR'ye göre dosyalama sistemi olarak kabul edilir.

Bu tanımla ilgili altı çizilmesi gereken en önemli husus, GDPR'nin yalnızca dijital olan dosyalama sistemlerini kapsadığına ilişkin bir ibare olmamasıdır. Başka bir ifade ile GDPR'nin kapsamı geniş tutulduğundan sürecin herhangi bir noktasında veriler kağıt üzerinde dijital

[66] Kuner, Christopher, European data protection law: Corporate compliance and regulation, Oxford University Press, Oxford, 2007, s. 66.
[67] Mourby, Miranda, Mackey, Elaine, Elliot, Mark, Gowans, Heather, Wallace, Susan, E. Bell, Jessica, Smith, Hannah, Aidinlis, Stergios, Kaye, Jane, "Are 'pseudonymised' data always personal data? Implications of the GDPR for administrative data research in the UK", Computer Law & Security Review, Cilt 34, Sayı 2, 2018, s. 232.
[68] Mourby, ve diğerleri, 2018: 223.

olmayan biçimde işlenerek GDPR'nin getirdiği düzenlemelerin etrafından dolanmak mümkün değildir.[69]

h. Kontrolör

GDPR'ye göre kontrolör, kişisel verilerin hangi amaç ve yöntemler ile işleneceklerini belirleyen gerçek veya tüzel kişi yahut kamu kurumu veya diğer herhangi bir organdır.

Maddenin lafzından açık biçimde anlaşıldığı üzere GDPR, yalnızca gerçek kişilere ilişkin verilerin toplanması ve işlenmesinde uygulanmaktadır ancak kontrolörün gerçek kişi olma zorunluluğu bulunmamaktadır. Diğer bir deyişle kontrolör, gerçek kişi olabileceği gibi tüzel kişi de olabilecektir.

Kontrolör, veri işlemeye yönelik kararları alan taraf olup, çoğunlukla veri sahibinin kişisel verilerini teslim ettiği taraf Kontrolörlerdir. Örneğin bir hastanenin web sitesindeki formu kişisel bilgileriniz ile doldurursanız, formu siteye hastane değil web sitesini yapan kişi koyduğu halde, hastane kontrolördür.[70]

i. İşleyici

İşleyici, verileri Kontrolör adına işleyen bir gerçek ya da tüzel kişi, kamu kuruluşu, kurumu veya diğer herhangi bir organdır. Burada altı çizilmesi gereken husus; işleyicinin faaliyetlerini kontrolör adına yürütmesi gerekliliğidir. İşleme faaliyetlerinin amacı ve yöntemi kontrolör tarafından belirlenir. Şayet işleyici, kişisel verilerin işlenmesine ilişkin amaç ve yöntemlerin belirlenmesinde karar mekanizması olarak rol oynuyor ise o halde işleyiciden değil kontrolör haline gelmiştir.

Örneğin, popüler müzik dinleme uygulaması Spotify'ın müşterilerinin dinleme geçmişlerini depolayıp daha sonra Google Cloud tarafından sağlanan bulut hizmetlerini kullanarak müşterilerine müzik zevklerine uygun yeni şarkılar önermektedir. Bu senaryoda

[69]Torre, Lydia F de la, "What is a 'filing system' under EU data protection law?", (Erişim) https://medium.com/golden-data/what-is-a-filing-system-under-eu-data-protection-law-6e7222743f71, 3 Ocak 2020

[70] Calder, 2016: 21.

işleme faaliyetinin amacına ve yöntemine ilişkin kararları veren Spotify kontrolör, işleme faaliyetini Spotify adına gerçekleştiren Google Cloud işleyicidir.[71]

j. Alıcı

Alıcı, GDPR kapsamında aktif rol oynayan taraflardan biri değildir. Ancak kontrolör ve işleyiciler veri sahibini kişisel verilerin açıklandığı alıcılarla ilgili bilgilendirmek zorunda olduğundan önemli bir kavramdır.[72]

GDPR'ye göre alıcı; *"üçüncü bir kişi olsun veya olmasın, kişisel verilerin açıklandığı bir gerçek ya da tüzel kişi, kamu kuruluşu, kurumu veya diğer herhangi bir organ"*dır. Birlik veya üye devlet hukuku uyarınca kişisel verileri bir soruşturma çerçevesinde almaya yetkili kamu kuruluşları alıcı sıfatına sahip olamazlar. Belirtmek gerekir ki somut olayın niteliğine göre alıcı kontrolör veya işleyici de olabilir. Böyle bir durumda, faaliyetleri ikinci madde ile belirlenen kapsamda kaldığı sürece alıcılar da kontrolör ve işleyiciler için konulan kurallara uymak zorundadırlar.

Örneğin kontrolörün veya işleyicinin temsilcisi ve çalışanları alıcı konumundadırlar.[73] Ancak Birlik veya üye devlet hukukuna göre gerekli soruşturmaların yürütmekte olan vergi veya gümrük otoriteleri alıcı konumunda değillerdir.[74]

k. Üçüncü Kişi

Kişisel verilerin işlenmesi bağlamında; veri sahibi, kontrolör, işleyici ve kontrolör ya da işleyicinin doğrudan yetkisi altında olup kişisel verileri işleme yetkisi bulunan kişiler haricindeki bir gerçek veya tüzel kişi, kamu kurumu, kuruluşu veya organlar GDPR kapsamında üçüncü kişi olarak kabul edilirler.

---

[71] Shastri, Supreeth, Wasserman, Melissa, Chidambaram, Vijay, "The seven sins of personal-data processing systems under GDPR", (Erişim) https://arxiv.org/pdf/1903.09305.pdf, 3 Şubat 2020

[72] Waem, Heidi, van Essen, Jacqueline, Wellens, Vincent, "Can the GDPR's Main Players still fulfil their Roles Effectively in an Era Characterised by Developments such as the Blockchain and the Internet of Things?", (Erişim) https://www.e-nautadutilh.com/56/2412/landing-pages/part-2---gdpr.asp?sid=c5019f94-05ff-4f2c-a894-a5ba75ac9208, 5 Şubat 2020

[73] University of Reading, "Data Protection Glossary", (Erişim) https://www.reading.ac.uk/internal/imps/DataProtection/imps-d-p-glossary.aspx, 5t Şubat 2020

[74] Waem, van Essen ve Wellens, 2016.

l. Veri Sahibinin Rızası

GDPR'ye göre kişisel verilerin işlenmesi prensiplerinin başında hukuka uygunluk geldiğinden ve veri sahibinin rızası bir hukuka uygunluk sebebi olduğundan rızanın GDPR'nin uygulanmasındaki en önemli bileşenlerden biri olduğunu söylemek yanlış olmayacaktır. GDPR'nin 4. maddesinde 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"

şeklinde tanımlanmıştır. Düzenlemenin lafzından anlaşıldığı üzere, rızanın niteliği de en az varlığı kadar önemlidir. Bu nedenle veri sahibinin rızasının GDPR kapsamında geçerli sayılması için sahip olması gereken nitelikler çalışmanın ilerleyen bölümlerinde detaylı olarak incelenecektir.

m. Kişisel Veri İhlali

GDPR'de 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 ihlali olarak tanımlanır.

İhlaller ile ilgili en önemli husus, ihlalin tespit edilmesi üzerine kontrolörün yerine getirmesi gereken bildirim yükümlülüğüdür. Kontrolör ve denetim makamı arasındaki bildirim yükümlülüğünde sorumluluklar şu şekildedir;

- Şayet ihlal işleyici seviyesinde olmuşsa (örneğin işleyicinin bilgisayarlarına sızılması gibi) bu durumda işleyici kontrolöre bildirmelidir,
- Kontrolör, ihlalin tespit edilmesinden itibaren en geç 72 saat içerisinde denetim makamına bildirmelidir,
- Yapılacak bildirimde; ihlalin yapısı, ilgili veri sahiplerinin sayısı ve kategorileri, veri koruma görevlisinin irtibat bilgileri, ihlalin olası sonuçları ve alınan veya alınması önerilen önlemler mutlak suretle yer almalıdır.[75]

GDPR, 34. Maddesinde ihlalin gerçek kişilerin hakları ve özgürlükleri açısından yüksek bir riske sebebiyet vermesinin muhtemel olduğu hallerde veri sahibine bildirilmesini de öngörmüştür. Ancak kontrolörün aldığı bazı teknik önlemler (örneğin verilerin şifrelenmesi) neticesinde verinin erişim yetkisi olmayanlarca okunamayacak olması, 34. Maddede atıf

[75] i-scoop, "Personal data breach notification and communication duties under the GDPR", (Erişim) https://www.i-scoop.eu/gdpr/personal-data-breach-notification/, 4 Ocak 2020

yapılan yüksek riskin ortaya çıkmasını engelleyecek tedbirler alınmış olması veya bildirimin ölçüsüz bir çaba gerektirecek olması durumlarında ihlalin veri sahibine bildirilmesi gerekmez.

n. Genetik Veri

Bir gerçek kişinin fizyoloji veya sağlığı ile ilgili eşsiz bilgiler sağlayan ve özellikle söz konusu gerçek kişiden alınan bir biyolojik numunenin analizinden kaynaklanan ve söz konusu kişinin kalıtım yoluyla alınan veya kazanılan özelliklerine ilişkin kişisel veriler GDPR kapsamında genetik veri kabul edilirler.

o. Biyometrik Veri

Bir gerçek kişinin özgün bir şekilde teşhis edilmesini sağlayan fiziksel, fizyolojik veya davranışsal özelliklerine ilişkin olan kişisel veriler biyometrik verilerdir. Örneğin parmak izi veya yüz görüntüsü gibi.

Özellikle akıllı telefonlarda parola yerine kilit açmak için parmak izi ve yüz tanıma gibi özelliklerin kullanılmaya başlanması ve son zamanlarda hayatımıza giren dijital asistanların sesimizi de bir güvenlik mekanizması olarak kullanmanızı[76] sağlaması; biyometrik verilerin işlenmesinin hem teknik hem de hukuki açıdan gün geçtikçe daha önemli hale gelmesine yol açmaktadır.[77]

p. Sağlıkla İlgili Veri

Sağlık hizmetlerinin sağlanması da dahil olmak üzere bir gerçek kişinin sağlık durumuyla ilgili bilgilerin açıklandığı, söz konusu gerçek kişinin fiziksel veya ruhsal sağlığına ilişkin kişisel verilerdir.

q. Asıl Kuruluş

GDPR; kontrolör ve işleyicilerin işleme faaliyetleri ile ilgili olarak Birlik içerisindeki tüm veri koruma otoriteleri ile tek tek muhatap olmalarının önüne geçmek amacıyla, işleyici

[76] Khitrov, Mikhail, "Talking passwords: voice biometrics for data access and security", Biometric Technology Today, Cilt 2013, Sayı 2, 2013, s. 9-11.
[77] Calder, 2016: 19.

ve kontrolörlerin tek bir veri koruma otoritesi ile muhatap olabilmelerine olanak sağlayan (one-stop-shop) bir düzenlemeye sahiptir. Buna göre kontrolör veya işleyici; "asıl kuruluş"larının bulunduğu yerin veri koruma otoritesi ile muhatap olurlar. [78]

Asıl kuruluşun nasıl belirleneceği GDPR'nin 4. Maddesinde açıklanmıştır:

Birden fazla üye devlette işletmesi bulunan bir kontrolör için; Birlik içerisindeki merkezi idare yeri asıl kuruluştur. Ancak kişisel verilerin işlenmesine ilişkin amaçlar ve yöntemlere yönelik kararlar, merkezi idarede değil de Birlik içerisindeki başka bir işletmesinde alınıyor ise kararların alındığı ve uygulatıldığı yer işletmesi asıl kuruluş kabul edilir.

Diğer durum ise birden fazla üye devlette işletmesi bulunan bir işleyici için; kural olan yine birlik içerisindeki merkezi idare yeridir. Şayet işleyicinin birlik içerisinde bir merkezi idare yeri olmayan hallerde, işleyicinin temel işleme faaliyetlerini gerçekleştiği Birlik içerisindeki işletmesidir.

r. Temsilci

Birlik içerisinde kurulu bulunan, 27. madde uyarınca kontrolör veya işleyici tarafından yazılı olarak belirlenen, bu GDPR kapsamındaki yükümlülükleri ile ilgili olarak kontrolör veya işleyiciyi temsil eden bir gerçek veya tüzel kişidir.

s. İşletme

Düzenli olarak bir ekonomik faaliyetle iştigal eden ortaklıklar veya birlikler de dahil olmak üzere hukuki biçimine bakılmaksızın bir ekonomik faaliyetle iştigal eden bir gerçek veya tüzel kişidir.

t. Teşebbüsler Grubu

Bir denetleyici teşebbüs ve onun denetlediği teşebbüslerdir.

[78]Data Protection Comission, "One Stop Shop (OSS)", (Erişim) https://www.dataprotection.ie/en/organisations/one-stop-shop-oss, 10 Eylül 2019

u. Bağlayıcı Kurumsal Kurallar

Bağlayıcı Kurumsal Kurallar; Birlik'in üye devletlerinden birinin topraklarında kurulmuş olan bir kontrolör veya işleyici tarafından, ortak bir ekonomik faaliyet gösterdiği ve üçüncü ülke topraklarında yer alan işletme veya teşebbüslere veri aktarılırken uyulan kişisel veri koruma politikalarıdır. Büyük kuruluşların veya grupların güvenli ve asgari bürokrasi ile uluslararası veri transferi yapabilmesine imkan sağladıkları için önemlidirler. [79]

v. Denetim Makamı

Her üye devlet tarafından kurulan, kişisel verilerin korunmasına yönelik denetlemeleri yapmaktan sorumlu bağımsız kamu kuruluşudur.

w. İlgili Denetim Makamı

Birlik içerisinde her üye devletin kendine ait denetim makamının bulunması, bir kişisel veri işleme faaliyeti söz konusu olduğunda hangi denetim makamının ilgili olduğunu tespit etmek gerekir. Faaliyeti gerçekleştiren kontrolör ve işleyici ile aynı üye devlet topraklarında bulunan denetim makamı bunların faaliyetleri bakımından ilgili denetim makamı olacaktır. Benzer şekilde bir üye devlette ikamet eden veri sahiplerinin işleme faaliyetinden kayda değer biçimde etkilenmesi veya kayda değer biçimde etkilenme ihtimalinin bulunması hallerinde, o üye devletim denetim makamı ilgili denetim makamıdır. Son olarak bir denetim makamına şikayet doğrudan iletilmişse, o denetim makamı ilgili denetim makamıdır.

x. Sınır Ötesi İşleme

Birlik içerisinde uluslararası veri aktarımı neticesinde gerçekleşen kişisel veri işleme faaliyetleri GDPR tarafından sınır ötesi işleme olarak adlandırılmışlardır.[80] Birlik içi veri aktarımı ve işleme faaliyetleri söz konusu olduğunda hangi denetim makamının görevli olacağına ilişkin açıklama çalışmanın önceki bölümlerinde yapılmıştır.

[79] Calder, 2016: 18.
[80] European Union Agency for Fundamental Rights and Council of Europe, 2018: 20.

y. Yerinde ve Gerekçeli İtiraz

Bir taslak karar hakkında; öngörülen eylemin GDPR'ye uygunluğunu inceleyerek, eylemin veri sahibinin hak ve özgürlükleri ile Birlik içerisinde verilerin serbest dolaşımı açısından teşkil ettiği riskleri açık şekilde gösteren itirazdır.

II. BÖLÜM: KİŞİSEL VERİLERİN İŞLENMESİNDE İLKELER

A. KVKK'DA YER ALAN KİŞİSEL VERİLERİN İŞLENMESİ İLKELERİ

1. Genel İlkeler

a. Dürüstlük Kurallarına ve Hukuka Uygun Olma İlkesi

Şüphesiz hukuka ve dürüstlük kurallarına uygunluk, sadece verilerin korunmasının değil bilakis hukukun genel ilkelerindendir. Türk Medeni Kanun'un 2. maddesine göre *"Hukuk, hakkın kötüye kullanılmasını korumaz."*. Kişisel verilerin işlenmesi bağlamında dürüstlük kuralı uygun ilişkin davranış modeli; orta zekalı, makul ve mantıklı bir toplum ferdinin aynı işi yaparken göstereceği davranış modeli olacaktır.[81] Diğer bir deyişle veri işleyenler, ilgili kişilerin çıkarları ile beklentilerini gözetmelidirler. [82]

Dürüstlük kuralına uygunluk ilkesi, ilgili kişinin çıkarlarının gözetilmesi için geniş bir çerçeve çizmek suretiyle, verilerin ilgili kişinin bilgisi dışında yahut onun göremeyeceği biçimde işlemesin önüne geçmiştir. Nitekim verilerin toplanması ve işlenmesi esnasında ilgili kişinin hangi verilerinin toplandığı, bu verilerin hangi amaçlarla ve ne şekilde toplandıkları ile nasıl işlenecekleri konusunda bilgilendirilmesi de bu ilkenin bir parçasıdır. Bilgilendirmenin yapılmaması halinde dürüstlük kuralına uygun olma ilkesi sağlanmayacaktır.[83] Bazı hallerde işleme faaliyeti, görünürde hukuka uygun olmasına rağmen dürüstlük kuralına uygunluk ilkesine aykırı olması mümkündür. Örneğin işlemenin hukuka uygunluk sebebi rıza olarak görünürken aslında kanunda düzenlenen diğer hukuka uygunluk sebeplerinden birine dayanarak işleme yapılmaktaysa, ilgili kişinin rızasını geri çektiğinde işlemenin duracağına inanması sebebi ile dürüstlük kuralına uygunluk ilkesi ihlal edilmiş olacaktır.[84]

---

[81] Oğuz, Habip, "Elektronik Ortamda Kişisel verilerin Korunması, Bazı Ülke Uygulamaları ve Ülkemizdeki Durum", Uyuşmazlık Mahkemesi Dergisi, Cilt 0, Sayı 3, 2014, s. 23

[82] Kişisel Verileri Koruma Kurumu, 2018: 35.

[83] Oğuz, 2014: 23.

[84] Yücedağ, Nafiye, "Kişisel verilerin korunması kanunu kapsamında genel ilkeler", Kişisel Verileri Koruma Dergisi, Cilt 1, Sayı 1, 2019, s. 50.

Dürüstlük kuralına uygunluğun yanı sıra kişisel verilerin işlenmesinde hukuka uygunluk şartının da sağlanmış olması gerekmektedir. Kimi yazarlar bu ilkenin, mevzuattaki tüm hukuk kurallarına aykırılıkları değil yalnızca kişisel verilerin işlenmesi bakımından hukuka uygunluk sebebi olarak belirlenen hallere aykırılık hallerini kapsadığını; aksi halde ilkenin uygulama alanının Kanun'un amaçladığına aykırı biçimde genişleyeceğini de ifade etmektedir.[85]

Gerçekten, kural olan kişisel verilerin işlenmesinin yasak olmasıdır.[86] Bu nedenle kişisel verilerin işlenmesi ancak kanun ile belirlenen hukuka uygunluk sebebinin varlığı halinde mümkün olabilecektir. KVKK, kişisel verilerin işlenmesinin hukuka uygun sayıldığı durumları 5. Madde ile sıralamıştır. Bu maddeye göre kişisel veriler ancak ilgili kişinin açık rızası alınmak suretiyle işlenebilirler. Fakat;

- Kanunlarda açıkça öngörülmesi,
- Fiili imkansızlık nedeniyle rızasını açıklayamayan yahut rızası geçerli olmayan ilgili kişinin veya bir başkanının hayatını yahut beden bütünlüğünü korumak için zorunlu olması,
- Bir sözleşmenin kurulması veya ifası için gerekli olması,
- Veri sorumlusunun hukuki bir yükümlülüğünü yerine getirebilmek için zorunlu olması,
- Verinin ilgili kişi tarafından alenileştirilmiş olması,
- Bir hakkın tesisi, kullanılması veya korunması için zorunlu olması ya da ilgili kişinin temel hak ve özgürlüklerine zarar vermemesi kaydıyla veri sorumlusunun meşru menfaatleri için zorunlu olması

durumlarında ilgili kişinin açık rızası olmaksızın da kişisel verilerin işlenmesi mümkündür.

b. Doğru ve Gerektiğinde Güncel Olma İlkesi

Kişisel verilerin gerektiğinde doğru ve güncel olması ilkesi, toplanan ve işlenen kişisel verilerin gerçeğe aykırı olması sebebi ile ilgili kişinin zarara uğramasının önüne geçmek üzere kabul edilmiş bir ilkedir. Örneğin adresi veya telefon numarası yanlış veya eski şekilde kaydedilen kişi, kendisine ulaşılamaması sebebi ile zarara uğrayabilecektir.[87] Özellikle kişisel verilerin ilgili kişi hakkında karar verilmek üzere kullanılacağı durumlarda bu ilke hayati önem

[85] Yücedağ, Kişisel verilerin korunması kanunu kapsamında genel ilkeler, 2019: 49.
[86] Yücedağ, Kişisel verilerin korunması kanunu kapsamında genel ilkeler, 2019: 48.
[87] Kişisel Verileri Koruma Kurumu, 2018: 36.

arz etmektedir. Bu nedenle veri sorumlusu doğru olmayan kişisel verilerin silinmesi veya düzeltilmesini sağlamalıdır.[88]

Bu bağlamda veri sorumlusu tarafından alınacak önlemlerin niteliği ve yeterliliği somut olaya göre değerlendirilmelidir. Zira verinin doğruluğu ve güncelliğini hem toplama anında hem de işleme esnasında kontrol etmek için alınabilecek önlemler, verinin niteliği başta olmak üzere birçok etkene doğrudan dayanmaktadır. Benzer şekilde verinin güncel olmasının ne zaman "gerektiği"nin değerlendirilmesi de somut olaya göre yapılmalıdır. Ama genel kabul gören görüş verinin güncel olmamasının ilgili kişi üzerinde ağır etkiler yaratacağı hallerin, verilerin güncel olmasını gerekli kıldığı yönündedir.[89]

KVKK, kişisel verilerin doğru ve gerektiğinde güncel olması ilkesi kapsamında hem ilgili kişiye hem de veri sorumlusuna görev yüklemektedir. Veri sorumlusu; ilgili kişinin kendisi ile ilgili saklanan verileri görebilmesini, bu verileri silebilmesini ve istediğinde verileri güncelleyebilmesini sağlayan bir sistem kurmak zorundadır. İlgili kişi ise bu verileri gerektiğinde denetleme ve doğruluğunu sağlama konusunda üzerine düşeni yapmalıdır.[90]

Bu ilke bakımından, diğer ilkelerde olduğu gibi, veri sorumlusunun özen göstermesi gereklidir fakat bu durum veri sorumlusuna ilgili kişinin bilgilerini araştırma hakkı veya yükümlülüğü tanımaz. Zira ilgili kişinin bilgilerinin doğruluğu konusunda veri sorumlusu tarafından araştırma yapılması, ilgili kişinin özel hayatının ihlali anlamına gelebilecektir. Bu yüzden bilgilerin güncelliği ve doğruluğu ile ilgili veri sorumlusu ve ilgili kişi arasında bir sorumluluk dengesi kurulmuştur. Veri sorumlusu, ilgili kişiye kişisel verilerini kontrol etme ve gerektiğinde silme veya düzeltme yapmasına olanak sağlayan araçları sağladığında üzerine düşeni yaptığı kabul edilmektedir.[91] Diğer bir ifade ile bu ilkenin uygulanması yalnızca veri sorumlusunu değil, ilgili kişiyi tarafından da aktif biçimde rol alınmasını gerektirmektedir.

Sosyal medya sitelerinin, kişilerin profiline ilişkin tüm bilgileri kişisel bilgisayarlarına indirebilmelerine ve dolayısıyla sitenin kendileri ile ilgili sahip olduğu tüm verileri inceleyebilmelerine olanak sağlayan sistemleri ile bu verilerin görüntülenerek gerektiğinde düzenlenebilmesine olanak sağlayan "Profil düzenleme" sayfaları bu ilkenin yerine getirilmesi için gerekli sistemlere örnek olarak gösterilebilirler.

---

[88] Yücedağ, Kişisel verilerin korunması kanunu kapsamında genel ilkeler, 2019: 50.
[89] Yücedağ, Kişisel verilerin korunması kanunu kapsamında genel ilkeler, 2019: 51.
[90] Küzeci, Elife, Kişisel Verilerin Korunması, Turhan Kitapevi, Ankara, 2019, s. 213,214.
[91] Küzeci, 2019: 214.

c. Belirli, Açık ve Meşru Amaçlar İçin İşlenme İlkesi

KVKK'nın 4. maddesinin 2. Fıkrasının c bendine göre; kişisel veriler belirli, açık ve meşru amaçlar için işlenirler. Bu ilke kapsamında belirli amaç; işleme faaliyetlerinin niteliğine ve işlenen verilerin içeriğine ilişkin olarak muğlak olmayan bir sınırlama getirilmesini ve kullanıcıya açıklanmasını ifade eder.[92] Dikkat edilmesi gereken husus, amacın belirlenmesi ve açıklanması için uzun ve hukuki dille yazılmış metinler kullanılmasının doğru olmayacağıdır. Zira her ne kadar uzun ve detaylı anlatım amacı daha belirliymiş gibi gösterse de ilgili kişinin anlamasını güç kılabileceğinden belirlilik ilkesinin ihlal edilmesine sebep olabilir.[93]

Amacın belirli olmasının yanı sıra, meşru olması da gerekmektedir. KVKK'nın gerekçesine göre amacın meşru olması; toplanan veya işlenen verinin veri sorumlusunun yaptığı iş ile yahut sunduğu hizmet ile bağlantılı olması gerektiğini ifade etmektedir. Veri sorumlusu önceden kullanıcıyı amacı ile ilgili aydınlatsa dahi, şayet veri işleme amacı veri sorumlusunun faaliyetleri ile örtüşmüyor ise amacın meşruluğundan söz edilemez. Bu yüzden ilgili kişinin rızası olsa dahi bu amaç için veri toplanması ve işlenmesi bu ilkenin ihlali sonucunu doğuracağından kanuna aykırı bir faaliyet olacaktır.

Bu ilke, yukarıda açıklanan dürüstlük kuralına uygunluk kıstasının sağlanmasında yol gösterici olabilir. Açıklandığı üzere kişinin verilerin işlenmesine ilişkin rızası alınırken veri işleme amacı kendisine doğru bir biçimde aktarılmış olmalıdır. Ancak bu haliyle amacın açık olması şartının sağlandığı kabul edilecektir. Bunun doğal bir sonucu olarak, bir amaç için toplanmış verinin başka bir amacı gerçekleştirmek için kullanılması bu ilkenin ihlali anlamına gelmektedir. Şayet daha evvel toplanmış bir veri, rızanın alındığı anda belirli açık olmayan bir başka amaç için işlenecekse ilgili kişiden bu amaca ilişkin yeniden rıza alınması gerekmektedir.

Veri sorumlusuna verilerin hangi amaçlarla işleneceği konusunda ilgili kişiyi aydınlatma yükümlülüğü getirilmek suretiyle, veri sorumlusunun bu ilkeye uygun hareket etmesi güvence altına alınmıştır.

---

[92] Yücedağ, Kişisel verilerin korunması kanunu kapsamında genel ilkeler, 2019: 52.
[93] Yücedağ, Kişisel verilerin korunması kanunu kapsamında genel ilkeler, 2019: 52-53.

d. Amaçla Bağlantılı, Sınırlı ve Ölçülü Olma İlkesi

Kişisel verilerin işlenmesine yönelik ilkelerin en önemlilerinden biri, işlemenin amaçla bağlantılı, sınırlı ve ölçülü olması ilkesidir. Bu ilkenin kabul edilmesi, veri sorumlusu tarafından iki önemli sonuç doğurur. Birincisi, toplanacak kişisel verilerin türlerinin işleme faaliyetleri için belirlenen amaca uygun olmak zorunda olmasıdır. Diğer bir ifade ile kişisel veriler, toplanırken belirli olmayan fakat gelecekte ortaya çıkması muhtemel bir amaç için toplanamazlar. Bu ilkenin veri sorumlusu bakımından ikinci önemli sonucu ise verilerin toplandıktan sonra yalnızca toplandıkları amaçlar için işlenebilmeleridir. Yeni bir amaç dahilinde işleme yapılabilmesi için, verilerin ilk defa toplanması sırasında sağlanması gereken şartlar yine geçerli olacaktır.[94]

Yukarıdaki ilkede açıklandığı üzere kişisel verilerin işlenmesi için veri sorumlusunun amaçlarının meşru olması gerekmektedir. Ancak bu meşru amaçlar doğrultusunda her türlü verinin depolanabileceği ve işlenebileceği anlamına gelmez. Çünkü Kanun, toplanacak kişisel verilerin amaçla bağlantılı olmasını zorunlu kılmıştır. Bir diğer ifade ile amaç meşru olsa bile, bu amaca hizmet etmeyecek nitelikteki herhangi bir verinin toplanması ve işlenmesi söz konusu olamayacaktır. Örneğin evcil hayvan sahiplendirmeyi hedefleyen bir uygulamanın, kayıt olanlardan ırk, din, cinsel yönelim gibi bilgiler istemesi amaçla ilişkili olmadığından bu ilkeye aykırı olacaktır.

Kanunun lafzının "ölçülülük" ibaresine de yer vermiş olması, kimi yazarlarca maddenin geniş biçimde yorumlanmasına sebep olmaktadır. Kanaatimizce de doğru olan bu görüşe göre; KVKK'nın lafzındaki ölçülülük ifadesi, "yeterli", "ilgili" ve "gerekli olanla sınırlı olma" koşullarının hepsini kapsayacak şekilde yorumlanmalıdır.[95]

e. İlgili Mevzuatta Öngörülen veya İşlendikleri Amaç İçin Gerekli Olan Süre Kadar Muhafaza Edilme İlkesi

Amaçla bağlantılı olma ilkesine paralel olarak, toplanan kişisel verilerin mevzuatta öngörülen sürenin veya verinin işlenme amacı için gerekli olan sürenin sonunda yok edilmesi gereklidir. Her ne kadar Kanun'un lafzından sanki bu süreden sonra verilerin tamamen

[94] Kişisel Verileri Koruma Kurumu, 2018: 39.
[95] Yücedağ, Kişisel verilerin korunması kanunu kapsamında genel ilkeler, 2019: 60.

silinmesi gerekliymiş gibi bir sonuç çıksa da Kanun'un gerekçesi incelendiğinde anonim hale getirme yoluyla verilerin daha uzun süreler saklanmasına olanak sağlandığı da görülecektir.[96]

Bu aşamada eğer herhangi bir mevzuatta ilgili amaca ilişkin bir zaman sınırlaması yoksa kanun uygulayıcının hangi amaçla hangi verilerin ne kadar süreyle muhafaza edilebileceğine nasıl karar vereceği akıllara gelebilir. Burada yukarıda açıkladığımız dürüstlük kuralına uygunluk ilkesine başvurulmalı ve orta zekalı normal bir veri sorumlusunun bu amaç için öngöreceği sürenin o amaç için verinin saklanması gerekli olan süre olduğu kabul edilmelidir.

2. Özel Nitelikli Kişisel Verilerin İşlenmesine İlişkin Şartlar

a. Özel Nitelikli Kişisel Verilerin Tanımı

KVKK, özel nitelikli kişisel verilerin işlenmesini de kural olarak yasaklamış üstelik işlemenin hukuka uygunluğunu daha da ağır şartlara bağlayarak özel nitelikli kişisel verilerin işlenmesini zorlaştırmıştır. KVKK'nın gerekçesine göre; alenileştirildiğinde kişinin ayrımcılığa uğramasına ve mağduriyetine sebep olabilecek veriler, "özel nitelikli" kişisel veri niteliğindedirler.[97] Bu tür verilerin işlenmesi daha sıkı şartlara bağlandığından, kanun bu verilerin neler olduğunu sınırlı şekilde sayarak tanımın kapsamının genişletilmesinin önüne geçmiştir. KVKK'da özel nitelikli kişisel verilerin neler olduğu tahdidi olarak sayılmıştır. Buna göre kişinin;

- Irkı,
- Etnik Kökeni,
- Siyasi Düşüncesi,
- Felsefi İnancı,
- Dini,
- Mezhep Veya Diğer İnançları,
- Kılık Ve Kıyafeti,
- Derneklere, Vakıflara Ya Da Sendikalara Üyeliği,
- Sağlık Verileri,
- Cinsel Hayatına İlişkin Verileri,
- Ceza Mahkûmiyeti Ve Güvenlik Tedbirleriyle İlgili Verileri İle
- Biyometrik Ve Genetik Verileri

[96] Kişisel Verilerin Korunması Kanunu Tasarısı (1/541) ve Adalet Komisyonu Raporu, s.8.
[97] Kişisel Verilerin Korunması Kanunu Tasarısı (1/541) ve Adalet Komisyonu Raporu, s.9.

özel nitelikli kabul edilen kişisel verilerdendir.

Özel nitelikli verilerin tahdidi olarak sayılma durumu, KVKK'nın kimi yazarlarca eleştirilmesine yol açmaktadır. Bu eleştirilerden ilki; toplanan verinin özel nitelikli olup olmadığının ancak veri işleyen veya veri sorumlusunun menfaatlerinin, verinin toplanma amacının ve ilgili kişiyi etkileyebilecek olası sonuçların değerlendirilmesi ile belirlenebilecek olduğu yönündedir. Bir diğer bir eleştiri ise kavrama daha amaçsal bir bakış açısı ile yaklaşarak ancak verinin işlenmesindeki amaç, hassas nitelikte bir verinin işlenmesi ise bu durumlarda hukuki korumanın artırılması gerektiğini savunmuştur. Örneğin kişinin gözlüklü fotoğrafı, onun sağlık durumu ile ilgili bilgi içermektedir. Bu halde kişinin gözlüklü fotoğrafı onun ayrımcılığa uğramasına sebep olmayacak dahi olsa özel nitelikli veri olarak mı işleme tabi tutulacaktır? Yine benzer bir durum kişinin herhangi bir fotoğrafının, o kişinin ırkı ile ilgili de bilgi verebileceği göz önünde bulundurularak da söylenebilir. Bu durumda hemen her fotoğrafın özel nitelikli kişisel veri olarak kabul edilmesi gerekir. Bu konuda İngiltere'de verilmiş bir yargı kararı, verinin paylaşım amacı karşısında davacının ırksal kökeni ile ilgili bilginin açıklanmasının önemsiz kaldığına kanaat getirmiştir. Dolayısıyla şayet verinin kullanılma amacı, kişisel veriyi özel nitelikli olarak değerlendirmek değilse, bu tip durumlarda veriler özel nitelikli olarak nitelendirilmeyecektir.[98]

O halde kanun uygulayıcılar, verinin yukarıda sayılan kategorilerle ilişkisine ve kullanım amacına bakarak verin özel nitelikli kişisel veri niteliğinde olup olmadığını yorumlayacaklardır. [99]

b. Özel Nitelikli Kişisel Verilerin İşlenmesi

KVKK'nın 6. Maddesinin ikinci fıkrasına göre; özel nitelikli kişisel veriler, ilgili kişinin açık rızası olmaksızın işleme tabi tutulamazlar. Fakat ilgili kişinin sağlığına ilişkin verileri ve cinsel hayatına ilişkin verileri hariç olmak üzere diğer kişisel veriler; kanunlarda öngörülen istisnai hâllerde açık rıza olup olmadığına bakılmaksızın işleme tabi tutulabilirler. İlgili kişinin sağlığına ve cinsel hayatına ilişkin kişisel veriler ise yalnızca kamu sağlığını korumak, koruyucu hekimlik, teşhis, tedavi ve bakım hizmetlerinin yürütülmesi, sağlık hizmetleri ile finansmanının planlanması ve yönetimi amacıyla, sır saklama yükümlülüğü

[98]Kaya, Cemil, "Avrupa Birliği Veri Koruma Direktifi Ekseninde Hasas (Kişisel) Veriler ve İşlenmesi", İstanbul Üniversitesi Hukuk Fakültesi Mecmuası, Cilt 69, Sayı 1-2, 2011, s. 317. Ve Küzeci, 2019: 244.
[99] Küzeci, 2019: 245.

altında bulunan kişiler veya yetkili kurum ve kuruluşlar tarafından ilgilinin açık rızası aranmaksızın işleme tabi tutulabilir. Tüm bunlara ek olarak özel nitelikli kişisel verilerin işlenebilmesi için Kurul tarafından belirlenen yeterli önlemlerin alınması şarttır.

Özel nitelikli kişisel verilerin, ilgili kişinin açık rızası olmadan işlenebileceği hallere ilişkin 6. Maddede yer alan düzenlemenin lafzı, özel nitelikli olmayan kişisel verilerin işlenmesine yönelik hukuka uygunluk sebeplerinin belirlendiği 5. Maddedeki düzenlemenin lafzı ile çeliştiği gerekçesi ile eleştirilmektedir. Gerçekten, kanun koyucu 5. Maddede "kanunda açıkça öngörülme" şartı getirmiş iken, daha sıkı tedbirler ile korumayı hedeflediği özel nitelikli kişisel veriler için 6. Maddede yalnızca "kanunda öngörülme" şartı getirmiştir. Fakat bizim de katıldığımız görüşe göre özel nitelikli verilerin rıza olmaksızın işlenmesi de evleviyetle kanunda açıkça öngörülmesine bağlıdır[100].

Yukarıda da ifade edildiği üzere, özel nitelikli kişisel verilerin işlenmesi için bir hukuka uygunluk sebebi bulunduğu hallerde bu işleme ancak Kurul tarafından belirlenecek yeterli önlemlerin alınması halinde mümkün olacaktır. Kurul, bu bağlama yeterli önlemlerin neler olduğunu 7 Mart 2018'de Resmi Gazete'de yayımlanan, 31 Ocak 2018 tarih ve 2018/10 Sayılı "Özel Nitelikli Kişisel Verilerin İşlenmesinde Veri Sorumlularınca Alınması Gereken Yeterli Önlemler" kararı ile açıklamıştır. Bahse konu karar, veri sorumlusuna kişisel verilerin güvenliğine ilişkin politika ve prosedürleri belirleme konusuna yükümlülük getirmekte ve aynı zamanda teknik bazı gereksinimler koymak suretiyle yol göstermektedir.

3. Veri Aktarımına İlişkin İlkeler

Kişisel verilerin aktarımı, özellikle yurt dışına aktarımlar söz konusu olduğunda KVKK ve benzeri düzenlemeler ile korunması hedeflenen değerlerin zarar görmesine yol açabilecektir. Zira herhangi bir kişisel verileri koruma düzenlemesi bulunmayan veya var olan düzenlemelere uyulup uyulmadığı bağımsız otoriteler tarafından denetlenmeyen ülkelere veri aktarımı olması durumunda, KVKK kapsamında temel hak ve özgürlükleri korunan vatandaşların hakları ihlal edilebilecektir.

[100] Küzeci, 2019: 350-351.

KVKK'da verilerin aktarılması hususu verilerin yurt içinde aktarılması ve verilerin yurt dışına aktarılması olmak üzere iki şekilde düzenlenmiştir. Veri aktarımı konusunda KVKK tarafından benimsenin kural sadece açık rıza ile mümkün olabileceğidir.

Özel nitelikli kişisel verilerin işlenmesinde olduğu gibi asıl olan açık rızanın alınması olsa da, KVKK bazı istisnai durumlarda açık rıza alınmaksızın veri aktarımı yapılmasını da mümkün kılmaktadır. Yurt içi ve yurt dışı veri aktarımı usulleri arasındaki asıl farklılık da tam olarak açık rıza aranmaksızın veri aktarımı yapılabilecek hallerde karşımıza çıkmaktadır.

a. Yurt İçinde Veri Aktarımı

KVKK 8. Maddenin 1. Fıkrasına göre ilgili kişinin rızası olmaksızın yurt içinde veri aktarımı yapılamaz. Fakat kanun 5. Maddede yer alan hukuka uygunluk sebeplerine gönderme yaparak; kanunlarda açıkça öngörülmesi, fiili imkansızlık nedeniyle rızasını açıklayamayan yahut rızası geçerli olmayan ilgili kişinin veya bir başkanının hayatını yahut beden bütünlüğünü korumak için zorunlu olması, bir sözleşmenin kurulması veya ifası için gerekli olması, veri sorumlusunun hukuki bir yükümlülüğünü yerine getirebilmek için zorunlu olması, verinin ilgili kişi tarafından alenileştirilmiş olması, bir hakkın tesisi, kullanılması veya korunması için zorunlu olması ya da ilgili kişinin temel hak ve özgürlüklerine zarar vermemesi kaydıyla veri sorumlusunun meşru menfaatleri için zorunlu olması durumlarında ilgili kişinin açık rızası olmaksızın da kişisel verilerin yurt içinde aktarılmasını mümkün kılmıştır.

Benzer şekilde 8. Maddede 6. Maddeye de atıfta bulunulmak suretiyle yeterli önlemlerin varlığı halinde; kişinin sağlığı ve cinsel hayatına ilişkin verilerin kamu sağlığının korunması, koruyucu hekimlik, tıbbî teşhis, tedavi ve bakım hizmetlerinin yürütülmesi, sağlık hizmetleri ile finansmanının planlanması ve yönetimi amacıyla, sır saklama yükümlülüğü altında bulunan kişiler veya yetkili kurum ve kuruluşlar tarafından yurt içinde aktarılabileceğini düzenlemiştir.

Kişisel verilerin hukuka aykırı olarak aktarılması, TCK 136. Maddesi kapsamında verileri hukuka aykırı olarak verme, yayma veya ele geçirme suçunu oluşturacaktır.[101]

[101] Korkmaz, 2016: 123.

b. Yurt Dışında Veri Aktarımı

Kişisel verilerin yurt dışına aktarılmasını düzenleyen 9. Maddenin 1. Fıkrası da aslen 8. Madde ile paralel olarak ilgili kişinin açık rızası olmaksızın kişisel verilerin yurt dışına aktarılamayacağını düzenlemektedir. Ve yine 8. Maddeye benzer olarak, hukuka uygun biçimde veri aktarımı için açık rıza aranması şartına, KVKK'nın 5. Ve 6. Maddelerine atıfla birtakım istisnalar getirilmiş ve buna ek olarak da bazı şartlar belirlenmiştir.

Kişisel verilerin, ilgili kişinin rızası olmaksızın yurt dışına aktarılabilmesi için;

- kanunlarda açıkça öngörülmesi,
- fiili imkansızlık nedeniyle rızasını açıklayamayan yahut rızası geçerli olmayan ilgili kişinin veya bir başkanının hayatını yahut beden bütünlüğünü korumak için zorunlu olması,
- bir sözleşmenin kurulması veya ifası için gerekli olması, veri sorumlusunun hukuki bir yükümlülüğünü yerine getirebilmek için zorunlu olması,
- verinin ilgili kişi tarafından alenileştirilmiş olması veya
- bir hakkın tesisi, kullanılması veya korunması için zorunlu olması ya da ilgili kişinin temel hak ve özgürlüklerine zarar vermemesi kaydıyla veri sorumlusunun meşru menfaatleri için zorunlu olması gerekmektedir.

Kişinin sağlığı ve cinsel hayatına ilişkin veriler ise ancak;

- kamu sağlığının korunması,
- koruyucu hekimlik,
- tıbbî teşhis,
- tedavi ve bakım hizmetlerinin yürütülmesi,
- sağlık hizmetleri ile finansmanının planlanması ve yönetimi amacıyla,
- sır saklama yükümlülüğü altında bulunan kişiler veya yetkili kurum ve kuruluşlar tarafından yeterli önlemlerin alınması şartıyla yurt dışına aktarılabilirler.

Yukarıda sayılan hallerden biri veya birkaçının varlığı, kişisel verilerin yurt dışına aktarımı için yeterli değildir. Bunlara ek olarak "verinin aktarılacağı ülkede yeterli korumanın bulunması" veya "yeterli korumanın veri sorumlularınca taahhüt edilmesi ve Kurulun buna izin vermesi" şartları getirilmiştir. Yeterli korunmasının veri sorumlularınca taahhüt edilmesi için hazırlanacak taahhütnamelere ilişkin şartlar ve örnekler Kurum'un internet sitesinde yayınlanmıştır.[102]

[102] Kişisel Verileri Koruma Kurumu, "Yurtdışına Veri Aktarımında Veri Sorumlularınca Hazırlanacak Taahhütnamede Yer Alacak Asgari Unsurlar", (Erişim) https://www.kvkk.gov.tr/Icerik/4236/Yurtdisina-Veri-Aktariminda-Veri-Sorumlularinca-Hazirlanacak-Taahhutnamede-Yer-Alacak-Asgari-Unsurlar, 20 Ocak 2020

Aynı maddenin 3. Fıkrasına göre *"Yeterli korumanın bulunduğu ülkeler Kurulca belirlenerek ilan edilir."* Maddenin devamında Kurulun hangi ülkelerde korumanın yeterli olup olmadığına ilişkin kararını:

- Türkiye'nin taraf olduğu uluslararası sözleşmeleri,
- Kişisel veri talep eden ülke ile Türkiye arasında veri aktarımına ilişkin karşılıklılık durumunu,
- Her somut kişisel veri aktarımına ilişkin olarak, kişisel verinin niteliği ile işlenme amaç ve süresini,
- Kişisel verinin aktarılacağı ülkenin konuyla ilgili mevzuatı ve uygulamasını,
- Kişisel verinin aktarılacağı ülkede bulunan veri sorumlusu tarafından taahhüt edilen önlemleri,

değerlendirmek ve ihtiyaç duyması hâlinde, ilgili kurum ve kuruluşların görüşünü de almak suretiyle karar vereceği belirtilmiştir. Bu çalışmanın yapıldığı tarihte kurulca yeterli korumanın bulunduğu ülkeler listesi henüz açıklanmamıştır.

Verilerin yurtdışına aktarılması konusu, özellikle son dönemde giderek yaygınlaşan bulut teknolojilerinin ülkemizde de yaygın biçimde kullanılması sebebiyle kişisel verilerin korunması anlamında en çok tartışılan konulardan biridir. Özellikle Kurul'un 31/05/2019 tarihinde verdiği 2019/157 Sayılı kararından Sonra Türkiye'deki birçok veri sorumlusu bu konunun üstüne eğilmiştir. Bahsi geçen karar, kurumların elektronik posta sağlayıcı olarak Google (GMail) kullanarak, bu uzantıya sahip posta adresi kullanması hakkındadır. Kararda

> *"Google firmasına ait GMail e-posta hizmeti altyapısının kullanılması durumunda, gönderilen ve alınan e-postaların dünyanın çeşitli yerlerinde bulunan veri merkezlerinde tutulması söz konusu olacağından, böyle bir durumda kişisel verilerin yurt dışına aktarılmış olacağına ve veri sorumlularının söz konusu uygulamayı 6698 sayılı Kişisel Verilerin Korunması Kanununun (Kanun) "Kişisel verilerin yurt dışına aktarılması" başlıklı 9. maddesi hükümlerine uygun olarak gerçekleştirmesine"* [103]

şeklinde hüküm kurulmuştur. Her ne kadar karar, Google üzerinde verilmiş olsa da niteliği itibariyle ülkemizde ve dünyada en çok kullanılan bulut sağlayıcıların (Amazon, Microsoft, Google) tamamını kapsayacaktır. Hal böyle olunca söz edilen sağlayıcılardan

[103] Kişisel Verileri Koruma Kurumu, "Kurumsal e-posta hizmetinin, Google (Gmail) üzerinden yine aynı uzantıya sahip olarak kullanılıp kullanılamayacağına ilişkin Kişisel Verileri Koruma Kurulunun 31.05.2019 tarihli ve 2019/157 sayılı karar özeti", (Erişim) https://www.kvkk.gov.tr/Icerik/5493/2019-157, 18 Kasım 2019

hizmet satın alan veri sorumluları, Kanun'un 9. Maddesine uymakla yükümlü hale gelmişlerdir.

Karar metninde dikkat çeken bir diğer husus, veri merkezlerinin dünyanın çeşitli yerlerinde olduğuna ilişkin bir ifade kullanılmış olmasıdır. Zira dünya çapında hizmet veren birçok bulut sağlayıcı artık veri merkezlerini kurduğu bölgeleri açıklamakta ve kullandığınız hizmete göre verilerimizi hangi veri merkezinde saklamayı tercih ettiğimizi seçmemize imkan vermektedir. Bu bağlamda bir an evvel Kurul tarafından yeterli önlemlerin alındığı kabul edilen ülkeler listesinin yayınlaması, veri sorumlularının KVKK'ya uyum sürecin, kolaylaştıracak ve konuya ilişkin tartışmaları büyük oranda sonlandıracaktır.

B. GDPR'DE YER ALAN KİŞİSEL VERİLERİN İŞLENMESİ İLKELERİ

1. Genel İlkeler

GDPR, 5. Maddesi ile kişisel verilerin işlenmesi bağlamında bazı temel ilkelere uyulmasını koymuştur. Bu prensiler, GDPR'nin devamında detaylandırılan kurallar için başlangıç noktası oluşturmaktadır.[104] Bu prensiplere ilişkin istisnalar ancak Birlik seviyesinde veya ulusal düzeyde çıkarılacak kanunlar ile, temel haklar ve özgürlüklerin özüne saygı göstermek, demokratik bir toplumda meşru menfaatlerin güvence altına alınması açısından gerekli ve orantılı olmak kaydıyla mümkündür. Bu şartların birlikte yer alması gerekir.[105]

GDPR tarafından getirilen ve kişisel verilerin işlenmesi faaliyetleri esnasında mutlak suretle uyulması gereken ilkeler şunlardır:

- Hukuka Uygunluk, Adalet ve Şeffaflık
- Amacın Sınırlandırılması
- Verilerin En Az Seviyeye İndirilmesi
- Doğru ve Gerektiğinde Güncel Olması
- Saklama Süresinin Sınırlandırılması
- Bütünlük ve Gizlilik
- Hesap Verebilirlik İlkesi

[104] European Union Agency for Fundamental Rights and Council of Europe, 2018: 116.
[105] European Union Agency for Fundamental Rights and Council of Europe, 2018: 116.

İlkelerin kapsamlarına geçmeden önce belirtmek gerekir ki; işleme faaliyetleri esnasında hem kendisinin hem de anlaştığı tüm işleyicilerin bu ilkeleri gözetmesinden sorumlu olan taraf kontrolördür.[106]

a. Hukuka Uygunluk, Adalet ve Şeffaflık İlkesi

Bu ilke, kişisel verilerin işlenmesine yönelik tüm faaliyetlerin sahip olması gereken üç unsuru barındırmaktadır. Bunlardan ilki ve belki de en kapsamlısı işleme faaliyetinin hukuka uygun olması gerekliliğidir. GDPR, işleme faaliyetlerinin ne zaman hukuka uygun olduklarını 6. Maddesi ile düzenlemiştir.

GDPR'nin 6. Maddesine göre bir işleme faaliyetinin hukuka uygun olabilmesi için; veri sahibinin rızası altında gerçekleşmesi veya veri sahibinin taraf olduğu bir sözleşmenin, kontrolörün uyması gereken bir yasal yükümlülüğün, veri sahibinin yahut başka bir gerçek kişinin hayati menfaatlerinin, kamu yararına gerçekleştirilen bir görevin ya da (veri sahibinin başka haklarının ağır basmadığı durumlarda) kontrolörün veya üçüncü kişinin meşru menfaatlerinin işleme faaliyetini gerektirmesi gerekir.

Bu ilkeye göre kişisel veri işleme faaliyetlerinin sahip olması gereken diğer bir özellik "adil olma"dır. Her ne kadar tanımı GDPR içerisinde doğrudan yapılmasa da doktrin "adillik"in "farkındalık"a atıf yaptığı kabul edilmektedir.[107] Diğer bir deyişle veri sahibi, kişisel verileri üzerinde yürütülen işleme faaliyetlerine dair bir farkındalığa sahip olmalıdır. Kontrolör; işleme faaliyetlerini gizli olarak gerçekleştirmemeli ve veri sahiplerini olası risklere karşı bilgilendirmelidirler. Buna ek olarak, özellikle işleme faaliyetinin hukuka uygunluğunun temelinde veri sahibinin rızasının yattığı durumlarda, kontrolörler mümkün mertebe veri sahiplerinin isteklerine uygun hareket etmelidirler.[108] Bu unsur, veri sahibinin kişisel verilerinin toplandığını ve işlendiğini unutması daha muhtemelen olan nesnelerin interneti cihazlarında ön plana çıkmaktadır.[109]

Son olarak kişisel verilere yönelik işleme faaliyetlerinin bu ilkeye göre sahip olması gereken diğer bir özellik şeffaflıktır. Direktif kapsamında yalnızca zımnen yer bulan bir

[106] Calder, 2016: 35.
[107] Wachter, Sandra, "The GDPR and the Internet of Things: a three-step transparency model", Law, Innovation and Technology, Cilt 10, Sayı 2, 2018, s. 272.
[108] European Union Agency for Fundamental Rights and Council of Europe, 2018: 118.
[109] Wachter, 2018: 272.

unsurken[110] GDPR'de açıkça düzenlenen şeffaflık unsuru; işleme faaliyetleri öncesinde veri sahibine bilgi vermeyi içerdiği gibi, süreç boyunca veri sahibinin talebi üzerine kendisini bilgilendirmeyi ve gerektiğinde veri sahibinin kendi verilerine erişimini mümkün kılmayı da içermektedir.[111]

Açıklamalarından da anlaşılacağı üzere adillik ve şeffaflık unsurları, veri sahibinin birazdan üzerinde duracağımız haklarından bilgilendirilme ve erişim hakları ile doğrudan ilgilidirler.

b. Amacın Sınırlandırılması İlkesi

Bu ilke, kontrolörlerin topladıkları verileri önceden belirlenmiş ve sınırları çizilmiş amaçlar dışında işlemelerinin önüne geçmeyi amaçlamaktadır. Başka bir ifade kişisel verilerin işlenmelerinin amacı toplandıkları anki amaç ile aynı olduğu müddetçe GDPR ile uyumlu bir işleme faaliyetinden söz edilebilir.[112] Gizlilik bildirimleri, ürün veya hizmetin kullanım şartları ve varsa rıza formları; veri sahibini kişisel verilerinin kullanılacağı amaca yönelik olarak net bir biçimde aydınlatmalı ve kontrolör kişisel verileri işlerken bu belgelerde belirttiği amaca sadık kalmalıdır.[113]

Toplanan veri; şayet asıl toplanma amacı dışında bir amaç ile işlenecekse, önceki işleme faaliyetinin temelindeki hukuka uygunluk nedenine dayanamaz. Yeni amacın meşru kılınması ancak kendine özgü bir hukuki geçerlilik sebebine dayanması ile mümkün olur.[114] Örneğin somut olayda veriler toplanırken asıl amaca yönelik veri sahibinin rızası alınmış ise bu durumda ası amacın dayandığı hukuka uygunluk nedeni veri sahibinin rızasıdır. Ancak her ne kadar rıza olsa bile, yeni amaç bu rızaya dayanarak meşruiyet kazanamaz. Veri sahibinin yeni amaca yönelik olarak bilgilendirilmesi ve kendisinden yeniden rıza alınması gerekir.

[110] oss, W. Gregory, "European Union Data Privacy Law Reform: General Data Protection Regulation, Privacy Shield, and the Right to Delisting", The Business Lawyer, Cilt 72, Sayı 1, 2016, s. 223.
[111] European Union Agency for Fundamental Rights and Council of Europe, 2018: 120.
[112] Wachter, 2018: 273.
[113] It Governance Privacy Team, EU General Data Protection Regulation (GDPR), third edition, IT Governance Publishing, Cambridgeshire, 2019, s.50.
[114] European Union Agency for Fundamental Rights and Council of Europe, 2018: 123.

c. Verilerin En Az Seviyeye İndirilmesi İlkesi

Bu ilkeye göre kontrolör tarafından toplanacak veriler; işleme faaliyetinin amaçları ile ilgili olarak yeterli, yerinde ve gerekli olacak miktar ile sınırlandırılmalıdırlar. İşleme faaliyetlerinin önceden belirlenmiş amaçları ile bağdaşmayan yahut bu amacın yerine getirilmesi için zorunlu olmayan kişisel verilerin toplanması halinde GDPR'ye uygunluktan bahsetmek mümkün olmaz. Örneğin; özellikle büyük şehirlerimizde sıklıkla kullandığımız toplu ulaşım kartlarının üzerinde ve içindeki çipte kartın sahibine ilişkin isim, soyisim, TC Kimlik numarası gibi bilgiler yer alıyor olsaydı, toplu taşımayı kullanan kişinin kimliğinin ulaşım ücretinin ödenmesi işlemi için gerekli olmadığında bahisle GDPR'ye aykırılıktan bahsedilirdi.[115] Burada akıllara kimi illerimizde öğrenciler ve 65 yaşın üzerindeki vatandaşlar için basılan ve üzerinde kimlik bilgileri yer alan özel nitelikli ulaşım kartları gelebilir. Ancak bilindiği üzere bu kartlar, sahiplerinin içinde bulundukları sosyoekonomik şartlar sebebi ile ulaşım hizmetlerini indirimli veya ücretsiz olarak kullanmalarına olanak sağlamaktadır. Kanaatimizce bu durumda kartın sahibinin kişisel verilerinin, ulaşım hizmetinde ücretin ödenmesi bağlamında gerekli olduğu kabul edilebilir.

Son olarak altını çizmek gerekir ki; kontrolörler, işleyiciler ile yaptıkları anlaşmalarda ve bu anlaşmaların uygulanması esnasında da verilerin en aza indirilmesi ilkesine uygun hareket etmelidirler.[116] Örneğin toplanan veriler birden fazla işleyici tarafından kontrolör adına işleniyor ise, her bir işleyiciye kontrolör ile yaptıkları anlaşmaları yerine getirmesi için gereken en az miktarda bilgi aktarılmalıdır.

d. Doğru ve Gerektiğinde Güncel Olma İlkesi

Kontrolör, herhangi bir işleme faaliyetinde bulunmadan önce mutlak suretle verilerin doğru ve güncel olduğundan emin olmalıdır. Bu ilke veri sahibinin işlenen yanlış bilgiler sebebi ile zarar görmesine engel olduğu gibi, kontrolörün de doğru ve güncel olmayan bilgileri işleyerek yanlış sonuçlar elde etmesinin önüne geçer. Örneğin veri sahibinin profilini çıkarmayı hedefleyen bir kontrolörün, yanlış veya eski bilgiler üzerinden çıkarımlar yapması amacına ulaşmasına engel olacaktır.[117]

---

[115] European Union Agency for Fundamental Rights and Council of Europe, 2018: 126.
[116] It Governance Privacy Team, 2019: 52.
[117] It Governance Privacy Team, 2019: 52,53.

Veri sahibinin haklarından "Düzeltme hakkı" bu ilkenin sonuçlarından biridir. Ancak bazı durumlarda verilerin "güncellenmesi" yahut "düzeltilmesi" yasaklanmıştır. Bu veriler genelde geçmişte bir noktanın kaydını tutma amacı ile saklanan verilerdir. Örneğin hasta geçmişinizden önceden geçirdiğiniz bir hastalığın silinmesini/sağlık geçmişi verilerinizin düzeltilmesini talep edemezsiniz.[118]

e. Saklama süresinin sınırlandırılması İlkesi

GDPR, verinin işlenme amacı için gerekli olan sürenin sonunda kişisel verilerin veri sahibinin kimliğinin belirlenebileceği şekilde saklanmasını yasaklamaktadır. Diğer bir ifade ile kişisel veriler veri işleme faaliyeti için yeterli olan sürenin sonunda silinmelidirler. Şayet daha uzun süre depolanacaklar ise bu depolamanın hukuka uygun olabilmesi için anonimleştirilmelidirler.[119]

Saklama süresinin sınırlandırılması ilkesi, bir sistemin veri saklama sisteminin temeline alınması gereken bir ilkedir. Şayet hem veri toplanmasına ilişkin sözleşme ve diğer yasal metinlerin hazırlanmasında hem de işleme faaliyetleri tamamlandığında verilerin GDPR'ye uygun biçimde silinmesi yahut anonimleştirilmesi işleminin tetikleneceği teknik altyapının kurulması gerekir.[120]

f. Bütünlük ve Gizlilik İlkesi

GDPR'de yer alan ve kontrolörü belki de finansal olarak en çok etkileyecek[121] olan ilke bütünlük ve gizlilik ilkesidir. Bu ilkeye göre kontrolör; kişisel verilerin yetkisiz veya yasa dışı işlemeye karşı ve kazara kayba, imhaya veya tahribe karşı korunmasına ilişkin teknik veya yönetimsel tüm tedbirleri almakla mükelleftir.

Burada altı çizilmesi gereken iki nokta vardır. Bunlardan ilki veri ihlalinin yaşanmasının tek başına bu ilkenin ihlal edildiğine dair kanıt olmasıdır. Diğeri ise teknik önlemlere ek olarak; veriye erişimi mecburi olmayan personelin de erişiminin, alınacak yönetimsel tedbirler ile kısıtlamanın gerekmesidir.[122]

---

[118] European Union Agency for Fundamental Rights and Council of Europe, 2018: 128.
[119] European Union Agency for Fundamental Rights and Council of Europe, 2018: 129.
[120] It Governance Privacy Team, 2019: 55-56.
[121] It Governance Privacy Team, 2019: 56.
[122] It Governance Privacy Team, 2019: 57.

g. Hesap Verebilirlik İlkesi

GDPR, kontrolörü bu yukarıda açıklanan ilkelere uymakla yükümlü kıldığı gibi bu ilkelere uyduğunu gösterebilmekle de yükümlü kılmıştır. Diğer bir deyişle ispat yükü kontrolördedir.

Kontrolör; bu ilkeye uyabilmek için öncelikle tüm veri işleme faaliyetlerinin kayıtlarını tutmalıdır. Ayrıca hizmetin veya ürünün temeline gizliliği alarak geliştirme yapması gerekmektedir. Son olarak yüksek riskli veri işleme faaliyetleri için veri koruma etki değerlendirmesinden geçmesi gerekmektedir.[123]

Her ne kadar madde 5 yalnızca kontrolörün hesap verme yükümlülüğünü ele alsa da işleyiciler de hesap verme yükümlülüğüne sahiptirler. Zira yukarıda izah edilen yükümlülüklerin çoğu hem kontrolör hem de işleyiciyi kapsamaktadır.[124]

2. Veri Sahibinin Rızasına İlişkin Şartlar

Önceki bölümde ifade edildiği üzere; işleme faaliyetinin hukuka uygun olması, GDPR'nin 6. Maddesindeki şartlardan birini sağlamasına bağlıdır. Bu madde kapsamında öngörülen hukuka uygunluk şartlarından belki de en önemlisi ilgili kişinin rızasıdır. Rızanın varlığının yanı sıra bazı özelliklere niteliklere de sahip olması gereklidir. Daha spesifik olmak gerekirse GDPR'nin bir hukuka uygunluk sebebi olarak benimsediği rıza türü "aydınlatılmış rıza"dır.[125]

Aydınlatılmış rızanın benimsendiğine ilişkin düzenleme GDPR'nin 7. Maddesinde yer almaktadır. Buna göre; rıza talebi diğer hususlardan açık bir şekilde ayırt edilebilecek bir şekilde, anlaşılır ve kolayca erişilebilir bir biçimde, sade bir dil kullanılarak sunulur. Veri sahibi rıza verdiği işleme faaliyeti ile ilgili açık biçimde aydınlatılmadıysa, rıza mekanizması bir onay eylemine dayanmıyorsa veya veri sahibine rızasını geri çekme imkânı tanınmıyorsa verilen rızanın kişisel verilerin işlenmesi için hukuka uygunluk sebebi olarak değerlendirilmesi mümkün olmayacaktır.

---

[123] Wachter, 2018: 275.

[124] European Union Agency for Fundamental Rights and Council of Europe, 2018: 135.

[125] Bietti, Elettra, "Consent as a Free Pass: Platform Power and the Limits of the Informational Turn", Pace Law Review, Cilt 40, Sayı 1, 2020, s. 337

İnternette sıklıkla gördüğümüz bazı uygulamalardan örnekler vermek gerekirse; web sayfası açıldığında çoktan seçilmiş olan ve kullanıcının rıza verdiğine dair beyan içeren seçim kutuları, GDPR hükümlerine göre geçerli bir rıza beyanı olarak değerlendirilmeyeceklerdir. Benzer şekilde şayet bir işveren, işçilerinin kişisel verilerini işleyebilmek için rızalarının varlığını bir hukuka uygunluk sebebi olarak kullanıyor ise rızanın gerçekten veri sahibinin özgür iradesi ile verilip verilmediğinin objektif olarak değerlendirilmesi gerekmektedir.[126]

Rızanın geçerliliğine ilişkin önemli kararlardan biri Fransız Veri Koruma Otoritesi (CNIL) tarafından Google'a kesilen 57 Milyon dolarlık cezanın kararıdır.[127] GDPR'nin yürürlüğe girmesinden kısa bir süre sonra None Of Your Business ("NOYB") ve La Quadrature du Net ("LQDN") isimli iki grup tarafından; Google'ın reklamları kişiselleştirmek için kullanıcıların verilerini işlemeye yönelik aldığı rızanın GDPR kapsamında geçerli olmadığı gerekçesi ile CNIL'ye şikayette bulunulmuştur. CNIL yaptığı inceleme neticesinde iki nedenden dolayı Google'ın aldığı rızanın geçerli olmadığını vurgulamıştır. İlki veri sahibinin yeterince aydınlatılmadığıdır. Komite; reklamların kişiselleştirilmesi için kişisel verilerin işlendiğine yönelik bilgilendirmenin seyrek olduğunu ve "Reklamların Kişiselleştirilmesi" kısmında bu faaliyetlerin kapsadığı hizmetlerin birden fazla olduğunun (Google arama, YouTube, Google Home vb.) anlaşılmadığının altını çizmiştir. Rızanın geçerli olmamasının ikinci nedeni ise işleme faaliyetlerine özel ve sade nitelikte olmamasıdır. Bir hesap oluştururken "Daha Fazla Seçenek" butonuna basmak suretiyle ulaşılan kısımda kişiselleştirilmiş reklamların gösterilmesine ilişkin ayarlamalar yapmak mümkündür. Ancak yine de GDPR ihlal edilmiştir zira hem kullanıcı bu ayarı görebilmek için "Daha fazla seçenek" butonuna basmak zorundadır hem de kişiselleştirilmiş reklamların gösterilmesine ilişkin rıza kutucuğu varsayılan olarak dolu/seçili biçimde gelmektedir. Son olarak kullanıcı üyelik işlemini tamamlamadan önce "Google'ın Kullanım Şartlarını Kabul Ediyorum" ve "Yukarıda belirtildiği ve Gizlilik Sözleşmesinde açıklandığı üzere kişisel bilgilerimin işlenmesini kabul ediyorum" seçeneğini işaretlemek zorundadır. Ancak bu iki seçenek Google tarafından

[126] Gabel, Detlev, Hickman, Tim, "Chapter 8: Consent – Unlocking the EU General Data Protection Regulation", (Erişim) https://www.whitecase.com/publications/article/chapter-8-consent-unlocking-eu-general-data-protection-regulation?s=consent, 20 Mart 2020

[127] Blackmer, W. Scott, "Google Fined $57 Million under GDPR", (Erişim) https://www.infolawgroup.com/insights/2019/1/23/google-fined-57-million-under-gdpr, 21 Kasım 2019

yürütülen tüm faaliyetlere yönelik bir rıza anlamına geldiğinden "diğer hususlardan açık bir şekilde ayırt edilebilme" niteliğini taşımadığından "özel" nitelikte rıza değildir.[128]

3. Çocuğun Rızasına İlişkin Şartlar

GDPR; veri sahibinin çocuk olması halinde işleme faaliyetlerine yönelik olarak verilecek rızanın niteliği hakkında bazı özel düzenlemeler getirmiştir. Zira GDPR'nin gerekçesinin 38. Maddesinde ifade edildiği üzere çocuklar kişisel verilerinin işlenmesinin risklerini ve işleme faaliyetlerinin sonuçlarını kavrayamayabilirler. GDPR'nin 8. Maddesine göre; işleme faaliyetlerinin hukuka uygunluğunun veri sahibinin rızasına dayalı olduğu hallerde rızanın geçerli olabilmesi için çocuğun en az 16 yaşında olması gerekmektedir. 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.

Burada ispat yükü yine kontrolöre verilmiştir. GDPR'ye göre kontrolör, rızanın çocuğun velisi tarafından verildiğini doğrulamak adına "mevcut teknolojiyi dikkate alarak" "makul çaba" sarf eder. Mevcut teknolojinin hangi unsurlarının bu sürece etki edeceği veya "makul çabanın" kapsamının ne olduğu konuları GDPR ile düzenlenmemiştir.[129]

Çalışmanın önceki kısımlarında ifade edildiği üzere kontrolörün veya üçüncü kişinin meşru menfaatleri de veri işleme faaliyetleri için hukuka uygunluk sebebi teşkil edebilir. Ancak bu şartın sağlanması için, veri sahibinin menfaatlerinin ağır basmaması gerekir. İşte veri sahibinin çocuk olduğu durumlarda, çocuğun menfaatinin bu bağlamda her zaman daha ağır bastığı kabul edildiğinden bu hukuka uygunluk nedeni geçerli olmayacaktır.[130]

---

[128] Commission Nationale de l'Informatique et des Libertés, "The CNIL's restricted committee imposes a financial penalty of 50 Million euros against GOOGLE LLC", (Erişim) https://www.cnil.fr/en/cnils-restricted-committee-imposes-financial-penalty-50-million-euros-against-google-llc, 21 Kasım 2019

[129] Verdoodt, Valerie, Valcke, P (Supervisor), Lievens, E (Co supervisor), Children's Rights And Advertising Literacy In The Digital Era: Towards An Empowering Regulatory Framework For Commercial Communication, Yayımlanmamış Yüksek Lisans Tezi, Ghent University, Faculty Of Law And Criminology, Ghent, 2018, s. 182.

[130] Lievens, Eva, Verdoodt, Valerie, "Looking for needles in a haystack: Key issues affecting children's rights in the General Data Protection Regulation", Computer Law & Security Review, Cilt 34, Sayı 2, 2018, s. 275.

4. Özel Nitelikli Kişisel Verilerin İşlenmesine İlişkin Şartlar

GDPR, bazı kişisel verilerin işlenmesinin diğerlerine nazaran daha riskli olduğunu kabul ederek bu verileri "özel kategorideki kişisel veriler" olarak belirlemiş ve işlenmelerine ilişkin ayrı bir düzenleme getirmiştir. GDPR'nin 9. Maddesine göre özel kategorideki kişisel veriler şunlardır;

- Irk veya etnik köken,
- Siyasi görüşler,
- Dini veya felsefi inançlar,
- Sendika üyeliği,
- Genetik veriler,
- Biyometrik veriler,
- Sağlık ile ilgili veriler,
- Cinsel yaşama veya cinsel eğilime ilişkin veriler.

9. Maddeye göre bu kategorilerdeki verilerin işlenmesi kesinlikle yasaktır. Ancak;

veri sahibinin açık rızası bulunması,

- İşleme faaliyetinin amacının kontrolörün veya veri sahibinin istihdam ve sosyal güvenlik ve sosyal hukuku koruma alanındaki yükümlülüklerinin gerçekleştirilmesi ve haklarının kullanılması amacıyla yürütülmesi,
- Veri sahibinin rıza veremeyecek durumda olduğu hallerde veri sahibi veya başka bir gerçek kişinin hayati menfaatlerinin korunması açısından işleme faaliyetinin gerekli olması,
- İşleme faaliyetinin bir vakıf,
- Birlik veya kar amacı gütmeyen başka bir organ tarafından yürütülen meşru faaliyetleri esnasında verilerin söz konusu organ dışında açıklanmaması koşuluyla gerçekleştirilmesi,
- işleme faaliyetinin veri sahibi tarafından açık bir biçimde kamuya açıklanan kişisel verilerle ilgili olması, yasal iddialarda bulunulması,
- Bu iddiaların uygulanması veya savunulması açısından veya mahkemeler kendi yargı yetkisi çerçevesinde hareket ettiğinde,
- İşleme faaliyetinin gerekmesi, gözetilen amaçla orantılı olan ölçüde kamu yararı adına nedenlerden ötürü işleme faaliyetinin gerekmesi,
- Sağlık veya sosyal bakım sistemleri ve hizmetlerinin yönetilmesi açısından işleme faaliyetinin gerekli olması,
- Halk sağlığı alanında kamu yararına yönelik olarak işleme faaliyetinin gerekmesi, gözetilen amaçla orantılı olan ölçüde kamu yararına yönelik arşivleme amaçları,
- Bilimsel veya tarihi araştırma amaçları ya da istatistiki amaçlar doğrultusunda işleme faaliyetinin gerekmesi durumlarında bu kategorilerdeki veriler işlenebilir.

Burada üzerinde durulması gereken bir konu "açık rıza" kavramıdır. Çalışmanın önceki bölümlerinde ifade edildiği üzere GDPR'ye göre işleme faaliyetinin hukuka uygunluğu için

öngörülen hallerden biri zaten veri sahibinin rızasının varlığıdır. Bu durum işleme faaliyetine konu olacak verinin özel kategorilerden birine ait olup olmamasından bağımsızdır. Özel kategorilerdeki veriler söz konusu olduğunda ise bu rızanın açık (bariz) biçimde verilmesi gerekmektedir.[131]

Bu durumda akıllara "aydınlatma yükümlülüğünün yerine getirilmiş sayılması için de zaten açık bir şekilde işleme faaliyetlerinin açıklanmasına müteakip rıza alındığından, özel kategorilerde farklı bir yol izlenmesine gerek var mı?" sorusu gelebilir. Aradaki fark; özel kategorilerde olmayan verilerin işlenmesinde aydınlatma eyleminin açık bir şekilde (sade bir dil kullanarak, kafa karışıklığına müsaade etmeyecek biçimde) icra edilmesi yeterli iken, özel kategorilerdeki kişisel verilerin işlenmesi için buna ek olarak rıza verme fiilinin de açık (bariz, aleni) olarak gerçekleştirilmesi gerekir. Örneğin bir formda e-posta kutucuğunun üzerinde *"Vermiş olduğunuz e-posta sizinle iletişime geçmek için kullanılacaktır."* şeklinde bir uyarının bulunduğunu görerek bu kutucuğu dolduran veri sahibi açık biçimde aydınlatılmış ve rıza vermiştir. Fakat eğer toplanan veri özel kategorideki bir veri olsaydı, rızanın "Kabul ediyorum" butonuna basılarak verilmesi gerekirdi.[132]

Bazı yazarlar açık rızanın iki aşamalı olarak alınmasının ispat kolaylığı sağlayacağını ifade etmektedirler. Rıza verdiği yönünde irade beyan eden veri sahibine tekrar "Emin misiniz?" şeklinde sorulması buna örnek olarak verilebilir.[133]

5. Mahkumiyet Kararları ve Suçlara İlişkin Kişisel Verilerin İşlenmesi Şartları

GDPR'nin 10. Maddesine göre mahkumiyet kararlarının veya suçlara ilişkin kişisel verilerin işlenmesinin hukuka uygun olabilmesi için;

- İşleme faaliyetinin yetkili makamının kontrolünde yapılması veya
- Veri sahibinin hak ve özgürlüklerinin korunması için yeterli önlemin alınması ve işlemenin Birlik yahut üye devlet hukuku tarafından meşru görülmesi

gerekmektedir. GDPR aynı madde ile, mahkumiyet kararlarına ilişkin kapsamlı bir sicilin ise ancak yetkili makamın kontrolü altında tutulabileceğini de düzenlemektedir.

---

[131] European Union Agency for Fundamental Rights and Council of Europe, 2018: 161.

[132] Datastreams, "Explicit vs. unambiguous consent: what's the difference?", (Erişim) https://www.datastreams.io/explicit-vs-unambiguous-consent-whats-the-difference/, 2 Aralık 2019

[133] i-scoop, "Explicit consent and how to obtain it – new GDPR consent guidelines", (Erişim) https://www.i-scoop.eu/gdpr/explicit-consent/, 1 Ocak 2020

6. Veri Aktarımına İlişkin İlkeler

GDPR, verilerin Birlik içerisinde serbest dolaşımına herhangi ek bir işlem yapılmasına gerek olmaksızın izin vermektedir. Buna ek olarak; Avrupa Ekonomik Alanı Ortak Komitesinin aldığı karar ile GDPR, Avrupa Ekonomik Alanı (AEA) Anlaşması'nın bir parçası haline getirildiğinden verilerin serbest dolaşımı Birlik ülkelerinin yanı sıra Norveç, İzlanda ve Lihtenştayn'ı da kapsamaktadır.[134]

GDPR buna ek olarak verilerin Avrupa Ekonomik Alanı (AEA) dışına aktarılması ihtiyacını da öngörmüş ancak bu tür aktarımların kişisel verilerin korunması bakımından teşkil ettiği riskleri en aza indirmek için ek bazı tedbirler getirmiştir. Bunlar; aktarımın bir yeterlilik kararına dayanması hali, bağlayıcı kurumsal kurallar ve diğer bazı durumlara yönelik istisnalardan oluşmaktadır.

a. Yeterlilik Kararına Dayanan Aktarımlar

GDPR'nin 45. Maddesine göre; Komisyon tarafından hakkında yeterli düzeyde koruma sağladığına yönelik karar alınan ülkelere veya uluslararası kuruluşlara veri aktarımı, herhangi başka bir izin aranmaksızın yapılabilir. Komisyon bu yeterlilik kararlarını alırken aralarında;

- hukukun üstünlüğü,
- insan hakları ve temel özgürlüklere saygı,
- etkili ve uygulanabilir veri sahibi hakları ile kişisel verileri aktarılmakta olan veri sahiplerine yönelik etkili idari ve adli tazmin,
- bağımsız denetim makamının varlığı ve etkili bir şekilde işlev göstermesi

gibi hususların da yer aldığı çok sayıda niteliğin varlığını göz önünde bulundurur.

Şimdiye dek Komisyon tarafından hakkında yeterlilik kararı alınan ülkeler; Andora, Arjantin, Kanada (ticari kuruluşlar), Faroe Adaları, Guernsey, İsrail, Man Adası, Japonya, Jersey, Yeni Zelanda, İsviçre ve Uruguay'dır.[135] Birlik Amerika Birleşik Devletleri'nin kanunlarını yeterli bulmamaktadır ancak Birlik ve ABD arasında veri aktarımının sağlanması için 2016 yılında AB ve ABD Güvenlik Kalkanı Anlaşması yapılmıştır.[136]

---

[134] AEA Komitesi 6 Temmuz 2018 tarih ve 154/2018 numaralı kararı, 2018.

[135] European Comission, "Adequacy decisions", (Erişim) https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en, 20 Ocak 2020

[136] Sullivan, Clare, "EU GDPR or APEC CBPR? A comparative analysis of the approach of the EU and APEC to cross border data transfers and protection of personal data in the IoT era", Computer Law & Security Review, Cilt 35, Sayı 4, 2019, s. 386.

b. Uygun Güvencelere Tabi Olarak Yapılan Aktarımlar

Veri aktarımı yapılacak ülke veya uluslararası kuruluş hakkında 45. Madde kapsamında bir yeterlilik kararı alınmayan hallerde veri aktarımı yapılması, 46. Maddede ifade edildiği üzere uygun güvencelerin sağlamış olmasına yani veri sahibi hakları ve veri sahiplerine yönelik etkili kanun yollarının mevcut olmasına bağlıdır.

Uygun güvenceler;

- Kamu kuruluşları veya organları arasında yasal bağlayıcılığı bulunan ve uygulanabilir bir anlaşma,
- Bağlayıcı kurumsal kurallar,
- Komisyon tarafından kabul edilen veya bir denetim makamı tarafından kabul edilen ve komisyon tarafından onaylanan standart veri koruma şartları (standart data protection clauses),
- Onaylı davranış kuralları ile birlikte üçüncü ülkedeki kontrolör veya işleyicinin veri sahibinin hakları ile ilgili de olmak üzere uygun güvenceler uygulamaya ilişkin bağlayıcı ve uygulanabilir taahhütleri,
- Onaylı bir belgelendirme (certification) mekanizması ile birlikte üçüncü ülkedeki kontrolör veya işleyicinin veri sahibinin hakları ile ilgili de olmak üzere uygun güvenceler uygulamaya ilişkin bağlayıcı ve uygulanabilir taahhütleri

unsurlarından biri ile sağlanabilir.

c. Bağlayıcı Kurumsal Kurallar

Ortak bir ekonomik faaliyette bulunan bir teşebbüsler grubunun veya bir işletmeler grubunun faaliyetleri çerçevesinde kendi içerisinde AEA dışındaki ülkelere veri aktarımı yapması bağlayıcı kurumsal kurallar yoluyla mümkündür. GDPR'nin 47. Maddesine göre bağlayıcı kurumsal kuralların veri aktarımı için hukuki bir temel oluşturabilmesi, yetkin denetim makamınca onaylanmalarına bağlıdır.[137]

Onaylanabilmeleri için bağlayıcı kurumsal kuralların (BKK) hukuksal olarak bağlayıcı, tüm veri koruma ilkelerini kapsayan ve tüm üyelerce uygulanan nitelikte olması gerekmektedir. Aynı zamanda kuralların veri sahibinin haklarını açıkça ifade etmesi ve uygulanabilir biçimde barındırması ve kişisel verilerin korunması prensiplerinin nasıl uygulanacağını açıklaması da

[137] European Union Agency for Fundamental Rights and Council of Europe, 2018: 262.

gerekmektedir. Tüm bunlara ek olarak BKK'ler içerisinde olası bir ihlal durumunda sorumluluk ve tazminat kurumlarının da belirtilmiş olması gerekmektedir.[138]

BKK'lerin en büyük avantajı, özellikle çok uluslu kuruluşların kendi içlerinde olabildiğince az müdahale altında hızlıca veri aktarımı yapmalarını sağlamaktır. Ancak altı çizilmesi gereken bir nokta bu verilerin yalnızca kuruluşun faaliyetleri ve denetim makamının onayladığı kurallar çerçevesinde aktarılabileceğidir. Ayrıca kuralların uygulandığı kuruluşu büyütmek için denetim makamından onay alınması gereklidir.[139]

d. Spesifik Durumlara Yönelik Derogasyonlar

GDPR'nin 49. Maddesine göre bazı hallerde bir yeterlilik kararı yahut güvencelerin sağlanması söz konusu olmadan da AEA dışındaki ülkelere ver aktarımı yapılabilir. Bu haller sınırlı sayıda GDPR'de sayılmışlardır. 49. Maddeye göre;

- Veri sahibinin, aktarımın riskleri konusunda aydınlatılmasına rağmen açık rıza göstermesi,
- Aktarımın veri sahibi ile kontrolör arasındaki bir sözleşmenin yürütülmesi veya veri sahibinin talebiyle alınan sözleşme öncesi tedbirlerin uygulanması açısından gerekli olması,
- Aktarımın kontrolör ile başka bir gerçek veya tüzel kişi arasında veri sahibi yararına yapılan bir sözleşmenin imzalanması veya yürütülmesi açısından gerekli olması,
- Aktarımın kamu yararına ilişkin önemli sebeplerden dolayı gerekli olması;
- Aktarımın yasal iddialarda bulunulması, bu iddiaların uygulanması veya savunulması açısından gerekli olması,
- Veri sahibinin fiziksel veya hukuki olarak rıza veremeyecek durumda olması halinde, aktarımın veri sahibi veya diğer kişilerin hayati menfaatlerinin korunması açısından gerekli olması,
- Aktarımın kamuoyu veya meşru bir menfaati gösterebilen herhangi bir kişi tarafından, istişareye açık olan bir sicilden yapılması

hallerinde veri aktarımı yapılması mümkündür.

Burada önemli konu bu hallerde veri transferi yapılmasının istisnai olmasıdır. Diğer bir deyişle hukuki veri aktarımı için son çare olarak bu derogasyonlara başvurulmalıdır ve büyük çaplı yahut tekrar eden transferlerin hukuka uygunluğu için bu hallerin varlığına dayanılmamalıdır.[140]

[138] European Union Agency for Fundamental Rights and Council of Europe, 2018: 263.
[139] It Governance Privacy Team, 2019: 262.
[140] European Union Agency for Fundamental Rights and Council of Europe, 2018: 264.

C. DÜZENLEMELERİN ÖNGÖRDÜKLERİ İLKELER BAKIMINDAN FARKLARI

1. Hesap Verebilirlik İlkesine Yaklaşımdan Doğan Farklar

Her iki düzenleme de kişisel veriler işleme faaliyetine tabii tutulurken uyulması gereken bazı temel ilkelere yer vermişlerdir. Bu ilkelerin büyük çoğunluğu her iki metinde de benzer şekillerde hükme bağlanmışlardır. Ancak GDPR'de düzenlenmiş olmasına rağmen KVKK da açıkça düzenlenmeyen hesap verebilirlik ilkesi, iki düzenlemenin kişisel verileri korumak amacıyla merkeze aldığı değerin farkını göstermektedir.

GDPR, hesap verebilirlik ilkesini 5. Maddesinin 2. Fıkrası ile düzenler. Buna göre:

> *"Kontrolör, 5. Maddenin 1. Fıkrası ile düzenlenen ilkelere uygun şekilde faaliyet gösterdiğini gösterebilmek zorundadır."*

Kendisinden önce gelen Direktif'te zımnen yer bulmuş olan hesap verebilirlik ilkesi, GDPR'de açık ve ayrı biçimde düzenlenmiştir. Hesap verebilirlik ilkesinin açık ve ayrı biçimde hükme bağlanması, işlemenin hukuka uygunluğunun veri sahibine ve denetim makamına gösterilebilmesinin önemini vurgulamak yoluyla veri sorumlularının şeffaflığa yönelik kapsamlı ve somut adımlar atmasını zorunlu kılmıştır.[141] Bu nedenle veri sorumlusu hukuka uygun işleme yapmanın yanı sıra bunu gerektiğinde ispat edebilmesini sağlayacak teknik ve idari önlemleri de almalıdır.

Şüphesiz içinde bulunduğumuz dönemde işlenen kişisel verilerin miktarı gün geçtikçe artmaktadır ve gelişen teknoloji bu verilerin emsali örülmemiş bir hızda dünyada yayılabilmesini mümkün kılmaktadır. Üstelik bazı sektörlerde online hizmetlerin ücretsiz kullanımı için karşılığında kişisel verilerin işlenmesine izin vermek üzerine kurulu bir ekonomi oluşmuştur. Bu durum; kişisel verilerin korunması kurumunun artık teoriden uygulamaya daha sert ve daha somut tedbirler ile dökülmesini gerektirmektedir ve hesap verebilirlik temelli düzenlemelerin amacı da bunu sağlamaktır.[142]

---

[141] The Office of the Data Protection Authority, " Accountability and Governance", (Erişim) https://odpa.gg/wp-content/uploads/2018/03/Accountability.pdf, 20 Kasım 2019

[142] Article 29 Data Protection Working Party Opinion 3/2010 on the principle of accountability, s. 4,5.

Hesap verebilirlik yalnızca denetim makamına karşı işleme faaliyetlerinin detaylarını ispatlama anlamına gelmez, aynı zamanda aydınlatma yükümlülüğü ve veri sahibinin bilgi edinme hakkı kapsamında veri sahibine karşı hesap verilebilirliği de kapsamaktadır.[143]

Hesap verebilirlik ilkesi sürekliliği içinde barındırır. Diğer bir ifade ile hesap verebilirlik ilkesini benimseyen bir kontrolörün, belli başlı bazı önlemleri aldıktan sonra bir işleme faaliyetinin artık hesap verilebilir nitelikte olduğuna kanaat getirip süreci kendi haline bırakması söz konusu olmayacaktır.[144] Çalışmanın başından beri vurgulandığı üzere hızlı gelişen bir alan olan kişisel verilerin işlenmesi alanında faaliyet gösteren organizasyonların, hesap verebilirlik ilkesi gereğince aldıkları önlemleri de sürecin gelişimi ile aynı hızda denetlemeleri ve güncellemeleri gerekmektedir.

Kontrolörün hesap verebilirlik ilkesi gereğince alabileceği teknik ve idari somut önleme örnek olarak:

- Personelin eğitilmesi,
- İşleme faaliyetlerinin iç denetimlerin yapılması
- Kurum politikalarının hazırlanması,
- İşleme faaliyetlerine yönelik hangi işlemin neden ve nasıl yapıldığına dair belgelerin hazırlanması,

hususlarında politikaların hazırlanması ve gerekli belgelendirmenin yapılması verilebilir.[145] Bu ilkenin bazı yansımalarının, GDPR tarafından kontrolörün yükümlülüğü olarak ayrı ve açık bir biçimde düzenlendiğini;

- 25. Madde ile düzenlenen, kontrolörün gerek verilerin toplanması anından gerekse işlenmesi anından önce hangi verilerin toplanacağını, ne şekilde işleme yapılacağını ve hangi veri koruma önlemlerinin alınacağını belirlemesi anlamında gelen gizliliğe dayalı tasarım (privacy by design) yükümlülüğü,
- Yine 25. Madde ile düzenlenen, kontrolörün yalnızca işleme faaliyeti için gerekliolan verilerin işlenmesini sağlaması anlamına gelen varsayılan olarak gizlilik (privacy by default) yükümlülüğü,
- 30. Madde ile kontrolöre yüklenen, sorumluluğu altında yürüyen veri işleme faaliyetlerinin kaydını tutma yükümlülüğü,
- 35. Madde ile belirlenen, işleme faaliyetinin yüksek riske yol açabileceği durumlarda veri koruma etki değerlendirmesinin yapılması yükümlülüğü,

[143] The Office of the Data Protection Authority, " Accountability and Governance", (Erişim) https://odpa.gg/wp-content/uploads/2018/03/Accountability.pdf, 20 Kasım 2019
[144] The Office of the Data Protection Authority, " Accountability and Governance", (Erişim) https://odpa.gg/wp-content/uploads/2018/03/Accountability.pdf, 20 Kasım 2019
[145] The Office of the Data Protection Authority, " Accountability and Governance", (Erişim) https://odpa.gg/wp-content/uploads/2018/03/Accountability.pdf, 20 Kasım 2019

- 37. Madde ile düzenlenen, gerekli hallerde veri koruma yetkilisi atanması yükümlülüğü

ile görüyoruz. Bunlara ek olarak kontrolörün (varsa) sertifikasyon programlarından faydalanarak GDPR'ye uygun hareket ettiğini belgeleyebilmesine imkan sağlayan 42. Madde de hesap verilebilirlik ilkesi kapsamında değerlendirilebilir.

Hukukumuzda hesap verilebilirlik ilkesinin ayrıca düzenlenmemesi, tabii ki veri sorumlusunun faaliyetlerine ilişkin hesap vermediği yahut herhangi bir yükümlülük altında olmadığı anlamına gelmemektedir. Nitekim KVKK da GDPR'den önceki Direktif'te olduğu gibi hesap verebilirlik ilkesini zımnen benimsemektedir. KVKK'da hesap verilebilirlik ilkesinin yansımalarını;

- Veri sorumlusunun veri güvenliğine ilişkin yükümlülüklerini düzenleyen 12. Maddenin 2. Fıkrasında yer alan:

"Veri sorumlusu, kişisel verilerin kendi adına başka bir gerçek veya tüzel kişi tarafından işlenmesi hâlinde, birinci fıkrada belirtilen tedbirlerin alınması hususunda bu kişilerle birlikte müştereken sorumludur."

- Yine veri sorumlusunun veri güvenliğine ilişkin yükümlülüklerini düzenleyen 12. Maddenin 3. Fıkrasında yer alan:

"Veri sorumlusu, kendi kurum veya kuruluşunda, bu Kanun hükümlerinin uygulanmasını sağlamak amacıyla gerekli denetimleri yapmak veya yaptırmak zorundadır."

hükümlerinde görmekteyiz. 12. Madde ile yüklenen sorumluluklara aykırı davranışların 18. Maddede cezaya bağlanması da bu yükümlülüklerin kanun koyucu tarafından önemli görüldüğünü göstermektedir.

Açıklandığı üzere hesap verebilirlik ilkesini yasal düzenlemenin temel noktalarından biri haline getirmenin; kişisel verilerin korunması noktasında daha somut adımların atılmasını teşvik edeceğinden, gizliliğin sürecin en başından beri varsayılan olarak benimsenmesini sağlayacağından ve kişisel verilerin korunmasının sürekli bir iş olduğunu veri sorumlularına daha net aktaracağından doğru olduğu kanaatindeyiz.

Özellikle internet üzerinden faaliyet gösteren veri sorumluları, GDPR'nin kapsamına giren faaliyetlerde de bulunmaları olası olduğundan hesap verilebilirlik ilkesine uygun hareket etmeleri büyük önem arz etmektedir.

2. Çocukların Kişisel Verilerinin Korunması Konusundaki Farklılıklar

GDPR; çocukların kişisel verilerinin önemini, bu verilerin işlenmesinin teşkil edebileceği riskleri, işleme faaliyetlerinin sonuçlarını veya kişisel verilerini koruma bağlamında sahip oldukları hakları çok iyi bilemeyebileceklerinden[146] hareketle çocukların kişisel verilerin işlenebilmesi, çocuklara yönelik pazarlama faaliyetlerinde kişisel verilerin kullanılabilmesi ya da kişisel veriler kullanılarak çocukların profilinin çıkarılması işlemleri için ayrı ve daha ağır birtakım şartlar öngörmüştür. GDPR'nin 8. Maddesine göre;

- İşleme faaliyeti için dayanılan hukuka uygunluk sebebinin veri sahibinin izni olduğu durumlarda, çocuk tarafından verilen rızanın geçerli olabilmesi için çocuğun en az 16 yaşında olması gerekir.
- Çocuğun 16 yaşından küçük olduğu durumlarda işlemenin rızaya dayalı olarak yapılabilmesi ancak çocuğun velayetine sahip kişinin rıza vermesine veya verilen rızayı onaylamasına bağlıdır.

Çocuğun yaşının 16'dan büyük olduğunu göstermek yahut velayet sahibinden uygun biçimde rıza alındığını belgelemek ile ilgili sorumluluk yine kontrolöre verilmiştir. Bu konuda GDPR, kontrolörün çocuğun yaşının veya rızanın velayet sahibi tarından verildiğinin ispatı için makul çaba göstererek ve mevcut teknolojiden yararlanarak önlem alması gerektiğini vurgulamıştır. Makul çabanın detayları ve mevcut teknolojinin kullanımına yönelik herhangi bir örneğe GDPR kapsamında yer verilmemiştir.[147]

KVKK ise, GDPR'nin halefi olan Direktif'e benzer şekilde çocukların kişisel verilerinin korunmasına yönelik ayrı bir düzenleme getirmemiştir. Bu sebeple hukukumuzda çocukların kişisel verilerinin işlenmesine yönelik verdiği rızanın geçerliliğini değerlendirmek için;

- Çocukların fiil ehliyetlerinin,
- Kişisel verilerin işlenmesine rıza verme hakkının niteliğinin ve
- Çocukların kanuni temsilcilerinin bu hakkı kullanıp kullanamayacağının

mevzuatımızdaki genel hükümler çerçevesinde irdelenmesi gerekmektedir.

Türk Medeni Kanunu'nun (TMK) 11. maddesine göre 18 yaşını doldurmamış kişi çocuk (küçük) kabul edilir. TMK madde 14 ve 16 ise çocukların fiil ehliyetine ilişkin olarak,

[146] GDPR Gerekçe m. 38.
[147] Verdoodt, Valcke ve Lievens, 2018: 182.

çocuğun ayırt etme gücünün bulunup bulunmaması bakımından ikili bir ayrıma gitmiştir. Buna göre;

- Ayırt etme gücüne sahip olmayan çocuğun fiilleri hukuki sonuç doğurmaz, bu nedenle verdiği rıza geçerli değildir.
- Ayırt etme gücüne sahip çocuklar, yasal temsilcilerinin rızası olmadan kişiye sıkı sıkıya bağlı haklarını kullanabilirler.

Görüldüğü üzere, genel hükümlerimize göre çocuğun kişisel verilerinin işlenmesine rıza gösterip gösteremeyeceği aslında rıza verme hakkının hukuki niteliğine (kişiye sıkı sıkıya bağlı haklardan olup olmadığına) ve çocuğun ayırt etme gücüne sahip olup olmadığına göre belirlenecektir.

Kişisel verileri koruma kurumu tarafından hazırlanan yayınlarda da açık biçimde ifade edildiği üzere kişisel verilerinin işlenmesi için rıza verme hakkı kişiye sıkı sıkıya bağlı bir haktır.[148] Kişisel verilerin işlenmesine rıza gösterme hakkının kişiye sıkı sıkıya bağlı bir hak olmasından ve TMK'ya göre ayırt etme gücüne sahip çocuklar kişiye sıkı sıkıya bağlı haklarını kanuni temsilcilerinin rızası gerekmeksizin kullanabilmelerinden hareketle ayırt etme gücüne sahip çocukların kişisel verilerinin işlenmesi için verecekleri rızanın hukuken geçerli olacağı kanaatindeyiz.

Ayırt etme gücüne sahip olmayan çocukların ise kişisel verilerin işlenmesine yönelik verdikleri rızanın hukuki geçerliliği yoktur. Özellikle günümüzde sosyal medya kullanımının artması ile ebeveynlerin ayırt etme gücüne sahip olmayan çocuklarının kişisel verilerini, özellikle fotoğraflarını, veri işlemesi yaptığı bilinen platformlara yüklediğini sıklıkla görmekteyiz. Eğer ayırt etme gücüne sahip çocuk bu işleme faaliyetine rıza gösteremiyor ise rızanın kanuni temsilcileri tarafından verilip verilemeyeceğinin incelenmesi bahse konu platformların faaliyetlerinin geçerliliği bakımından oldukça önemlidir. Burada sorulması gereken soru, kişisel verilerin işlenmesine rıza verme hakkının nispi kişiye sıkı sıkıya bağlı hak mı yoksa mutlak kişiye sıkı sıkıya bağlı hak mı olduğudur. Helvacı'nın yaptığı değerlendirmeye göre kişisel verilerin işlenmesine yönelik rıza verme hakkı nispi kişiye sıkı sıkıya bağlı nitelikte bir haktır[149] ve bunun bir sonucu olarak bu hak çocuğun kanuni temsilcisi tarafından kullanılabilir.

[148] Kişisel Verileri Koruma Kurumu, 2018: 29.

[149] Helvacı, İhsan, Kişisel Verilerin Korunması Kanunu Hakkında Hukuki Mütalaa, TBB, İstanbul, 2018 aktaran Özcan, Göknil, Bankacılık İş Ve İşlemlerinde Kişisel Verilerin Korunması, Yayımlanmamış Yüksek Lisans Tezi, İstanbul Üniversitesi, Sosyal Bilimler Enstitüsü, İstanbul, 2019, s. 51.

Erdoğan, bu konuya velinin çocuk üzerindeki mutlak hakkı perspektifinden yaklaşmış ve çocuğun menfaatleri gözetildiği müddetçe kanuni temsilcisinin bu hakkı kullanabileceğini ifade etmiştir. Ancak verilen rızanın çocuğun menfaatlerine aykırı olması yahut çocuğun bu işlem sebebi ile zarara uğraması hallerinde uğradığı zararın tazminini talep edebileceğini veya kişisel verileri ihlale uğrayan ilgili kişinin haklarından faydalanabileceğini de dile getirmiştir.[150]

Şayet GDPR çocuğun kişisel verilerinin işlenmesi için verilmesi gereken rızanın niteliğini ayrı bir madde ile düzenlememiş olsaydı, pek tabii üye ülkelerin mevzuatlarındaki genel hükümler bu konuya ışık tutabilecekti. Ancak GDPR'nin uygulama alanının geniş olduğu ve her üye ülkenin genel hükümlerinin aynı olmadığı düşünüldüğünde ayrı bir düzenleme getirilerek standartlaştırılması yerinde olmuştur. Buna ek olarak konunun ayrıca düzenlenmesi, hesap verilebilirlik ilkesinde olduğu gibi kanun koyucunun bu konuya ayrı bir önem atfettiğini göstermektedir. Benzer şekilde, GDPR'nin hesap verebilirlik ilkesini kabul etmesine dayanarak çocuğun yaşının veya velisinin rızasının alınıp alınmadığının ispat yükünün kontrolörde olacağı çıkarımı zaten yapılabilecekken, madde içerisinde bu konunun ayrı ve açık biçimde vurgulanması da yine GDPR'nin konuya atfettiği önemi göstermekte ve kontrolörleri bu konuda somut adılar atmaya yönlendirmektedir.

Yukarıda detaylı biçimde irdelendiği üzere KVKK'nın çocukların kişisel verilerine yönelik ayrı bir düzenleme getirmemiş olması, mevzuatımızda bu konuda ayrı bir koruma olmadığı anlamına gelmemektedir. Genel hükümler bu konuda çıkacak uyuşmazlıkların çözümünde kanun uygulayıcılara yol göstereceklerdir. Ancak hem veri sorumlularının bu konuda somut idari ve teknik tedbirleri almalarını teşvik etmek yönünden GDPR'nin yaklaşımının daha uygun olduğu kanaatindeyiz.

3. Özel (Hassas) Nitelikli Kabul Edilen Kategorilerdeki Kişisel Veriler Bakımından Farklılar

Kişisel verilerin işlenmesi söz konusu olduğunda, bazı kategorilerde yer alan kişisel verilerin başkaları tarafından öğrenilmesinin ilgili kişinin veya veri sahibinin mağduriyetine ve/veya ayrımcılığa maruz kalabilmesine neden olabilecek nitelikte olmaları sebebiyle bu

[150] Erdoğan, Canan, "Çocukların Kişisel Verilerinin Korunması (Sosyal Medya Örneği Kapsamında)", DEÜ Hukuk Fakültesi Dergisi, Cilt 21, Sayı Özel, 2019, s. 2461.

kategorilerdeki kişisel verilere diğerlerinden farklı ve daha sert koruma önlemleri getirilmiştir. Çalışmamızda incelediğimiz her iki düzenleme de bunu öngördüğünden özel kategorilerdeki veya hassas nitelikli kişisel verilere dair koruyucu hükümleri ayrı bir madde ile düzenlemişlerdir.

Elbette kişisel verilerin sahip oldukları hassasiyet derecesi ve hangi kategorilerdeki verilerin özel bir korumaya tabi tutulması gerektiği sosyokültürel yapıdan etkileneceğinden ülkeden ülkeye farklılıklar gösterecektir. GDPR öncesi dönemde Avrupa içinde dahi farklılıklar gösteren özel/hassas nitelikli veri kategorileri listesi[151], çalışmamıza konu iki düzenlemede de paralel ve benzer olmakla beraber birebir aynı değildir. Zira düzenlemenin uygulanacağı toplumun değerlerine bağlı olan bu gibi konuların evrensel olarak belirlenmesi beklenemez. Bu nedenle GDPR tarafından hassasiyet addedilmişken KVKK'da ayrıca koruma altına alınmamış yahut KVKK tarafından özel nitelikli görülmüşken GDPR metninde yer bulmamış bazı kişisel veri kategorileri bulunmaktadır.

Yukarıda da değinildiği üzere GDPR'nin 9. maddesine göre özel kategorideki kişisel veriler şunlardır; ırk veya etnik köken, siyasi görüşler, dini veya felsefi inançlar, sendika üyeliği, genetik veriler, biyometrik veriler, sağlık ile ilgili veriler, cinsel yaşama veya cinsel eğilime ilişkin veriler. GDPR, bu kategorilerdeki verilerin işlenmesine, kesin bir biçimde yasak koymuş ancak yukarıda detaylı biçimde açıkladığımız bazı istisnai hallerin varlığı veya veri sahibinin açık rızası olması durumunda işlenmelerine müsaade etmiştir.

KVKK'nın 6. Maddesi ile belirlenen özel nitelikli kişisel veriler ise; kişinin ırkı, etnik kökeni, siyasi düşüncesi, felsefi inancı, dini, mezhep veya diğer inançları, kılık ve kıyafeti, derneklere, vakıflara ya da sendikalara üyeliği, sağlık verileri, cinsel hayatına ilişkin verileri, ceza mahkûmiyeti ve güvenlik tedbirleriyle ilgili verileri ile biyometrik ve genetik verileridir. KVKK bu kategorilerdeki verilerin işlenmesini yasaklamıştır. Ancak GDPR ile benzer şekilde kişinin açık rızasının varlığı ve kanunda öngörülen sınavların bulunduğu hallerde özel nitelikli kişisel veriler işleme tabi tutulabilirler.

Veri Kategorisi	**KVKK**	**GDPR**
Irk	✔	✔
Etnik köken	✔	✔
Siyasi düşünce	✔	✔

[151] Kaya, 2011: 319-320.

Felsefi inanç	✔	✔
Din, mezhep veya diğer inançlar	✔	✔
Dernek, vakıf ya da sendika üyeliği	✔	Yalnızca sendika üyeliği düzenlenmiş
Sağlık	✔	✔
Cinsel hayat	✔	✔
Cinsel yönelim	—	✔
Kılık ve kıyafet	✔	—
Ceza mahkûmiyeti ve güvenlik tedbirleriyle ilgili veriler	✔	Ayrı bir madde ile koruma altına alınmış
Biyometrik ve genetik veriler	✔	✔

Tablo 1: KVKK ve GDPR Kapsamında Özel Nitelikli Olarak Belirlenen Veri Kategorilerinin Karşılaştırılması

Tablo incelendiğinde karşımıza çıkan ilk farklılık GDPR'de tahdidi olarak sayılan özel kategorilerdeki verilerden olan cinsel yönelime ilişkin verilere dair KVKK kapsamında ayrıca bir koruma öngörülmemiş olmasıdır. Ancak bu hususta kanaatimize göre cinsel yönelim de KVKK'da özel nitelikli olarak düzenlenmiş olan cinsel hayata ilişkin verilerden olduğundan, mevzuatımız bakımından da özel nitelikli kişisel veri niteliğinde sayılacaktır.

İki düzenleme arasında özel nitelikli sayılan veriler konusundaki bir diğer farklılık KVKK'da yer alan kılık ve kıyafete ilişkin verilerin özel nitelikli kişisel veri sayılması hususunun GDPR'de bir karşılığı olmamasıdır. Kılık ve kıyafette ilişkin verilerin özel nitelikli sayılması durumu, kültürümüzde kılık kıyafetin kimlik belirleyici nitelikte bir yapıya sahip olmasına dayanmaktadır. Gerçekten, çokuluslu yapıdaki Osmanlı Devleti'nde giyim ve kuşam sosyal, ekonomik, hatta dini bir belirteç; insanları tanımak için bir araç olarak görülmekteydi.[152] Günümüzde de bu durumun geçerli olduğu, kişinin kılık kıyafetine ilişkin verilerin açık rızası olmaksızın işlenmesinin özellikle din ve vicdan hürriyetini ihlal edebileceği açıktır.

Bu nedenlerle 1982 Anayasası'nın 24. Maddesinde yer alan din ve vicdan hürriyeti kapsamında kimsenin dini inanç ve kanaatlerini açıklamaya zorlanamayacağına ilişkin

[152] Aysal, Necdet, "Tanzimat'tan Cumhuriyet'e Giyim ve Kuşamda Çağdaşlaşma Hareketleri", Çağdaş Türkiye Tarihi Araştırmaları Dergisi, Cilt 10, Sayı 22, 2011, s. 3,4.

düzenleme de göz önünde bulundurulduğunda kılık ve kıyafetin özel nitelikli kişisel veriler sayılması kanaatimizce uygundur.

4. Veri Aktarımı Konusundaki Farklılıklar

Teknolojinin gelişmesi ve internetin yaygınlaşması ile beraber kişisel verilerin düzenlemelerin hakimiyet alanı olan bölgelerde korunmasına rağmen internetin hızından ve esnekliğinden faydalanarak uygulama alanının dışına kaçırılmalarının ve bu yolla düzenlemelere aykırı olacak biçimde işleme faaliyetlerine sürdürülmesinin ciddi bir risk teşkil ettiği söylenebilir. Bu nedenle kişisel verilerin korunmasına yönelik düzenlemeler aynı zamanda bu verilerin düzenlemenin hakimiyet alanı içinde ve hakimiyet alanının dışına aktarımlarını da bazı şartlara bağlamaları gerekmektedir.[153]

GDPR bu konuda AEA içerisinde veri aktarımını serbest bırakarak veri sorumlularına kısmi bir serbesti sağlamıştır. Ancak 3. ülkelere veri aktarımı konusunu sıkı tutan GDPR, kişisel verilerin hukuka uygun olarak üçüncü ülkelere aktarılabilmesi için aktarımın bir yeterlilik kararına dayanmasını, uygun güvencelere tâbi olarak yapılmasını, bağlayıcı kurumsal kurallar kapsamında yapılmasını veya kanunda açıkça sayılan istisnai durumlardan birinin varlığını şart koşmuştur.

KVKK ise, veri aktarımının ortaya çıkarabileceği negatif sonuçları öngörmüş ve bu sebeple hem yurt içinde hem de yurtdışında veri aktarımını ilgili kişinin açık rızası olmayan durumlarda kesinlikle yasaklamıştır. Ancak yukarıda detaylı biçimde değinildiği üzere KVKK kapsamında da ilgili kişinin rızası olmaksızın hem yurt içinde hem de yurt dışında veri aktarımı yapılmasını mümkün kılan bazı istisnalar mevcuttur. Yurt içinde veri aktarımının ilgili kişinin rızası olmaksızın yapılabilmesi için KVKK'nın 5. ve 6. maddelerinde öngörülen hukuka uygunluk sebeplerinden birinin varlığı gerekmektedir. Yurt dışına veri aktarımı için ise daha ağır bir tedbir öngörülmüş olup buna göre ilgili kişinin açık rızası olmayan hallerde yurtdışına veri aktarılabilmesi için KVKK'nın 5. ve 6. Maddelerindeki hukuka uygunluk sebeplerine ek olarak aynı zamanda verilerin aktarılacağı ülkede yeterli korumanın bulunması veya yeterli korumanın veri sorumlularınca taahhüt edilmesi ve kurulun buna izin vermesi gerekmektedir.

[153] GDPR Gerekçe m. 101.

İki düzenleme, veri aktarımının düzenlenmesi bakımından uygulama alanlarının ve hukuki niteliklerinin farklı olması sebebiyle birbirinden ayrılmaktadırlar. Her ne kadar KVKK, uygulama alanı içerisinde dahi kişisel verilerin aktarılmasını açık rıza şartına bağladığı için daha sert koşullar altında veri aktarımına izin veriyor gibi gözükse de zaten 5. veya 6. maddedeki hukuka uygunluk sebepleri olmaksızın kişisel verilerin veri sorumlusu tarafından işleme faaliyetlerine tabii tutulmaları hukuka uygun olamayacağından, hukuka uygun veri işleme faaliyeti gerçekleştiren her veri sorumlusunun yurt içinde veri aktarımı yapabileceği söylenebilir. Bu sebeple kişisel verilerin düzenlemenin uygulama alanı içerisinde serbest dolaşımı bakımından KVKK ve GDPR'nin aynı noktada olduğu kanaatindeyiz.

Düzenlemelerin birbirlerinden ayrıldığı asıl nokta kişisel verilerin düzenlemenin uygulama alanı dışına aktarımı noktasıdır. Öncelikle kişisel verilerin yurtdışına veya Birlik dışında 3. ülkelere aktarımı söz konusu olduğunda, akıllara bu işlemin gerekliliği ile ilgili bazı sorular gelebilir. Ancak veri aktarımının birçok sebebi olabileceği gibi bu sebep bir işverenin şirketinde kullandığı e-posta sağlayıcısının, e-postaları yurtdışında bir server'da saklaması kadar basit bile olabilir. Bu nedenle özellikle bulunduğu ülkedeki veri saklama ve işleme hizmetlerinin yeterli olmayabileceği durumlarda her veri sorumlusunun topladığı ve işlediği kişisel verileri yurt dışına aktarması gerekebileceği kabul edilmelidir. Burada veri sorumlularına ölçüsüz birtakım sorumluluklar yüklemek, şüphesiz kişisel verilerin işlenmesinden sağlanacak yararı azaltacaktır.

Verilerin 3. ülkelere aktarımı konusunda GDPR, hem bazı ülkelerle ilgili yeterlilik kararı alarak hem uygun güvencelerin varlığında veri aktarımını mümkün kılarak hem de özellikle çokuluslu şirketlerin kendi içerisinde veri aktarımında bürokrasi engeline takılmalarını engellemek adına bağlayıcı kurumsal kuralları kabul ederek kontrolörler için fayda sorumluluk dengesini kurmaya çalışmıştır.

KVKK da benzer şekilde veri sorumlularının bürokrasi sebebiyle faaliyetlerini durdurmalarının önüne geçmek adına bazı kolaylıklar sağlamıştır. Ancak özellikle işbu çalışmanın hazırlandığı sırada kanunun çıkmasının üstünden yaklaşık 4 yıl geçmesine rağmen hala yeterli korumanın bulunduğu ülkeler listesinin Kurul tarafından yayınlanmamış olması sebebiyle mevzuatımızda yurt dışına veri aktarımı maalesef veri sorumluları bakımında hala kafa karıştırıcı ve külfetli bir durumdadır. Şu halde ilgili kişinin açık rızası olmaksızın yurt

dışına veri aktarımı yapılabilmesinin yolu 9. Maddenin 2. Fıkrasının b bendinde belirtildiği üzere yeterli korumanın taahhüt edilmesi ve Kurul tarafından onaylanması yoludur.[154]

Burada yeterli koruma bulunan ülkelerin listesinin açıklanması bakımından yalnızca idari, teknik ve hukuki değil aynı zamanda siyasi bazı unsurların varlığı da göz ardı edilmemelidir. Özellikle uluslararası hukukta kabul gören ilkelerden biri olan karşılıklılık ilkesinin kişisel verilerin korunmasında yeterli korumaya sahip ülkeler listesi hazırlanırken de etkisi olacaktır. Dolayısıyla mevzuatımızda yer alan kişisel verilerin korunmasına yönelik düzenlemelerin, özellikle GDPR gibi uluslararası alanda etki gösteren ve uygulama alanı geniş olan diğer düzenlemelerle uyumlu olması gerekir ki karşılıklı olarak yeterlilik kararı alınması konusunda siyasi engeller ortaya çıkmasın.

[154] Taahhütname örnekleri için bkz: https://www.kvkk.gov.tr/Icerik/4236/Yurtdisina-Veri-Aktariminda-Veri-Sorumlularinca-Hazirlanacak-Taahhutnamede-Yer-Alacak-Asgari-Unsurlar

III. BÖLÜM: İHLALLER VE YAPTIRIMLAR

A. TARAFLARIN HAK VE YÜKÜMLÜLÜKLERİ

1. KVKK'da Hak ve Yükümlülükler

a. İlgili Kişinin Hakları

KVKK'nın 11. Maddesi ile ilgili kişinin kişisel verileri üzerindeki denetimini artırmak için birtakım haklar verilmiştir. Buna göre ilgili kişi; veri sorumlusuna başvuruda bulunmak yoluyla kişisel verilerinin işlenip işlenmediğini, işlenmişse işlenme amacını ve verilerinin amacına uygun kullanılıp kullanılmadığını, yurt içinde ve yurt dışında verilerinin aktarıldığı üçüncü kişileri öğrenme hakkına sahiptir.

İlgili kişi, kişisel verilerinin işlenmesine yönelik bilgi edinmeye yönelik haklarına ek olarak; gerektiğinde yine veri sorumlusuna başvurmak suretiyle eksik veya yanlış olan kişisel verilerinin düzeltilmesini isteme, işlenme sebebi ortadan kalkan kişisel verilerinin silinmesini veya yok edilmesini talep etme ile düzeltme ve silme gibi işlemlerden üçüncü kişilerin haberdar edilmesini talep etme hakkına da sahiptir.

Münhasıran otomatik işleme yapan sistemler aracılığı ile analiz yapılan durumlarda ilgili kişi, kendisi hakkında aleyhe bir sonuç çıkmasına itiraz edebilir. KVKK'nın gerekçesinde performansı otomatik bir siteme analiz ettirilerek buna göre değerlendirmesi yapılan işçinin, bu hakka dayanarak itiraz edebileceği düzenlenmiştir.

Veri sorumlusuna başvurunun usulü ve esasları Veri Sorumlusuna Başvuru Usul Ve Esasları Hakkında Tebliğ'inde düzenlenir. Tebliğin 4. Maddesinin 2. Fıkrasına göre *"İlgili kişiler, başvurularını Türkçe olarak yapmak kaydıyla bu haktan yararlanabilir."* Tebliğin 5. Maddesi ile ilgili kişinin 11. Madde kapsamındaki taleplerini veri sorumlusuna iletebileceği kanallar sayılmıştır. Buna göre ilgili kişi; 11. Madde kapsamındaki taleplerini yazılı olarak iletebileceği gibi, kayıtlı elektronik posta (KEP) adresi, elektronik ya da mobil imza ile imzalanmış şekilde de iletebilir. Ek olarak, veri sorumlusuna önceden bildirilmiş elektronik

posta adresini kullanmak suretiyle veya başvuru için özel olarak geliştirilmiş bir yazılım vasıtasıyla da iletebilir.

b. Veri Sorumlusunun Yükümlülükleri

(1) Aydınlatma Yükümlülüğü

Şüphesiz, ilgili kişinin işleme faaliyetlerine dair denetimini ve kişisel verilerinin üzerindeki kontrolünü artırmanın en önemli aşaması işleme ile ilgili kişiyi bilgilendirmektir. Nitekim, yukarıda açıklanan kişisel verilerin işlenmesi ilkelerinin birçoğunun temelinde de ilgili kişinin bilgilendirilmesi yatmaktadır. Bu kapsamda kanun koyucu, veri sorumlusunu verileri topladığı esnada ilgiliyi bilgilendirmek ile sorumlu tutmuştur.

KVKK'nın 10. Maddesinde yer verilen aydınlatma yükümlülüğüne göre ilgili kişilere:

- Veri sorumlusunun ve varsa temsilcisinin kimliği,
- Kişisel verilerin işlenme amacı,
- İşlenen kişisel verilerin aktarılacağı kişiler,
- Verilerin hangi yöntemle ve hangi hukuki dayanak ile toplandığı ve
- İlgili kişinin KVKK'nın 11. Maddesi ile tanınan hakları

hususlarındaki bilgiler, verilerin elde edilmesi esnasında ilgili kişiye verilmek zorundadır.

Aydınlatma yükümlülüğünün yerine getirilmesi, ilgili kişinin onayına tabii değildir. Veri sorumlusu tek taraflı irade beyanı ile bu yükümlülüğünü yerine getirebilir. Ancak bu yükümlülüğün yerine getirildiğine ilişkin ispat yükü veri sorumlusundadır.[155]

(2) Veri Güvenliğine İlişkin Yükümlülükler

Kanun koyucu ilgili kişiye verdiği kişinin verileri üzerindeki hakimiyetini kuvvetlendirmeyi amaçlayan hakların yanı sıra, verilerin güvenliğini sağlamak üzere veri sorumlularına da çok sayıda idari ve teknik yükümlülük getirmiştir. KVKK'nın 12. Maddesine göre veri sorumlusu kişisel verilerin hukuka aykırı olarak işlenmesini ve bu verilere hukuka aykırı olarak erişilmesini önlemek ve kişisel verilerin muhafazasını sağlamak amacıyla teknik ve idari tedbirleri almak zorundadır. Buna paralel olarak şayet veri sorumlusu bir kurum veya

[155] Turan, Metin, Karşılaştırmalı Hukukta Kişisel Verilerin Korunması, Seçkin Yayınevi, Ankara, 2019, s. 86.

kuruluş adına hareket ediyor ise kendi kuruluşlarında KVKK'nın uygulanmasını sağlamak zorundadırlar. Veri sorumlularının öğrendikleri kişisel verilere ilişkin sır saklama yükümlülükleri vardır ve bu yükümlülük görevden ayrılsalar dahi devam eder.

Veri güvenliği bakımından belki de en çok karşılaşılan durumlardan biri verilerin sızdırılması hadiselerinin kamuoyundan gizlenmesidir.[156] Kanun koyucu bunu öngörmüş ve veri sorumlusunu; işlenen verilerin hukuka aykırı olarak başkaları tarafından ele geçirildiği hallerde ilgilisine ve Kurul'a bildirmekle sorumlu tutmuştur. Bildirim yükümlülüğü ile sızıntı sebebi ile oluşacak zararın en aza indirilmesi ve gelecekte olan sızıntıların önlenmesi yolunda adımlar atılması amaçlanmıştır.[157]

(3) İlgili Kişi Tarafından Yapılan Başvuruların Cevaplanması ve Kurul Kararlarının Yerine Getirilmesi Yükümlülüğü

KVKK'nın 13. maddesine ve Veri Sorumlusuna Başvuru Usul ve Esasları Hakkında Tebliğe göre veri sorumluları, ilgili kişi tarafından yapılan başvuruları en geç otuz gün içerisinde cevaplamak durumundadırlar.

İlgili kişinin cevabı yetersiz bulması veya cevap alamaması üzerine Kurul'a başvurduğu hallerde, Kurul veri sorumlusunun bir ihlali ortadan kaldırması yönünde karar verirse bu karar en geç otuz gün içerisinde veri sorumlusu tarafından yerine getirilir.[158]

(4) Veri Sorumluları Siciline Kaydolma Yükümlülüğü

Veri işleyen gerçek ve tüzel kişiler, KVKK'nın 16. Maddesine göre Başkanlık tarafından tutulan veri sorumluları siciline kaydolmak zorundadırlar. Veri Sorumluları Sicili Hakkında Yönetmelik ile bu zorunluluğa bazı istisnalar getirilmiş ve işlenen kişisel verilerin niteliği, sayısı ve işlemenin amacı gibi birtakım kriterlere göre bazı veri sorumluları 16. Madde ile getirilen kayıt yükümlülüğünden muaf tutulmuşlardır.[159]

---

[156] Küzeci, 2019: 358.

[157] Küzeci, 2019: 359.

[158] Kişisel Verileri Koruma Kurumu, "Kanun Kapsamında Hak Ve Yükümlülükler", (Erişim) https://www.kvkk.gov.tr/Icerik/4192/Kanun-Kapsamindaki-Hak-ve-Yukumlulukler, 20 Şubat 2020

[159] Kişisel Verileri Koruma Kurumu, "Kanun Kapsamında Hak Ve Yükümlülükler", (Erişim) https://www.kvkk.gov.tr/Icerik/4192/Kanun-Kapsamindaki-Hak-ve-Yukumlulukler, 20 Şubat 2020

(5) Bildirim Yükümlülüğü

İşlenen kişisel verilerin kanuna aykırı olarak herhangi bir şekilde üçüncü kişilerce ele geçirilmesi durumunda veri sorumlusu, en kısa sürede ilgili kişiye ve Kurul'a bildirmek zorundadır.[160]

2. GDPR'de Hak ve Yükümlülükler

a. Veri Sahibinin Hakları

GDPR, veri sahibinin haklarını kendisinden önceki düzenlemelere göre büyük ölçüde artırmasına karşın, bu haklar ile bilginin serbest akışı hakkı arasında da bir denge kurmaktadır. Veri sahibinin haklarının genişlemesi, veri sahibinin toplanan kişisel verileri ile neler yapıldığı ile ilgili daha derinlemesine bilgi sahibi olması ve genel olarak kişisel verileri üzerinde daha fazla kontrol sahibi olması sonucunu doğurmaktadır.[161]

GDPR ile veri sahibine tanınan hakların incelenmesi, GDPR'de kişisel verilerin işlenmesi faaliyetlerinin sınırlarının ve faaliyetlerin gerçekleştirilebilmesi için Kontrolörün yerine getirmesi gereken yükümlülüklerin anlaşılması bakımından büyük önem arz etmektedir.

(1) Bilgilendirilme Hakkı

Veri sahibinin verisi üzerinde bir kontrole sahip olabilmesi için mutlak suretle verilerin toplanma ve işlenme biçimleri ile ilgili bilgiye sahip olması gerekir.[162] Bu bağlamda bilgilendirilme hakkı ve bu hakka ilişkin mekanizmalar kendisinden önce yürürlükte olan Direktif'te olduğu gibi GDPR'de de yer almaktadır.

Bilgilendirilme hakkının GDPR içerisindeki ilk dayanağı, yukarıda açıklanan şeffaflık ilkesinin düzenlendiği 5. Maddedir. Tüzüğün 13. ve 14. Maddeleri, veri sahibinin bilgilendirilme hakkını kişisel verinin elde edildiği kaynağa göre iki ayrı şekilde

---

[160] Kişisel Verileri Koruma Kurumu, "Kanun Kapsamında Hak Ve Yükümlülükler", (Erişim) https://www.kvkk.gov.tr/Icerik/4192/Kanun-Kapsamindaki-Hak-ve-Yukumlulukler, 20 Şubat 2020

[161] Calder, 2016: 37,38.

[162] Bârsan, Maria-Magdalena, "A Partial Overview of the Data Subjects' Control over Their Personal Data under the General Data Protection Regulation", Bulletin of the Transilvania University of Braşov Series VII: Social Sciences., Cilt 11, Sayı 2, 2018, s. 130.

düzenlemektedirler. Tüzüğün 13. Maddesine göre kişisel verilerin veri sahibinden toplanması halinde;

- Kontrolörün ve varsa kontrolörün temsilcisinin kimlik ve irtibat bilgileri,
- Varsa veri koruma görevlisinin irtibat bilgileri,
- Kişisel verilerin planlanan işlenme amaçlarının yanı sıra işleme faaliyetinin yasal dayanağı,
- İşleme faaliyetinin GDPR'nin 6. Maddesinin 1. Fıkrasının f bendinde düzenlendiği şekilde meşru menfaatlere dayanması durumunda, gözetilen meşru menfaatlerin neler olduğu ve kimler tarafında gözetildiği,
- Varsa, kişisel verilerin alıcıları veya alıcı kategorileri,
- Uygun olduğu hallerde, kontrolörün kişisel verileri üçüncü bir ülke veya uluslararası kuruluşa aktarmayı amaçladığı ve komisyon tarafından bir yeterlilik kararı verilip verilmediği ya da, 46 veya 47. Maddelerde veya 49(1) maddesinin ikinci alt paragrafında atıfta bulunulan aktarımlar olması halinde, uygun veya münasip güvencelere ilişkin atıf ve bunların bir nüshasının elde edilme yolları veya bunların nerede sağlandığı,
- Kişisel verilerin saklanacağı süre veya, bunun mümkün olmaması halinde, bu sürenin belirlenmesi amacı ile kullanılan kriterler,
- Kontrolörden kişisel verilere erişim ve kişisel verilerin düzeltilmesi ya da silinmesini veya veri sahibi ile ilgili işleme faaliyetinin kısıtlanmasını talep etme ya da işleme faaliyetine itiraz etme hakkının yanı sıra verilerin taşınabilirliği hakkının varlığı,
- İşleme faaliyetinin veri sahibinin rızasına dayandığı hallerde, rızanın geri çekilmesinden önce rızaya dayalı olarak gerçekleştirilen işleme faaliyetinin hukuka uygunluğu etkilenmeden, herhangi bir zamanda rızayı geri çekme hakkının varlığı,
- Bir denetim makamına şikayette bulunma hakkı,
- 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,
- Profil çıkarma da dahil olmak üzere otomatik karar verme mekanizmalarının varlığı ve, en azından bu hallerde, yürütülen mantığa ilişkin anlamlı bilgilerin yanı sıra söz konusu işleme faaliyetinin veri sahibi açısından önemi ve öngörülen sonuçları

hususlarına ilişkin bilgiler, Kontrolör tarafından veri sahibine sağlanmalıdır. GDPR'nin 14. Maddesi ise, kişisel verilerin veri sahibinden alınmadığı durumlarda veri sahibine sağlanacak bilgileri şu şekilde sıralamıştır;

- Kontrolörün ve (varsa) kontrolörün temsilcisinin kimlik ve irtibat bilgileri,
- Varsa, veri koruma görevlisinin irtibat bilgileri,
- Kişisel verilerin planlanan işlenme amaçlarının yanı sıra işleme faaliyetinin yasal dayanağı,
- İlgili kişisel veri kategorileri,
- Varsa, kişisel verilerin alıcıları veya alıcı kategorileri,

- Uygun olduğu hallerde, kontrolörün kişisel verileri üçüncü bir ülke veya uluslararası kuruluşa aktarmayı amaçladığı ve komisyon tarafından bir yeterlilik kararı verilip verilmediği ya da, 46 veya 47. Maddelerde veya 49(1) maddesinin ikinci alt paragrafında atıfta bulunulan aktarımlar olması halinde, uygun veya münasip güvencelere ilişkin atıf ve bunların bir nüshasının elde edilme yolları veya bunların nerede sağlandığı,
- Kişisel verilerin saklanacağı süre veya, bunun mümkün olmaması halinde, bu sürenin belirlenmesi amacı ile kullanılan kriterler,
- İşleme faaliyetinin GDPR'nin 6. Maddesinin 1. Fıkrasının f bendinde düzenlendiği şekilde meşru menfaatlere dayanması durumunda, kontrolör veya üçüncü bir kişi tarafından gözetilen meşru menfaatler,
- Kontrolörden kişisel verilere erişim ve kişisel verilerin düzeltilmesi ya da silinmesini veya veri sahibi ile ilgili işleme faaliyetinin kısıtlanmasını talep etme ve işleme faaliyetine itiraz etme hakkının yanı sıra verilerin taşınabilirliği hakkının varlığı,
- İşleme faaliyetinin veri sahibinin rızasına dayandığı hallerde, rızanın geri çekilmesinden önce rızaya dayalı olarak gerçekleştirilen işleme faaliyetinin hukuka uygunluğu etkilenmeden, herhangi bir zamanda rızayı geri çekme hakkının varlığı,
- Bir denetim makamına şikayette bulunma hakkı,
- Kişisel verilerin hangi kaynaktan alındığı ve uygun olduğu hallerde, kişisel verilerin kamunun erişebileceği kaynaklardan gelip gelmediği,
- Profil çıkarma da dahil olmak üzere otomatik karar vermenin varlığı ve en azından bu hallerde, yürütülen mantığa ilişkin anlamlı bilgilerin yanı sıra söz konusu işleme faaliyetinin veri sahibi açısından önemi ve öngörülen sonuçları.

Yukarıda ifade edildiği üzere, GDPR'den önce Direktif de veri sahibinin bilgilendirme hakkını düzenlenmiştir. Bu bağlamda Direktif'in yürürlükte olduğu tarihlerde Avrupa Birliği Adalet Divanı tarafından verilen kararlar, bize GDPR kapsamında da bu hakkın uygulanması ile ilgili yol gösterici olmaktadır. ABAD, bir kararında veri sahiplerinin bilgilendirilme hakkının uygulanmasının diğer hakları uygulanması için de gerekli olması bakımından büyük önem arz ettiğini ifade etmiştir.[163] Buradan hareketle bilgilendirme hakkının, veri sahibinin kişisel verilerini koruma anlamında sahip olduğu en öncelikli hakkı olduğunu söylemek yanlış olmayacaktır.

Altını çizmekte fayda var; 13 ve 14. Maddeler ile düzenlenen bilgilendirilme şartları veri sahibinin herhangi bir başvurusuna gerek olmaksızın Kontrolör tarafından uyulması gerekli yükümlülüklerdir. Veri sahibinin bu bilgilendirmeyi özel olarak talep etmesine gerek yoktur.[164]

[163] Avrupa Birliği Adalet Divanı 1.10.2015 tarih ve C-201/14 sayılı kararı, 2015.
[164] Bârsan, 2018: 130.

Son olarak belirtmek gerekir ki kontrolörün veri sahibini bilgilendirmek zorunda olmadığı bazı istisnai durumlar da GDPR'de düzenlenmiştir. Şayet kişisel veri, veri sahibinden elde edilmişse ancak veri sahibi 13. Madde ile belirlenen tüm bilgilere haiz ise 13. Madde ile getirilen yükümlülükler uygulanmaz. Eğer kişisel veri, veri sahibi dışından birinden elde edilmişse ve

- Veri sahibinin halihazırda bilgisinin olması,
- GDPR'nin 89. Maddesinde belirlenen koşullara ve güvencelere tabi olarak kamu yararına arşivleme amaçları, bilimsel veya tarihi araştırma amaçları ya da istatistiki amaçlar başta olmak üzere söz konusu bilgilerin sağlanmasının imkânsız olması veya ölçüsüz bir çaba gerektirmesi halinde,
- Elde etme veya açıklamanın kontrolörün tabi olduğu ve veri sahibinin meşru menfaatlerinin korunması amacıyla uygun tedbirler sağlanan Birlik veya üye devlet hukukunda açık bir şekilde ortaya konması veya
- Kişisel verilerin yasal bir gizlilik yükümlülüğü de dahil olmak üzere Birlik ya da üye devlet hukuku ile düzenlenen bir mesleki gizlilik yükümlülüğüne tabi olarak gizli kalmasının gerekmesi

Hallerinden biri oluşmuşsa, bu durumda 14. Madde ile getirilen yükümlülükler uygulanmaz.

(2) Erişim Hakkı

Veri sahibinin, kişisel verilerinin işlenip işlenmediği konusunda kuşku duyması halinde Kontrolöre başvurmak yoluyla bu yönde bilgi edinmesi ve Kontrolörün kendisi hakkında sahip olduğu kişisel verileri talep etmesi mümkündür. Erişim hakkı olarak isimlendirilen bu hak, GDPR'nin 15. Maddesi ile düzenlenmiştir. Bu maddeye göre veri sahibi, kişisel verilerini işlenip işlenmediği onayına ve kişisel verilerinin kopyasına ek olarak, aşağıdaki verilere de erişebilir:

- İşleme amaçları,
- İlgili kişisel veri kategorileri,
- Üçüncü ülkeler veya uluslararası kuruluşlardaki alıcılar başta olmak üzere, kişisel verilerin açıklandığı veya açıklanacağı alıcılar veya alıcı kategorileri,
- Mümkün olması halinde, kişisel verilerin saklanması açısından öngörülen süre veya, bunun mümkün olmaması halinde, bu sürenin belirlenmesi amacı ile kullanılan kriterler,
- Kontrolörden veri sahibine ilişkin kişisel verilerin düzeltilmesi veya silinmesini veya söz konusu verilerin işlenmesinin kısıtlanmasını talep etme veya söz konusu işleme faaliyetine itiraz etme hakkının varlığı,
- Bir denetim makamına şikayette bulunma hakkı,
- Kişisel verilerin veri sahibinden elde edilmemesi halinde, bu verilerin kaynaklarına ilişkin mevcut bilgiler,

- Profil çıkarma da dahil olmak üzere 22(1) ve (4) maddelerinde atıfta bulunulan otomatik karar vermenin varlığı ve, en azından bu hallerde, yürütülen mantığa ilişkin anlamlı bilgilerin yanı sıra söz konusu işleme faaliyetinin veri sahibi açısından önemi ve öngörülen sonuçları,
- Kişisel verilerin üçüncü bir ülke ya da uluslararası bir kuruluşa aktarılması söz konusu ise, aktarımla ilgili olarak 46. Madde uyarınca alınan uygun güvenceler.

Kontrolörün zaten GDPR'nin 30. Maddesi ile düzenlenen işleme faaliyetlerinin kayıtlarının tutulması yükümlülüğü bulunmaktadır. Bu sebeple veri sahibinin erişim hakkını kullanması halinde sağlanacak verilerin hemen hemen hepsi zaten saklanmaktadır. Ancak, istisnai durumlar da olsa (özel kategorideki veya adli sicile ilişkin kişisel bilgileri işlemeyen ve 250'den az sayıda çalışanı olan organizasyonların durumunda olduğu gibi) Kontrolörün veri sahibinin erişim hakkını kullanarak talep ettiği bilgileri saklama zorunluluğu bulunmayabilir. Bu nedenle kural olanın bu bilgileri saklanması olduğu, istisnaların ise ancak somut olaya göre değerlendirilebileceği kabul edilmektedir.[165]

Erişim hakkının Kontrolör tarafından GDPR'ye aykırı olarak kısıtlanabileceği bir diğer durum ise erişim hakkını kullanan veri sahibine kendisi ile ilgili kişisel verilerin işleme tabii tutulmadığı yönünde bilgi verilmesi olacaktır. Bu halde, GDPR tarafından koruma altında olan hakları zarar gören veri sahibi, denetleyici otoriteye başvurmak veya hukuki işlem yapmak suretiyle haklarını arayabilecektir.[166]

(3) Düzeltme Hakkı

Veri sahibi, kendisi hakkındaki kişisel verilerin gecikme olmaksızın düzeltilmesini Kontrolörden talep edebilir. GDPR'nin 16. Maddesi ile düzenlenen bu hakka Düzeltme hakkı adı verilmektedir. Veri sahibi aynı zamanda, toplanan kişisel verilerinin veri işleme faaliyetlerinin amacı itibariyle eksik veya yetersiz kalması hallerinde 16. Maddeye dayanarak bu verilerin tamamlanmasını da talep edebilir. Bu sebeple bazı kaynaklarda 16. madde ile veri sahibine tanınan hakka düzeltme hakkı yerine Düzeltme ve Tamamlama Hakkı olarak da atıfta bulunulmaktadır.[167]

GDPR'nin 19. Maddesi düzelme hakkı kapsamında Kontrolöre bir görev daha yüklemektedir. Kontrolör, imkansız olmaması veya ölçüsüz bir çabayı gerektirmemesi halinde

[165] Bârsan, 2018: 131.
[166] Bârsan, 2018: 132.
[167] Wolters, P.T.J., "The Control by and Rights of the Data Subject Under the GDPR", Journal of Internet Law, Cilt 22, Sayı 1, 2018, s. 8.

veri düzeltme ve tamamlama işlemleri ile ilgili alıcıları bilgilendirmek zorundadır. Aynı zamanda veri sahibinin alıcılar ile ilgili bilgi alarak alıcıların da doğru ve tam verileri kullanmasını sağlayabilir.[168]

(4) Unutulma (Silme) Hakkı

Özellikle sosyal medya kullanımının giderek arttığı ve toplumun büyük çoğunluğunun genç yaşlardan itibaren bu platformları kullanmaya başladığı düşünüldüğünde, "internete yüklenen verilerin sonsuza dek internette kaldığı"[169] düşüncesi gittikçe korkutucu bir hal almaktadır. İşte tam olarak bu yüzden GDPR; veri sahibine Direktif ile sağlanmamış olan yeni bir hak tanımlamıştır.[170] GDPR ile veri sahibine tanınan unutulma (silme) hakkı hayati öneme sahiptir. GDPR, unutulma hakkının kapsamını 17. Madde ile belirlemiştir. Buna göre veri sahibinin kendisi ile ilgili kişisel verilerin silinmesini talep etmesi halinde veya;

- Kişisel verilerin toplanma veya işlenme amaçlarıyla ilişkili olarak artık gerekli olmaması,
- Veri sahibinin işleme faaliyetinin dayandığı rızasını geri çekmesi ve işleme faaliyetiyle ilgili başka bir yasal gerekçe bulunmaması,
- Veri sahibinin GDPR'nin 21. Maddesine göre itirazda bulunması ve işleme faaliyetine yönelik ağır basan meşru bir gerekçe bulunmaması,
- Kişisel verilerin yasa dışı biçimde işlenmiş olması,
- Kontrolörün tabi olduğu birlik veya üye devlet hukukundaki bir yasal yükümlülüğe uygunluk sağlanması amacı ile kişisel verilerin silinmesinin zorunlu olması,
- Kişisel verilerin GDPR'nin 8. Maddesinde atıfta bulunulan bilgi toplumu hizmetlerinin sağlanması ile ilgili toplanmış olması

hallerinden birinin oluşması durumunda Kontrolör herhangi bir gecikmeye mahal vermeksizin kişisel verileri silme yükümlülüğü altındadır. Buna ek olarak düzeltme hakkında olduğu gibi unutulma hakkında da Kontrolör, GDPR'nin 19. Maddesi'ne göre imkansız olmaması veya ölçüsüz çabayı gerektirmemesi halinde silme işleminden tüm alıcıları haberdar etmelidir.[171]

Unutulma hakkını özel kılan diğer bir neden, veri sahibi tarafından hakkın kullanılmasının Kontrolörün veya üçüncü kişilerin ifade özgürlüğünü zedeleyici yahut bilgi

[168] Wolters, 2018: 8.
[169] "What goes online, stays online": İnternette paylaşılan verilerin asla yok olmadığını ifade eden yaygın bir söyleyiş
[170] Voss, 2016: 225.
[171] Wolters, 2018: 8.

edinme hakkını kısıtlayıcı sonuçlara sebebiyet verebilecek olmasıdır. Bunun doğal bir sonucu olarak unutulma hakkı mutlak bir hak olarak tanımlanmamış, Kontrolörün verileri silme zorunluluğu bulunmayan bazı istisnalar da GDPR ile belirlenmiştir;

- İfade ve bilgi edinme hakkının kullanılması için,
- Kontrolörün tabi olduğu birlik veya üye devlet hukuku çerçevesinde işleme faaliyeti gerektiren bir yasal yükümlülüğe uygunluk açısından veya kamu yararına gerçekleştirilen bir görevin yerine getirilmesi veya kontrolöre verilen resmi bir yetkinin uygulanması açısından,
- Halk sağlığı alanındaki kamu yararı sebeplerinden dolayı,
- Hakkın kullanımının 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
- Yasal iddiaların dayandırılması, bu iddiaların uygulanması veya savunulması açısından

Verilerin gerekli olduğu ölçüde Kontrolörün verileri silme yükümlülüğü yoktur.

Unutulma hakkı da bilgilendirilme hakkı gibi GDPR'den önce Direktif ile korunan bir hak olduğundan, ABAD'ın Direktif'in uygulanmasına yönelik verdiği kararlar GDPR'ye göre bu hakkın kullanılması ve sınırları bakımından bize yol gösterecektir.

Bu bağlamda öne çıkan kararlardan ilki, veri sahibinin unutulma hakkı ile üçüncü kişilerin bilgi edinme hakkının çeliştiği bir dava hakkında verilmiştir. İspanya'da yaşayan ve İspanya vatandaşı olan veri sahibi; arama motoruna adını yazdığında, kendisinin borçları sebebi ile satışa çıkan bir taşınmazı hakkında çıkan haberlerin silinmesi/kaldırılması talebi ile haberi yayınlayan La Vanguardia gazetesi, Google Spain ve Google hakkında İspanyol Veri Koruma Otoritesine başvurmuştur. İspanyol Veri Koruma Otoritesi; şikayete konu yayının, Çalışma ve Sosyal Politikalar Bakanlığının açık artırma usulü yapılacak satış işleminin görünürlüğünün maksimize edilmesi yönündeki talimatı sebebi ile hukuka uygun olduğundan bahisle La Vanguardia hakkındaki şikayeti reddetmiştir. [172] Ancak Google Spain ve Google hakkındaki şikayetin veri koruma otoritesi tarafından kabul edilmesine karşı; Google ve Google Spain şu gerekçelerle uyuşmazlığı İspanyol Ulusal Mahkemesine taşımışlardır:

- Google; veri işleme faaliyetlerinden münhasıran sorumludur ve Merkezi California'da yer aldığından Direktif'in bölgesel kapsamının dışındadır, Google Spain arama motoru faaliyetlerinden sorumlu değildir,
- Arama işlevinde herhangi bir kişisel veri işleme faaliyeti yoktur,
- İşleme faaliyeti olsa bile Google da Google Spain de kontrolör değildir,

[172] Kranenborg, Herke, "Google and the Right to Be Forgotten (Case C-131/12, Google Spain)", European Data Protection Law Review, Cilt 1, Sayı 1, 2015, s. 70.

- Her halde şikayetçinin hukuka uygun biçimde yayınlanmış materyalin silinmesini talep etme hakkı yoktur.

Mahkeme, ön karar almak üzere dosyayı ABAD'a göndermiştir.[173]

ABAD kararında; arama motorunun işlevinin kişisel verilerin işlenmesi niteliğinde olduğunu, bu nedenle arama motorunun işletenin Kontrolör sıfatına haiz olacağını ve veri işleme faaliyetlerinin Google Spain'in bir üye devlet sınırları içerisinde yürüttüğü "faaliyetlerin bağlamında" gerçekleştiğini belirterek şikayetçinin unutulma hakkının gerek arama motoru işletenin ekonomik menfaatinden gerekse kamunun şikayetçinin adını aramak yoluyla bahse konu sayfaya ulaşmak suretiyle bilgiye erişme hakkını kullanmasından daha üstün olduğuna karar vermiştir.[174]

Unutulma hakkının kapsamı ile ilgili ABAD tarafından verilen bir diğer önemli karar, hakkın bölgesel kapsamına ilişkindir. Google unutulma hakkını; Avrupa Birliği bölgesinde bazı bağlantıların arama sonuçlarından gizlenmesi yoluyla kişisel verilere koruma sağlayan, ancak birliğin dışında kalan bölgelerde ise herhangi bir koruma sağlamayan bir kalkan olduğu kanaatindedir.[175] Bu konuda Google ve Fransız Veri Koruma Otoritesi arasındaki uyuşmazlıkta ABAD, Google'a hak vermiş ve arama motoru işleticisinin sonuçları gizleme veya kaldırma işlemini motorun tüm versiyonlarında değil yalnızca üye devletlerde kullanılmakta olan versiyonlarında gerçekleştirmesinin unutulma hakkının kullanılması bakımından yeterli olduğuna hükmetmiştir.[176]

(5) İşleme Faaliyetini Kısıtlama Hakkı

GDPR 18. Maddesi ile veri sahibine, kendisine ait kişisel verileri işleme faaliyetlerini kısıtlama hakkı tanımaktadır. Bu maddeye göre;

- Kişisel verilerin doğruluğuna veri sahibi tarafından itiraz edilmesi halinde, kontrolör kişisel verilerin doğruluğunu teyit edinceye dek geçici bir süreliğine,
- İşleme faaliyetinin yasa dışı olması ve veri sahibinin kişisel verilerin silinmesini herhangi bir sebeple istememesi ve bunun yerine verilerin kullanımının kısıtlanmasını talep etmesi halinde,
- Kontrolörün işleme amaçlarına yönelik olarak artık kişisel verilere ihtiyaç duymaması, ancak veri sahibinin yasal iddialarda bulunulması, bu iddiaların

[173] Torre, Lydia F de la, "Google Spain & the Right to be Forgotten", (Erişim) https://medium.com/golden-data/google-v-spain-the-right-to-be-forgotten-aaee50dae43c, 3 Şubat 2020.
[174] Avrupa Birliği Adalet Divanı 13.05.2014 tarih ve C-131/12 kararı, 2014.
[175] Bârsan, 2018: 133.
[176] Avrupa Birliği Adalet Divanı 24.09.2019 tarih ve C-507/17 kararı, 2019.

uygulanması veya savunulması amacıyla söz konusu verilere ihtiyaç duyması halinde veya
- Kontrolörün meşru gerekçelerinin veri sahibinin meşru gerekçelerine ağır basıp basmadığı doğrulanana kadar, veri sahibinin GDPR'nin 21. Maddesinde düzenlenen işleme faaliyetine itiraz etmesi halinde

veri sahibi, işleme faaliyetlerinin kısıtlanmasını kontolörden talep edebilir. Kontrolör tarafından veri sahibinin kişisel verileri üzerinde depolamak dışında herhangi bir işleme faaliyetinde bulunulamaz.[177] Kontrolör bu kısıtlamayı kaldırmadan önce veri sahibine bildirmek zorundadır.

Veri sahibinin işleme faaliyetini kısıtlama hakkını kullanması durumunda;

- Veri sahibinden rıza alınmadıkça veya
- Yasal iddialarda bulunulması, bu iddiaların uygulanması ve savunulması gerekmedikçe veya
- Başka bir kişinin meşru haklarının gözetilmesi için gerekmedikçe veya
- Kamu yararı gerektirmedikçe

Düzeltme ve unutulma haklarına paralel olarak, işleme faaliyetinin kısıtlanması hakkının kullanıldığı durumlarda da kontrolör, imkansız olmaması ve ölçüsüz çabayı gerektirmemesi halinde tüm alıcıları faaliyetin kısıtlandığı konusunda bilgilendirmek zorundadır.[178]

(6) Veri Taşınabilirliği Hakkı

Veri taşınabilirliği hakkı, GDPR'nin 20. Maddesi ile düzenlemiştir ve veri sahibinin kişisel verilerini bir kontrolörden diğerine aktarmasını kolaylaştırmayı amaçlayan bir haktır. 20. Maddeye göre kontrolörün, veri taşınabilirliği hakkını kullanmak isteyen veri sahibinin kişisel verilerini "yapılandırılmış, yaygın olarak kullanılan ve makine tarafından okunabilecek bir formatta" kendisine sağlaması gerekmektedir. Üstelik, teknik olarak mümkün olan durumlarda veri sahibi kişisel verilerinin doğrudan bir kontrolörden diğerine aktarılmasını da talep edebilir. Örneğin aralarında iş birliği bulunan bankalardan birinden diğerine kişisel verilerini taşımak isteyen veri sahibi bu hakkını kullanabilir.[179]

Veri taşınabilirliği hakkı mutlak bir hak değildir. Bu hakkın kullanılabilmesi için; veri işleme faaliyetlerinin, veri sahibinin rızasına dayanması yahut veri sahibinin taraf olduğu bir

[177] Torre, The right to restrict processing under EU data protection law, 2019.
[178] Wolters, 2018: 10.
[179] Calder, 2016: 42.

sözleşmenin uygulanması veya bir sözleşme yapılmadan önce veri sahibinin talebiyle adımlar atılması için yapılması gerekmektedir. Kamu yararına gerçekleştirilen bir görevin yerine getirilmesi veya kontrolöre verilen resmi bir yetkinin uygulanması için gereken işleme faaliyetlerine ilişkin olarak veri taşınabilirliği hakkı kullanılamaz. Benzer şekilde bu hak, başkalarının hak ve özgürlüklerini kısıtlamak için kullanılamaz.

Veri taşınabilirliği hakkının kapsamı, özellikle kontrolörün sorumluluğunun belirlenmesi bakımından önemlidir. Öncelikle belirtmek gerekir ki bu hak, veri sahibi tarafından Kontrolöre sağlanan kişisel verileri kapsar. Diğer bir deyişle, veri sahibi hakkında Kontrolör tarafından oluşturulan verileri kapsamaz.[180] Benzer şekilde bu hak yalnızca "otomatik yollar" ile işlenen kişisel verilere ilişkin olarak kullanılabilir.[181]

Veri taşınabilirliği hakkı, Direktif'de olmayan yani GDPR tarafından yaratılan bir haktır. Ancak kimi kaynaklar bu hakkın, yukarıda incelenen erişim hakkının genişletilmiş hali olduğunu ifade etmektedir.[182] Aradaki en önemli fark, veri taşınabilirliği hakkının kullanılması neticesinde veri sahibine teslim edilen verilerin "yapılandırılmış, yaygın olarak kullanılan ve makine tarafından okunabilecek bir formatta" olması gerekliliğidir. Bahse konu format, GDPR tarafından açıkça belirlenmemiştir ancak yaygın kullanımları ve yapıları itibariyle JSON, XML veya CSV gibi formatların bu hakkın kullanımına uygun olduğu düşünülmektedir.[183]

(7) İtiraz Hakkı

GDPR'nin 21. Maddesine göre, veri sahibinin kişisel verilerinin işlenmesine itiraz etme hakkı bulunmaktadır. İtiraz hakkının kullanılabileceği üç temel durum vardır. Bunlardan ilki, veri sahibinin kişisel verilerinin doğrudan pazarlama amaçları için kullanılması durumudur. Veri sahibinin bu duruma itiraz etmesi halinde, kendisine ait kişisel veriler doğrudan pazarlama amaçlarına yönelik olarak kullanılamaz hale gelirler.

İtiraz hakkının kullanımına konu olabilecek diğer bir durum; işleme faaliyetlerinin kamu yararına gerçekleştirilen bir görevin yerine getirilmesi veya kontrolöre verilen resmi bir yetkinin uygulanması hususunda gerekli olması durumudur. Ancak şayet kontrolör veri

[180] Wolters, 2018: 10.
[181] Wolters, 2018: 11.
[182] Wolters, 2018: 10,11.
[183] De Hert, Paul, Papakonstantinou, Vagelis, Malgieri, Gianclaudio, Beslay, Laurent, Sanchez, Ignacio, "The right to data portability in the GDPR: Towards user-centric interoperability of digital services", Computer Law & Security Review, Cilt 34, Sayı 2, 2018, s. 197.

sahibinin menfaatleri, hakları ve özgürlüklerinden ağır basan işleme faaliyetlerine yönelik olarak veya yasal iddialarda bulunulması, bu iddiaların uygulanması veya savunulması açısından zorlayıcı meşru gerekçeler gösterilmesi halinde itiraz eden veri sahibinin kişisel verilerini işlemeye devam edebilir.

Son olarak kişisel verilerin bilimsel veya tarihi araştırma amaçları ya da istatistiki amaçlar doğrultusunda işlendiği hallerde, eğer veri sahibi kendi özel durumu ile ilgili gerekçeler gösterebilirse ve işleme faaliyeti kamu yararı sebeplerinden dolayı gerçekleştirilen bir görevin yürütülmesi için gerekli değilse itiraz hakkını kullanabilir.

Görüldüğü üzere, doğrudan pazarlama amacı güden işleme faaliyetleri haricindeki hallerde itiraz hakkının kullanılıp kullanılamayacağı, yarışan menfaatlerden hangisinin ağır basacağına göre belirlenmektedir.[184]

(8) Profil Oluşturma Dahil Olmak Üzere Otomatik Karar Vermeyle İlgili Haklar

Profil çıkarma işlemleri de dahil olmak üzere, şayet herhangi bir otomatik veri işleme faaliyetine dayalı bir karar veri sahibi ile ilgili hukuki sonuçlar doğuruyor veya benzer biçimde veri sahibini kayda değer şekilde etkiliyorsa; veri sahibinin bu karara tabi olmama hakkı vardır. GDPR'nin 22. Maddesine göre veri sahibinin bu tip bir karar tabi olabilmesi açık rıza vermesi, veri sahibi ile kontrolör arasında bunu gerektirecek bir sözleşmenin bulunması veya kontrolöre, veri sahibinin hakları ile özgürlükleri ve meşru menfaatlerinin güvence altına alınması şartıyla, Birlik veya üye devlet hukukun çerçevesinde izin verilmesi gereklidir.

Madde lafzından da anlaşılacağı üzere, sayılan üç istisnai durumdan herhangi birinin oluşmaması durumunda veri sahibi maddede tanımlanan şekildeki bir karara tabi olamayacağından veri sahibine tanınan bu hak aynı zamanda kontrolöre getirilmiş bir yasaktır.[185]

[184] Wolters, 2018: 11.
[185] Wolters, 2018: 12.

b. Kontrolörün ve İşleyicinin Yükümlülükleri

(1) Kontrolörün Yükümlülükleri

Kontrolörler, işleme faaliyetlerinin GDPR ile uyumlu olarak gerçekleştirilmesi için gerekli idari ve teknik önlemleri almakla mükelleftirler. GDPR'nin 25. Maddesi bu önlemlere örnek olarak veri koruma politikalarının hazırlanmasını, GDPR'de belirlenen davranış kurallarına uyulmasını ve GDPR ile belirlenmiş sertifikasyon süreçlerinden faydalanılmasını göstermiştir.[186]

Buna ek olarak kontrolörler, işleme faaliyetlerinin tasarımını yaparken GDPR'ye uyumluluğu ön plana almalılardır. Data Protection By Design adı verilen bu prensibe göre kontrolörler hem işleme faaliyetlerinin belirlendiği anda hem de işleme faaliyetleri esnasında takma isim kullanılması, verilerin şifrelenmesi, işleme sisteminin dayanıklılaştırılması gibi birtakım önlemleri almaktan sorumludurlar. Benzer şekilde GDPR'nin 25. Maddesinin devamında düzenlenen Data Protection by Default ilkesi gereği kontrolörler yalnıza belirli olan amaç için işleme faaliyetlerini yürütmeli ve verileri ancak gerekli süre boyunca saklamalıdırlar. Aynı zamanda kontrolör, yalnızca GDPR ile uyumlu olarak çalışan işleyicilerle çalışmalıdır.[187]

GDPR'nin 37. Maddesine göre, şayet;

- İşleme faaliyeti yargı faaliyetlerini icra eden mahkemeler dışında bir kamu kuruluşu tarafından yapılıyorsa,
- Kontrolörün ana işi, kapsamı ve amacı göz önünde bulundurulduğunda büyük çaplı ve düzenli denetim gerektiren veri işleme faaliyetleri içeriyorsa veya
- Kontrolörün ana işi büyük çapta özel kategorilerde yer alan veya mahkumiyet kararlarına ilişkin verilerin işlenmesi faaliyetini içeriyorsa

kontrolör bir veri koruma görevlisi atamak zorundadır. Ver koruma görevlisi; denetim makamı ile olan irtibatı sağlar, kişisel verilerin korunmasına ilişkin sorumlulukları değerlendirir ve kurum içi eğitimler de dahil olmak üzere işçilerin farkındalığını artırma çalışmaları yapar.

---

[186] Gunathunga, Sagara, "All you need to know about GDPR Controllers and Processors", (Erişim) https://medium.com/@sagarag/all-you-need-to-know-about-gdpr-controllers-and-processors-248200ef4126 19 Ocak 2020.

[187] Gunathunga, Sagara, "All you need to know about GDPR Controllers and Processors", (Erişim) https://medium.com/@sagarag/all-you-need-to-know-about-gdpr-controllers-and-processors-248200ef4126 19 Ocak 2020.

Kontrolör, bunlara ek olarak GDPR'nin 35. maddesine göre özellikle yeni bir işleme teknolojisinin kullanılması gibi doğası gereği işlemenin yüksek risk içerdiği durumlarda ortaya çıkabilecek sonuçların değerlendirilmesi yapmalıdır. Veri koruma görevlisi varsa bu değerlendirme konusunda tavsiyeler vermek yine veri koruma görevlisinin görevleri arasındadır.

Olası bir veri sızıntısı halinde kontrolör denetim makamına bu durumu 72 saat içerisinde bildirmek zorundadır. Aynı zamanda veri sahibine de derhal anlaşılır bir dil ile durum izah edilmelidir.

(2) İşleyicinin Yükümlülükleri

İşleyici, yukarıda tanımı yapılırken de ifade edildiği üzere, yalnızca kontrolör tarafından verilen talimatlara uygun olarak işleme faaliyeti gerçekleştirmelidir. İşleyici şayet bulunduğu üye ülke sebebi ile özel yükümlülükler altında ise bunları kontrolöre bildirmekten de sorumludur.[188] İşleyicinin sorumlulukları genelde kontrolörün GDPR ile uyumlu çalışmasını destekler niteliktedirler. Buna örnek olarak; veri sahibi tarafından kontrolöre yapılan başvuruların işleme alınmasında kontrolöre yardımcı olma ve kontrolörün talimatı olan durumlarda saklanan kişisel verileri silme sorumlulukları gösterilebilir.

Bir veri sızıntısı yaşanması halince işleyici derhal kontrolöre haber vermelidir.

B. UYUŞMAZLIKLARIN ÇÖZÜMÜ VE CEZALAR

1. KVKK'da Uyuşmazlıkların Çözümü ve Cezalar

a. Veri Sorumlusuna Başvuru

İlgili kişinin hakları kısmında değinildiği üzere, ilgili kişi öncelikle KVKK'nın uygulanmasından doğan taleplerini veri sorumlusuna iletir. Veri sorunlusuna başvuru adı verilen bu usule ilişkin detaylar 13. Madde ile düzenlenmiştir. Buna göre veri sorumlusu

[188] Gunathunga, Sagara, "All you need to know about GDPR Controllers and Processors", (Erişim) https://medium.com/@sagarag/all-you-need-to-know-about-gdpr-controllers-and-processors-248200ef4126 19 Ocak 2020

başvuruda yer alan talepleri, talebin niteliğine göre en geç otuz gün içinde ücretsiz olarak sonuçlandırır. Veri sorumlusu talebi kabul edip gereklerini yerine getirebileceği gibi, talebi gerekçesini açıklamak suretiyle reddedebilir.

Her ne kadar başvuru hakkının kullanılmasının ücretsiz olacağı düzenlenmişse de, ilgili kişinin başvurusuna yazılı olarak cevap verilen haller için bir istisna getirilmiştir. Buna göre yazılı cevaplar için on sayfaya kadar başvuru ücreti alınmazken, on sayfanın üzerindeki her sayfa için 1 TL başvuru ücreti alınabilir.[189] Başvurunun veri sorumlusunun hatasından kaynaklandığı hallerde ise ücret iade edilir.

İlgili kişinin haklarının kullanımı için veri sorumlusuna başvuru şartı bulunmaktadır. Diğer bir ifade ile ilgili kişinin haklarının kullanımı kademelendirilmiştir. Başvuru yoluna gidilmeden Kurula şikâyette bulunulamaz.

b. Kurula Şikayet

Yukarıda açıklandığı üzere 11. Maddede düzenlenen hakların ilgili kişi tarafından kullanılması bakımından kademeli bir başvuru yolu öngörülmüştür. Şayet veri sorumlusuna yapılan başvuru reddedilirse, ilgili kişi tarafından Kurul'a başvuru yapılabilir. Kurul'a yapılacak başvurunun usulü KVKK'nın 14. Maddesi ile düzenlenmiştir. Buna göre; ilgili kişi, veri sorumlusunun cevabını öğrendiği tarihten itibaren otuz ve her hâlde başvuru tarihinden itibaren altmış gün içinde Kurula şikâyette bulunmalıdır.

Kurul, 5. Maddede düzenlenen usule göre şikayet tarihinden itibaren altmış gün içerisinde talebi inceleyerek ilgililere bir cevap vermek zorundadır. Şayet Kurul, bir ihlal olduğuna kanaat getirirse ihlalin veri sorumlusu tarafından giderilmesine karar verir. Veri sorumlusu bu kararı tebliğinden itibaren 30 gün içerisinde yerine getirmek zorundadır. Kurul, yaygın ihlallere karşı ilke karar alarak bunu yayımlayabilir. Benzer şekilde telafisi güç veya imkânsız zararların doğması ve açıkça hukuka aykırılık olması hâlinde, veri işlenmesinin veya verilerin yurt dışına aktarılmasının durdurulmasına da karar verebilir.

[189] Kişisel Verileri Koruma Kurumu, 2018: 58.

c. Yaptırımlar

(1) Genel Hükümler Kapsamında Hukuki Sorumluluk

Mevzuatımızda kişisel verilerin korunmasına yönelik olarak KVKK'dan önce de var olan genel hükümleri incelerken değindiğimiz üzere, kişisel verilerin hukuka aykırı olarak işlenmesi aslen kişilik hakkının ihlal edilmesi niteliğindedir. Bunun doğal bir sonucu olarak, kişisel verileri hukuka aykırı olarak işlenen ilgili kişi, genel hükümlere göre adli yargıda tazminat talep etme hakkına sahiptir.

Nitekim KVKK 14. Maddesi ile bu durumu açıkça düzenlemiş ve kurula şikayet halinde dahi kişilik hakları ihlal edilenlerin tazminat isteme hakkının saklı olduğunu ifade etmiştir. KVKK'nın uygulanması ile beraber kişisel veriler noktasında toplum bilincinin artması ile, aslen KVKK'dan eski olan bu kuruma olan başvuruların da artacağı öngörülmektedir.[190]

(2) Genel Hükümler Kapsamında Cezai Sorumluluk

Genel hükümler kapsamında tazminat talep etme usulüne benzer şekilde, şayet kişisel verilerin hukuka aykırı olarak işlenmiş olması aynı zamanda bir suç oluşturmuş ise TCK'nın 135 ila 140. Maddeleri uygulanacaktır.

Cezai sorumluluk bakımından KVKK, TCK'daki kişisel verilerin işlenmesine yönelik suçların içeriğini belirlemek konusunda kanun uygulayıcılara yol gösterici olmuştur. Örneğin TCK'daki "kişisel verilerin kaydedilmesi" suçu düzenlenmiş ancak "kişisel veri"nin tanımı yapılmamışken, KVKK ile bu gibi sorunlar çözülmüştür.[191] Bunun bir sonucu olarak kişisel verilerin korunması alanındaki TCK hükümlerine getirilen, belirsizlikler sebebi ile kanunilik ilkesine aykırı oldukları eleştirisi de cevaplanmıştır.[192]

[190] Küzeci, 2019: 373.
[191] Korkmaz, 2016: 141.
[192] Çokmutlu, 2014: 174., Korkmaz, 2016: 141.

(3) Kabahatler

Son olarak KVKK bünyesinde, veri sorumlusu tarafından yükümlülüklere aykırı davranılması halinde Kurul tarafından uygulanacak idari para cezaları belirlenmiştir. Buna göre veri sorumlusunun;

- Aydınlatma yükümlülüğünü yerine getirmemesi halinde 5.000TL'den 10.000TL'ye kadar,
- Veri güvenliğine ilişkin yükümlülüklerini yerine getirmemesi halinde 15.000TL'de 1.000.000TL'ye kadar,
- Kurul tarafından verilen kararları süresinde yerine getirmeyenler hakkında 25.000TL'den 1.000.000TL'ye,
- Veri Sorumluları Siciline kayıt ve bildirim yükümlülüğüne aykırı hareket edenler hakkında ise 20.000TL'den 1.000.000TL'ye kadar

İdari para cezası kesilir.

İdari para cezalarının uygulanması bakımından gerçek kişi tüzel kişi ayırımı olmadığı gibi, özel veya kamu tüzel kişileri arasında da fark yoktur. İhlalin kamu kurum ve kuruluşları ile kamu kurumu niteliğindeki meslek kuruluşları bünyesinde işlenmesi hâlinde, ilgili kamu kurum ve kuruluşunda görev yapan memurlar ve diğer kamu görevlileri ile kamu kurumu niteliğindeki meslek kuruluşlarında görev yapanlar hakkında disiplin hükümlerine göre işlem yapılır ve sonucu Kurula bildirilir.

2. GDPR'de Uyuşmazlıkların Çözümü ve Cezalar

a. Bir Denetim Makamına Şikayette Bulunma

Veri sahibi, şayet kişisel verilerinin işlenmesi faaliyetlerinin GDPR'ye uygun olmayan şekilde gerçekleştirildiğini düşünüyorsa yetkin denetim makamına başvurmak suretiyle şikayette bulunabilir. GDPR'nin 77. Maddesi ile veri sahibine tanınan bu hakka göre; yetkin denetim makamı, veri sahibinin yaşadığı veya çalıştığı yerdeki denetim makamı olabileceği gibi iddiaya konu ihlalin gerçekleştiği yerdeki denetim makamı da olabilir.

GDPR'nin 57. Maddesi, her denetim makamının veri sahiplerinin şikayetlerini toplaması ve kayıt altına alması için elektronik şikayet formu gibi bir takım araçların sağlanmasını zorunlu kılmıştır.

b. Etkili Bir Kanun Yoluna Başvurma

GDPR'de kanun yoluna başvurma hakkı iki farklı şekilde karşımıza çıkmaktadır. Bunlardan ilki 78. Madde ile düzenlenen denetim makamının bağlayıcı nitelikteki kararlarına karşı kanun yoluna başvurulması durumudur. Bu bağlamda "karar" kavramının geniş yorumlanması beklenmektedir. Zira denetim makamının yalnızca ceza kesilmesine yönelik kararları değil, şikayeti reddetme gibi kararlarına karşı da kanun yoluna başvurulabilir. Ancak 78. Madde hukuken bağlayıcı nitelikteki kararları kapsadığından, denetim makamının görüş veya tavsiyeleri gibi bağlayıcı nitelikte olmayan kararlarına karşı kanun yoluna gidilemez.[193]

Kanun yoluna başvurma hakkının GDPR'deki bir diğer yansıması, kişisel verilerinin GDPR'ye aykırı biçimde işlendiğini düşünen veri sahibinin kontrolör ve işleyiciye karşı kanun yoluna başvurmasını düzenleyen 79. Maddesidir. Bu maddeye göre veri sahibi dilerse şikayet ettiği kuruluşun bağlı bulunduğu üye devlet mahkemelerinde dilerse de kendi yerleşim yerinin bulunduğu üye devlet mahkemelerinde hakkını arayabilir. Ancak ihlali gerçekleştiren kontrolör veya işleyicinin kamu otoritesi olması ve ihlalin orantısız güç kullanımı neticesinde ortaya çıkması durumunda, bu kamu kuruluşunun bağlı bulunduğu üye devlet denetim makamı yetkilidir.

Bu konuda seçim hakkının veri sahibine verilmesinin ve özellikle kendi yerleşim yerinde dava açmasına veri sahibinin haklarını kullanmasını oldukça kolaylaştırdığı söylenebilir.[194]

c. Tazminat Talebi

Şüphesiz GDPR'nin etkili bir hukuki düzenleme olabilmesi için GDPR'ye aykırı davranan tarafların bu aykırılık neticesinde yol açtıkları zararı gidermesi, diğer bir deyişle sorumluluk ve tazminat kurumlarının yerleşmesi gerekmektedir. GDPR bu bağlamda hem kontrolörü hem de işleyiciyi oluşacak zararların giderilmesinden sorumlu tutmuştur.

GDPR'nin 82. Maddesine göre kişisel verilerin işlenmesi faaliyetlerinde yer alan tüm kontrolörler, GDPR'ye aykırılıklardan dolayı oluşacak zararın giderilmesinden sorumludurlar. İşleyiciler ise, GDPR'nin işleyiciler için getirdiği düzenlemelere aykırı olan işlemleri

[193] European Union Agency for Fundamental Rights and Council of Europe, 2018: 239.
[194] European Union Agency for Fundamental Rights and Council of Europe, 2018: 240.

neticesinde veya kontrolörün talimatı dışında hareket etmesi sonucunda doğan zararların giderilmesinden sorumludurlar. Hem kontrolörler hem de işleyiciler zararın oluşmasından sorumlu olmadıklarını ispatladıkları takdirde sorumluluktan kurutulurlar.

Zarara birden fazla tarafın birlikte yol açtığı hallerde veri sahibi tüm sorumlu taraflara husumet yöneltmek zorunda değildir. Husumeti taraflardan yalnızca birine yönelterek zararın tamamını talep edebilir. Diğer bir deyişle veri işleme faaliyetinde ortak olarak eden taraflar, ortaya çıkacak zararın giderilmesinden müteselsilen sorumludurlar. Husumet yöneltilen ve zararın tamamını karşılayan taraf, ödediği tazminatı zarara yol açtıkları orana göre diğer taraflara rücu edebilir.[195]

d. Yaptırımlar

GDPR'ye aykırılıklar sebebi ile oluşan zararın tazmininin yanı sıra, GDPR tarafından getirilen düzenlemelere uymayan taraflara düzeltici bazı tedbirler ve/veya idari para cezası da uygulanır.

(1) Denetim Makamının Düzeltici Yetkileri

Denetim makamı, GDPR'ye uyulmasını sağlamak amacı ile bazı düzeltici yetkilerle donatılmıştır. GDPR'nin 58. Maddesi ile düzenlenen düzeltici yetkilere göre denetim makamı;

- Kontrolör ve işleyiciye ihtarda bulunabilir,
- Kontrolör ve işleyiciye kınama cezası verebilir,
- Veri sahibinin haklarını kullanmasına yönelik taleplerine uyulması konusunda kontrolör ve işleyiciye talimat verebilir,
- İşleme faaliyetlerinin, GDPR'nin hükümlerine uyumlu hale getirilmesi hususunda kontrolör veya işleyiciye talimat verebilir;
- İşleme faaliyetlerine geçici veya kalıcı sınırlamalar getirebilir,
- Kişisel veri ihlalinin veri sahibine aktarılması hususunda kontrolöre talimat verebilir,
- Belgelendirme (Sertifikasyon) söz konusu ise bunları iptal edebilir veya ilgili kuruma iptal etmesi yönünde talimatta bulunabilir,
- AEA dışına veri aktarımlarını duraklatabilir.

Bunlara ek olarak denetim makamı, gerekli gördüğü hallerde 83. Madde kapsamında idari para cezası da uygulayabilir.

[195] European Union Agency for Fundamental Rights and Council of Europe, 2018: 246.

(2) İdari Para Cezaları

GDPR'nin 83. Maddesine göre her denetim makamı, GDPR'ye aykırılıklara ilişkin idari para cezalarını uygulamakla yükümlüdür. GDPR, kesilecek para cezalarının miktarını ihlalin niteliğine göre kademeli olarak belirlemiştir. İki kademedeki cezaları kısa şekilde özetlemek gerekirse; kontrolörün veya işleyicinin yükümlülüklerine aykırı hareket etmelerinden kaynaklanan ihlaller birinci kademe olarak değerlendirilirken; veri sahibinin hak ve özgürlüklerine aykırılıklar, rızanın alınış biçimindeki aykırılıklar, veri aktarımı kurallarına uyulmaması gibi durumlar ikinci kademe olarak değerlendirilmektedir.[196]

Birinci kademede yer alan ihlaller sebebi ile **en fazla**;

- 10.000.000,00€ veya
- Taraflardan birinin işletme olması halinde; önceki mali yılın yıllık dünya çapındaki cirosunun %2'si 10.000.000,00€'dan fazla ise bu meblağ kadar

ceza kesilebilir.

İkinci kademede yer alan ihlaller sebebi ile ise **en fazla**;

- 20.000.000,00€ veya
- Taraflardan birinin işletme olması halinde; önceki mali yılın yıllık dünya çapındaki cirosunun %4'ü 20.000.000,00€'dan fazla ise bu meblağ kadar

ceza kesilebilir.

GDPR kapsamında para cezası kesileceği zaman;

- İhlalin mahiyeti, ciddiyeti ve süresinin yanı sıra etkilenen veri sahibi sayısı ve veri sahiplerinin yaşadığı zarar düzeyi,
- İhlalin kasten veya ihmalkarlık sonucu ortaya çıkması,
- Zararın azaltılması için alınan önlemler,
- Kontrol ve işleyicinin sorumluluk dereceleri,
- Denetim makamı ile iş birliği derecesi,
- İhlalden etkilenen kişisel verilerin niteliği,
- Denetim makamının ihlalden haberdar edilme şekli,
- İhlalden doğrudan veya dolaylı şekilde fayda sağlanıp sağlanmadığı

hususları dikkate alınır.

[196] The GDPR Group Ltd., "Understanding GDPR Fines", (Erişim) https://www.gdpr.associates/what-is-gdpr/understanding-gdpr-fines/, 17 Şubat 2020

C. DÜZENLEMELERİN ÖNGÖRDÜKLERİ HAKLAR, YÜKÜMLÜLÜKLER VE CEZALAR BAKIMINDAN FARKLARI

1. İlgili Kişinin Hakları Bakımından Farklılıklar

Çalışmanın başından bu yana vurgulandığı üzere kişisel verilerin korunması bağlamında yapılan yeni düzenlemelerin tamamının ortak noktası kişilerin, kişisel verileri üzerindeki hakimiyetini ve kontrollü arttırmaktır. Bu bağlamda veri sahibinin/ilgili kişinin sahip olduğu haklar hem kişisel verileri üzerindeki hakimiyetleri hem de veri sorumlusu/kontrolörler ile olan ilişkilerini düzenlemek bakımından önemli bir konumdadır. Hem GDPR hem de KVKK bu bağlamda ilgili kişinin haklarını düzenleyerek, kişileri veri sorumluları/kontrolörler karşısında güçlendirici bazı önlemlere yer vermişlerdir.

İlgili kişinin hakları KVKK'nın 11. maddesi ile düzenlenmiştir. Buna göre ilgili kişi; veri sorumlusuna başvuruda bulunmak yoluyla kişisel verilerinin işlenip işlenmediğini, işlenmişse işlenme amacını ve verilerinin amacına uygun kullanılıp kullanılmadığını, yurt içinde ve yurt dışında verilerinin aktarıldığı üçüncü kişileri öğrenme hakkına sahiptir. Kişisel verilerinin işlenmesi hakkında bilgi edinmeye yönelik haklarına ek olarak; gerektiğinde yine veri sorumlusuna başvurmak suretiyle eksik veya yanlış olan kişisel verilerinin düzeltilmesini isteme, işlenme sebebi ortadan kalkan kişisel verilerinin silinmesini veya yok edilmesini talep etme ile düzeltme ve silme gibi işlemlerden üçüncü kişilerin haberdar edilmesini talep etme hakkına da sahiptir. Aynı zamanda münhasıran otomatik işleme yapan sistemler aracılığı ile analiz yapılan durumlarda ilgili kişi, kendisi hakkında aleyhe bir sonuç çıkmasına itiraz edebilir.

İlgili kişi KVKK kapsamında kendisine tanınan hakları kullanmak üzere veri sorumlusuna başvuruda bulunması ancak başvurunun gereklerinin yerine getirilmemesi veya veri sorumlusunun yükümlülüklerini ihlal ettiğinin tespit edilmesi halinde ilgili kişi, Kurul'a şikayet ve genel hükümlere göre dava açmak yoluyla zararın giderilmesini isteme hakkına sahiptir.

GDPR'nin, kendisinden önce gelen Direktif'le ve KVKK ile kıyaslandığında, veri sahibine daha geniş haklar tanıdığı görülmektedir. Bu haklar; bilgilendirilme hakkı, erişim hakkı, düzeltme hakkı, unutulma hakkı, işleme faaliyetini kısıtlama hakkı, veri taşınabilirliği

hakkı, itiraz hakkı, otomatik karar vermeye ilişkin hakları olmak üzere GDPR'nin 13. ve devam maddeleri ile düzenlemişlerdir.

Tanınan Hak	**KVKK**	**GDPR**
Bilgilendirilme hakkı	✔	✔
Erişim hakkı	—	✔
Düzeltme hakkı	✔	✔
Unutulma hakkı	Silme Hakkı olarak düzenlemiş	✔
İşleme faaliyetlerini kısıtlama hakkı	—	✔
Veri taşınabilirliği hakkı	—	✔
İtiraz hakkı	✔	✔
Otomatik karar vermeye ilişkin haklar	✔	✔

Tablo 2: KVKK ve GDPR Kapsamında İlgili Kişiye Tanınan Hakların Karşılaştırılması

Tabloda dikkat çeken önemli farklılıklardan ilki, GDPR'nin bilgilendirilme hakkına ek olarak düzenlemiş olduğu erişim hakkıdır. Zira KVKK, ilgili kişiye işlenen kişisel verilerine erişim hakkını ayrıca tanımamıştır. Bilgilendirme hakkı, mutlak suretle önemli olmakla beraber ilgili kişini verilerinin hukuka aykırı olarak işlenip işlenmediğine dair daha net bilgi edinebilmesi adına erişim hakkının önemli olduğu kanaatindeyiz.

İki düzenleme arasında, GDPR tarafından düzenlenen ancak kanunda yer bulunmayan bir diğer hak işleme faaliyetinin kısıtlanması hakkıdır. Bu hak, GDPR'nin 18. maddesi ile düzenlenmiştir. Buna göre GDPR'de sayılan hallerden birinin gerçekleşmesi durumlarında veri sahibinin kontrolörden işleme faaliyetlerini kısıtlamasını talep edebilir. Bu talep üzerine kontrolör, veri sahibinin kişisel veriler, üzerinde depolama dışında herhangi bir işleme faaliyetinde bulunamaz. KVKK'da kişisel verilerinin silinmesini istemeyen ancak bu veriler üzerinde depolama dışında herhangi bir işleme faaliyetinde bulunulmasına dair rıza göstermeyen kullanıcılar için işleme faaliyetinin kısıtlanması hakkına paralel herhangi bir hak yer almamaktadır. Kişisel verilerin korunması düzenlemelerinin ortak amacı kontrolör ve ilgili kişi arasındaki güç dengesini oluşturmak ve ilgili kişiye kişisel verileri üzerinde daha fazla kontrol sağlamak ise bu anlamda ilgili kişinin kişisel verileri üzerinde uygulanacak işleme faaliyetleri bakımından da söz sahibi olması pek tabii düzenlemenin amacına daha uygun olacaktır.

İki düzenleme arasında veri sahibinin/ilgili kişinin hakları bakımından yer alan son farklılık GDPR'nin yine kendisinden önce gelen düzenlemelerden farklı olarak tanıdığı veri taşınabilirliği hakkıdır. Veri taşınabilirliği hakkı, GDPR'nin 20. maddesi ile düzenlenmiş olup veri sahibinin kişisel verilerini bir kontrolörden diğer bir kontrolöre taşınmasını kolaylaştırmayı hedefleyen bir haktır. Yukarıda detaylı biçimde açıklandığı üzere veri sahibinin 20. maddeye dayanarak veri taşınabilirliği hakkını kullanması durumlarında kontrolör, veri sahibine verilerini yaygın biçimde kullanılan bir formatta sağlamak durumundadır.

KVKK'da ilgili kişinin verilerini başka bir veri sorumlusuna teslim etmek üzere talep etmesini öngören ve veri sorumlusunun ilgili kişiye talep etmesi halinde verilerini anlaşılır ve yaygın bir formatta sağlamasını öngören herhangi bir hüküm yer almamaktadır. İlgili kişinin hakları bakımından diğer farklılıklarda da değinildiği üzere bu hakkın yokluğunun büyük bir hak kaybına sebebiyet vereceğini düşünmemekle beraber, bu nitelikte bir hak tanınmasının ilgili kişinin kişisel verileri üzerindeki hakimiyetini artıracağı ve özellikle veri sorumlusunu özgürce seçebilmesini ve kolayca değiştirebilmesini kolaylaştıracağı göz önünde bulundurulduğunda, yine taraflar arasındaki güç dengesinin sağlanması bakımından faydalı olacağı kanaatindeyiz.

2. Veri Sorumlusu/Kontrolör Ve İşleyen Arasındaki Sorumluluk Dengesi Bakımından Farklılıklar

Kişisel verileri işleme faaliyetlerinin önemli iki aktörü olan veri sorumlusu/kontroller ve işleyen arasındaki ilişkinin detayları ve bu aktörler ile veri sahibi/ilgili kişi arasındaki ilişkinin dengesinin ilgili kişinin kişisel verileri üzerindeki hakimiyetini arttırmak ve olası bir zarar halinde tazminatın kimden veya kimlerden talep edebileceğini belirlemek anlamında önemlidir.

Kontrolör/veri sorumlusu her iki düzenleme bakımından da ana sorumlu olarak addedilmiş olup düzenlemelere aykırılık halinde zararın tazminini yahut idari para cezasının ödenmesini üstlenecek taraflardandır.[197] Bu bakımdan iki düzenleme birbirine paraleldir.

[197] Memiş, 2017: 14., Information Comissioner's Office, "What responsibilities and liabilities do controllers have when using a processor?", (Erişim) https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/contracts-and-liabilities-between-controllers-and-processors-multi/responsibilities-and-liabilities-for-controllers-using-a-processor/, 15 Ocak 2020.

Düzenlemeler arasındaki farklılık kontrolör ve işleyenin aynı anda faaliyet gösterdiği bir durumda zararın ortaya çıkması halinde zararın giderilmesi bakımından sorumluluğun kime ait olacağı noktasındadır.

KVKK'nın 12. maddesinde veri sorumlusunun üçüncü kişilerle veri işleme faaliyetlerde bulunması halinde kanuna uyulmamasından müşterek sorumlu olacakları düzenlenmiştir.[198] GDPR, veri işleyen bakımından daha dengeli bir sorumluluk mekanizması öngörmüştür. Buna göre veri işleyen ancak kontrollerin talimatları dışarı çıkması veya ihlal veya aykırılıkların spesifik olarak veri işleyen tarafından yapılan faaliyetlerin neticesinde ortaya çıkması durumlarında veri işleyenin sorumluluğu doğacağını belirtmiştir.[199]

Veri işleyenin veri sorumlusunun/kontrolörün talimatları ile iş yaptığı göz önünde bulundurulduğunda talimatların dışına çıkmadığı müddetçe ortaya çıkacak tüm zarardan müteselsil sorumlu tutulmasının ölçüsüz olduğu kanısındayız. Nitekim doktrinde de veri sorumlusunun bir veri işleyen vasıtasıyla verileri işlemesinin temel sebebinin teknik bilgiye sahip olmayışı olduğu, bu yüzden KVKK'ya uygunluk bakımından şayet işleyiciyi seçerken özenli davrandıysa teknik kısımlarla ilgili ortaya çıkabilecek ihlallerden sorumlu olmaması gerektiği vurgulanmaktadır.[200] Bu sebeplerle GDPR'deki düzenlemenin hem veri işleyen bakımından hem de kontrolör bakımından daha adil olduğunu düşünüyoruz.

3. Cezalar Arasındaki Farklılıklar

Tabii ki her hukuki düzenlemenin, koruduğu değerler zarar gördüğünde mağdurun zararının tazmin edilmesi ve gerekli hallerde sorumlunun cezalandırılması için mekanizmaları olduğu gibi kişisel verilerin korunması alanındaki düzenlemelerin de uyuşmazlıkları çözüm yolları ve yükümlülüklerine aykırı hareket eden tarafı cezalandırmak için koyduğu bir takım mekanizmalar mevcuttur. Hem KVKK hem de GDPR veri sahibinin/ ilgili kişinin haklarını koruyabilmek için hukuki çözüm yolları ve cezalar öngörmüşlerdir.

---

[198] Memiş, 2017: 17.

[199] Information Commissioner's Office, " What responsibilities and liabilities do processors have in their own right?", (Erişim) https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/contracts-and-liabilities-between-controllers-and-processors-multi/responsibilities-and-liabilities-for-processors-in-their-own-right/, 16 Ocak 2020

[200] Memiş, 2017: 17.

Öncelikle belirtmek gerekir ki her iki düzenleme de veri sahibinin/ilgili kişinin veri sorumlusuna/kontrollere başvuru hakkını ve başvurudan sonuç alamaması halinde Kurul'a/denetim makamına şikayet hakkını ve şikayete ek olarak uğradıkları zararın tazmini için hukuk davası açmaları hakkını düzenlemişlerdir. Her iki düzenlemede öngörülen hukuki başvuru yolları benzer olmasına rağmen gerek cezaların miktarları gerekse denetim makamı tarafından verilen karara karşı itiraz hakkı bakımından bazı farklar mevcuttur. Bunlardan ilki ihlallerde uygulanacak cezaların miktarlarındadır.

KVKK, ihlal edilen kanun maddesi bakımından farklı alt ve üst sınırlar belirlemek suretiyle idari para cezası kesilmesini öngörmüşken, GDPR cezaların belirlenmesi bakımından ihlal edilen değere göre ikili bir ayrıma gitmiştir. Bu ikili ayrım neticesinde verilecek idari para cezasının üst limitini ise cezanın kesileceği tarafın bir teşebbüs olduğu hallerde ikili bir ayrıma bağlamıştır. Yukarıda detaylı olarak açıklandığı üzere cezanın kesileceği teşebbüsün yıllık cirosunun yüzde ikisinin GDPR maddesinin üst sınır olarak belirlediği miktardan daha fazla olması halinde yıllık cironun yüzde ikisi üst sınır olarak kabul edilerek cezai işlem uygulanır.

İhlal Edilen Madde	**Ceza Alt Sınırı**	**Ceza Üst Sınırı**
10. Madde	5.000TL	100.000TL
12. Madde	15.000TL	1.000.000TL
15. Madde	25.000TL	1.000.000TL
16. Madde	20.000TL	1.000.000TL

Tablo 3: KVKK'da Düzenlenen Para Cezalarının Alt ve Üst Sınırları

İhlal Edilen Madde	**Ceza Alt Sınırı**	**Ceza Üst Sınırı**
8., 11., 25., 39., 41/4, 42., 43. Maddeler	—	10.000.000 EUR veya (daha yüksek bir miktar ise) teşebbüsün yıllık cirosunun %2'si
5., 6., 7., 9., 12-22., 44-49, 58. Maddeler	—	20.000.000 EUR veya (daha yüksek bir miktar ise) teşebbüsün yıllık cirosunun %2'si

Tablo 4: GDPR'de Düzenlenen Para Cezalarının Alt ve Üst Sınırları

Her ne kadar her iki düzenleme de geniş aralıklar belirlemek suretiyle kanun uygulayıcıya bir serbesti alanı tanımışlar ise de GDPR tarafından benimsenen metodun daha caydırıcı olabileceği kanaatindeyiz. Zira ceza üst sınırı belirlenirken ihaleli gerçekleştiren sorumlu teşebbüsünün yıllık cirosunun hesaplamaya baz alınabilmesi, özellikle büyük şirketlerin cezayı göze alarak işleme faaliyetlerini kanuna aykırı olarak sürdürmelerinin önüne geçmek konusunda etkili bir mekanizma olacaktır.

SONUÇ

Teknolojinin hızlı bir şekilde gelişmesi ve özellikle son dönemde kullanıcıların da katkıda bulunarak etkileşime geçebildikleri platformların kârlı bir sektör olduğunun kabul görmesi sebebiyle, her geçen gün kişisel verilerin toplanması ve işlenmesi alanlarında yeni araçların ortaya çıktığını görüyoruz. Üstelik nesnelerin interneti adı verilen, günlük işlerimizi kolaylaştıran cihazların internet üzerinden kontrol edilmesini sağlayan çalışmalar ve kullanıcıların bilgisayarla etkileşimlerini kolaylaştırmak, bilgi erişimlerini hızlandırmak ve cihazlarını konuşarak kontrol etmelerini sağlamak için geliştirilen dijital asistanların ortaya çıkışı ile beraber veri toplama ve işleme faaliyetlerinin sadece bilgisayar üzerinde yaptığımız faaliyetlere ilişkin verileri değil günlük hayatımızın her anına ilişkin verileri elde etmesi mümkün hale geliyor.

Şaşırtıcı olan şey ise geliştirilmesi ve üretilmesi oldukça maliyeti olan bu teknolojilerin birçoğu kullanıcılara ücretsiz olarak sunuluyor. Zira birçok platform, daha iyi hale gelebilmek için kullanıcı verilerini işleyerek adeta "öğreniyor" veya kullanıcıların verilerini onları daha iyi tanımak için kullanıyor ve kullanıcılara ilgili oldukları ürünlerin reklamını yaparak gelir elde ediyorlar. Kullanıcılar ise düzenli bir abonelik bedeli veya yazılımlara ciddi lisans ücretleri ödemek yerine kişisel verilerinin teknoloji firmaları tarafından ürünleri daha iyi hale getirme ve pazarlama amaçları ile kullanılmalarına müsaade ediyorlar. Diğer bir deyişle kişisel veriler günümüz teknoloji dünyasının para birimi haline gelmiş vaziyetteler.[201]

Her ne kadar veri işleyenler ve kullanıcılar arasında rızai bir ilişki olsa da kişisel verilerin işlenmesi alanının hukuk düzeni tarafından düzenlenmesi kişileri kötü niyetli işleme faaliyetlerine karşı korumak için elzemdir. Bilindik bir metafor ile örneklemek gerekirse çekiç nasıl çivi çakmak icat edilmiş olduğu halde insan yaralamak için de kullanılabiliyor ise kişisel verilerin işlenmesine yönelik araçlar da teknolojinin gelişmesine ve kullanıcılara daha iyi hizmet verilmesine hizmet etmek için icat edilmiş olmasına karşın kötüye kullanımları neticesinde kişilere ciddi zararlar vermeleri mümkün olan araçlardır.

Bu bağlamda dünyadaki en etkili düzenlemelerden biri Avrupa Birliği'nin 2018'de uygulamaya koydu GDPR olup, ortaya çıkışı ile beraber internetin küresel yapısının da etkisi ile adeta kişisel verilerin korunması alanında bir standart belirleyici haline gelmiştir.[202]

---

[201] Article 29 Data Protection Working Party Opinion 3/2010 on the principle of accountability, s. 5.

[202] Albrecht, Jan Philipp, "How the GDPR Will Change the World", European Data Protection Law Review (EDPL), Cilt 2, Sayı 3, 2016, s. 287-289

Mevzuatımızda bu alana ilişkin yürürlükte olan Kişisel Verilerin Korunması Kanunu da vatandaşların hak ve özgürlüklerini kişisel verilerin kötü niyetli işleme faaliyetlerine karşı korunması vasıtasıyla kollamaktadır. Çalışmada irdelendiği şekilde GDPR ve KVKK genel itibariyle birbirlerine paralel düzenlemeler olup, düzenlemenin hazırlandığı dönemde içerisinde bulunulan günün şartları ve düzenlemenin uygulanacağı bölgenin sosyal ve kültürel ekosistemine bağlı olarak bazı farklılıklara sahiptirler.

GDPR ve KVKK arasındaki farklılıklar, düzenlemelerden birinin veya diğerinin münhasıran uygulanmasını gerektirmemekte diğer bir deyişle birbirleri ile doğrudan çelişen hususlar yaratmamaktadırlar. Bu nedenlerle Türkiye'de faaliyet göstermekte olup Avrupa Birliği üye ülkelerinden birinin vatandaşlarına hizmet vererek bu vatandaşların kişisel verilerin, işleme faaliyetine tabi tutan teşebbüslerin her iki düzenlemeye de uygun bir kişisel verilerin korunması politikası oluşturmaları faydalı olacaktır.

KAYNAKÇA

AEA Komitesi, “6 Temmuz 2018 tarih ve 154/2018 numaralı kararı”, (Erişim) https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX%3A22018D1022, 28 Aralık 2019

Albrecht, Jan Philipp, "How the GDPR Will Change the World", European Data Protection Law Review (EDPL), Cilt 2, Sayı 3, 2016, s. 287-289

Anı, Nevzat Ali, Kişisel Verilerin İşlenmesi ve Açık Rıza, Yayımlanmamış Yüksek Lisans Tezi, İstanbul Üniversitesi, Sosyal Bilimler Enstitüsü, İstanbul, 2018

Article 29 Data Protection Working Party Opinion 3/2010 on the principle of accountability

Avrupa Birliği Adalet Divanı, “1.10.2015 tarih ve C-201/14 sayılı kararı”, (Erişim) http://curia.europa.eu/juris/liste.jsf?num=C-201/14, 20 Aralık 2019

Avrupa Birliği Adalet Divanı, “13.05.2014 tarih ve C-131/12 kararı”, (Erişim) http://curia.europa.eu/juris/liste.jsf?num=C-131/12, 20 Aralık 2019

Avrupa Birliği Adalet Divanı, “24.09.2019 tarih ve C-507/17 kararı”, (Erişim) http://curia.europa.eu/juris/liste.jsf?num=C-507/17, 20 Aralık 2019

Avrupa Birliği Adalet Divanı, “6 Kasım 2003 tarih ve C-101/01 sayılı kararı”, (Erişim) http://curia.europa.eu/juris/liste.jsf?num=C-101/01, 20 Aralık 2019

Aysal, Necdet, "Tanzimat'tan Cumhuriyet'e Giyim ve Kuşamda Çağdaşlaşma Hareketleri", Çağdaş Türkiye Tarihi Araştırmaları Dergisi, Cilt 10, Sayı 22, 2011, s. 3-32

Bârsan, Maria-Magdalena, "A Partial Overview of the Data Subjects’ Control over Their Personal Data under the General Data Protection Regulation", Bulletin of the Transilvania University of Braşov Series VII: Social Sciences., Cilt 11, Sayı 2, 2018, s. 129-134

Bietti, Elettra, "Consent as a Free Pass: Platform Power and the Limits of the Informational Turn", Pace Law Review, Cilt 40, Sayı 1, 2020, s. 307-397

Blackmer, W. Scott, "Google Fined $57 Million under GDPR", (Erişim) https://www.infolawgroup.com/insights/2019/1/23/google-fined-57-million-under-gdpr, 21 Kasım 2019

Calder, Alan, EU GDPR A Pocket Guide, IT Governance Publishing, Cambridgeshire, 2016

Commission Nationale de l'Informatique et des Libertés, "The CNIL’s restricted committee imposes a financial penalty of 50 Million euros against GOOGLE LLC", (Erişim) https://www.cnil.fr/en/cnils-restricted-committee-imposes-financial-penalty-50-million-euros-against-google-llc, 21 Kasım 2019

Çekin, Mesut, "6698 Sayılı Kişisel Verilerin Korunması Hakkında Kanun'un Big Data (Büyük Veri) Ve İrade Serbestisi Açısından Değerlendirilmesi", İstanbul Ünversitesi Hukuk Fakültesi Mecmuası, Cilt 74, Sayı 2, 2016, s. 629-644

Çokmutlu, Metin, Türk Ceza Hukukunda Kişisel Verilerin Korunması, Yayımlanmamış Yüksek Lisans Tezi, Kocaeli Üniversitesi, Sosyal Biliimler Enstütüsü, Kocaeli, 2014

Data Protection Comission, "One Stop Shop (OSS)", (Erişim) https://www.dataprotection.ie/en/organisations/one-stop-shop-oss, 10 Eylül 2019

Datastreams, "Explicit vs. unambiguous consent: what’s the difference?", (Erişim) https://www.datastreams.io/explicit-vs-unambiguous-consent-whats-the-difference/, 2 Aralık 2019

De Hert, Paul, Papakonstantinou, Vagelis, Malgieri, Gianclaudio, Beslay, Laurent, Sanchez, Ignacio, "The right to data portability in the GDPR: Towards user-centric interoperability of digital services", Computer Law & Security Review, Cilt 34, Sayı 2, 2018, s. 193-203

De Terwangne, Cécile, "The work of revision of the Council of Europe Convention 108 for the protection of individuals as regards the automatic processing of personal data", International Review of Law, Computers & Technology, Cilt 28, Sayı 2, 2014, s. 118-130

Elgesem, Dag, "The structure of rights in Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and the free movement of such data", Ethics and Information Technology, 1999, s. 283-293

Erdoğan, Canan, "Çocukların Kişisel Verilerinin Korunması (Sosyal Medya Örneği Kapsamında)", DEÜ Hukuk Fakültesi Dergisi, Cilt 21, Sayı Özel, 2019, s. 2445-2467

European Comission, "Adequacy decisions", (Erişim) https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en, 20 Ocak 2020

European Union Agency for Fundamental Rights and Council of Europe, Handbook on European Data Protection Law, Imprimerie Centrale, Luxembourg, 2018

Gabel, Detlev, Hickman, Tim, "Chapter 8: Consent – Unlocking the EU General Data Protection Regulation", (Erişim) https://www.whitecase.com/publications/article/chapter-8-consent-unlocking-eu-general-data-protection-regulation?s=consent, 20 Mart 2020

Gözüküçük, Merve, Veri işleme Süreçlerinde Tartışmalı Bir Çözüm: Veri Anonimleştirilmesi, Yayımlanmamış Yüksek Lisans Tezi, İstanbul Bilgi Üniversitesi, Sosyal Bilimler Enstitüsü, İstanbul, 2014

Gunathunga, Sagara, "All you need to know about GDPR Controllers and Processors", (Erişim) https://medium.com/@sagarag/all-you-need-to-know-about-gdpr-controllers-and-processors-248200ef4126 19 Ocak 2020

Güner, Oğuz, Günar, Altuğ, "Protection of Personal Data in the European Union-turkey Relations: Effect of Visa Liberalisation Dialogue", Yönetim ve Ekonomi Araştırmaları Dergisi, Cilt 17, Sayı 4, 2019, s. 35-58

Gürsel, Esin, Düğmeci, Fatih, "Yapısal Anlamda Türkiye Kişisel Verileri Koruma Kurumu'na İlişkin Bir Değerlendirme", R&S - Research Studies Anatolia Journal, Cilt 1, Sayı 2, 2018, s. 318-329

Helvacı, İhsan, Kişisel Verilerin Korunması Kanunu Hakkında Hukuki Mütalaa, TBB, İstanbul, 2018

Henkoğlu, Türkay, "Kişisel Verileriniz Ne Kadar Güvende? Bilgi Güvenliği Kapsamında Bir Değerlendirme", Arşiv Dünyası Dergisi, Sayı 17-18, 2017, s. 46-56

Information Comissioner's Office, "Guide to the Privacy and Electronic Communications Regulations", (Erişim) https://ico.org.uk/media/for-organisations/guide-to-pecr-2-4.pdf, 24 Aralık 2019

Information Comissioner's Office, "What responsibilities and liabilities do controllers have when using a processor?", (Erişim) https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/contracts-and-liabilities-between-controllers-and-processors-multi/responsibilities-and-liabilities-for-controllers-using-a-processor/, 15 Ocak 2020

Information Commissioner's Office, " What responsibilities and liabilities do processors have in their own right?", (Erişim) https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/contracts-and-liabilities-

between-controllers-and-processors-multi/responsibilities-and-liabilities-for-processors-in-their-own-right/, 16 Ocak 2020

Information Commissioner's Office, "Accountability and Governance", (Erişim) https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/, 15 Ocak 2020

It Governance Privacy Team, EU General Data Protection Regulation (GDPR), third edition, IT Governance Publishing, Cambridgeshire, 2019

i-scoop, "Explicit consent and how to obtain it – new GDPR consent guidelines", (Erişim) https://www.i-scoop.eu/gdpr/explicit-consent/, 1 Ocak 2020

i-scoop, "Personal data breach notification and communication duties under the GDPR", (Erişim) https://www.i-scoop.eu/gdpr/personal-data-breach-notification/, 4 Ocak 2020

Kartal, Mustafa Tevfik, "Kişisel Verilerin Korunması: Türk Bankacılık Sektörü Üzerine Kavramsal Bir Değerlendirme", Uluslararası Ekonomi ve Yenilik Dergisi, Cilt 4, Sayı 1, 2018, s. 1-18

Kaya, Cemil, "Avrupa Birliği Veri Koruma Direktifi Ekseninde Hasas (Kişisel) Veriler ve İşlenmesi", İstanbul Üniversitesi Hukuk Fakültesi Mecmuası, Cilt 69, Sayı 1-2, 2011, s. 317-334

Kersten, Jenna, "What is GDPR Personal Data and Who is a GDPR Data Subject?", (Erişim) https://kirkpatrickprice.com/blog/what-is-gdpr-personal-data-and-who-is-a-gdpr-data-subject/, 20 Ocak 2020

Khitrov, Mikhail, "Talking passwords: voice biometrics for data access and security", Biometric Technology Today, Cilt 2013, Sayı 2, 2013, s. 9-11

Kılınç, Doğan, "Anayasal Bir Hak Olarak Kişisel Verilerin Korunması", Ankara Üniversitesi Hukuk Fakültesi Dergisi, Cilt 61, Sayı 3, 2012, s. 1089-1169

Kierkegaard, Sylvia, Waters, Nigel, Greenleaf, Graham, Bygrave, Lee A., Lloyd, Ian, Saxby, Steve, "30 years on – The review of the Council of Europe Data Protection Convention 108", Computer Law & Security Report, Cilt 27, Sayı 3, 2011, s. 223-231

Kişisel Verileri Koruma Kurumu, "Açık Rıza", (Erişim) https://www.kvkk.gov.tr/SharedFolderServer/CMSFiles/66b2e9c4-223a-4230-b745-568f096fd7de.pdf, 24 Ocak 2020

Kişisel Verileri Koruma Kurumu, "Anayasal Bir Hak Olarak Kişisel Verilerin Korunmasını İsteme Hakkı", (Erişim) https://www.kvkk.gov.tr/SharedFolderServer/CMSFiles/cf706768-36ab-472c-bbd6-cb0b773405da.pdf, 23 Ocak 2020

Kişisel Verileri Koruma Kurumu, "Kanun Kapsamında Hak Ve Yükümlülükler", (Erişim) https://www.kvkk.gov.tr/Icerik/4192/Kanun-Kapsamindaki-Hak-ve-Yukumlulukler, 20 Şubat 2020

Kişisel Verileri Koruma Kurumu, "Kurumsal e-posta hizmetinin, Google (Gmail) üzerinden yine aynı uzantıya sahip olarak kullanılıp kullanılamayacağına ilişkin Kişisel Verileri Koruma Kurulunun 31.05.2019 tarihli ve 2019/157 sayılı karar özeti", (Erişim) https://www.kvkk.gov.tr/Icerik/5493/2019-157, 18 Kasım 2019

Kişisel Verileri Koruma Kurumu, "Yurtdışına Veri Aktarımında Veri Sorumlularınca Hazırlanacak Taahhütnamede Yer Alacak Asgari Unsurlar", (Erişim) https://www.kvkk.gov.tr/Icerik/4236/Yurtdisina-Veri-Aktariminda-Veri-Sorumlularinca-Hazirlanacak-Taahhutnamede-Yer-Alacak-Asgari-Unsurlar, 20 Ocak 2020

Kişisel Verileri Koruma Kurumu, 100 Soruda Kişisel Verilerin Korunması Kanunu, KVKK Yayınları, Ankara, 2018

Kişisel Verilerin Korunması Kanunu Tasarısı (1/541) ve Adalet Komisyonu Raporu

Kişisel Verilerin Otomatik İşleme Tabi Tutulması Karşısında Bireylerin Korunması Sözleşmesi

Kişisel Verilerin Otomatik İşleme Tabi Tutulması Karşısında Bireylerin Korunması Sözleşmesine Ek Denetleyici Makamlar Ve Sınıraşan Veri Akışına İlişkin Protokol

Korkmaz, İbrahim, "Kişisel Verilerin Korunması Kanunu Hakkında Bir Değerlendirme", Türkiye Barolar Birliği Dergisi, Cilt 29, Sayı 124, 2016, s. 81-152

Kranenborg, Herke, "Google and the Right to Be Forgotten (Case C-131/12, Google Spain)", European Data Protection Law Review, Cilt 1, Sayı 1, 2015, s. 70-79

Kuner, Christopher, European data protection law: Corporate compliance and regulation, Oxford University Press, Oxford, 2007

Küzeci, Elife, Kişisel Verilerin Korunması, Turhan Kitapevi, Ankara, 2019

Lievens, Eva, Verdoodt, Valerie, "Looking for needles in a haystack: Key issues affecting children's rights in the General Data Protection Regulation", Computer Law & Security Review, Cilt 34, Sayı 2, 2018, s. 269-278

Memiş, Tekin, "Veri Sorumlusu ve Veri İşleyen Arasındaki İlişkiler ve Sorumluluk Düzeni", Beykent Üniversitesi Hukuk Fakültesi Dergisi, Cilt 3, Sayı 6, 2017, s. 9-23

Mourby, Miranda, Mackey, Elaine, Elliot, Mark, Gowans, Heather, Wallace, Susan, E. Bell, Jessica, Smith, Hannah, Aidinlis, Stergios, Kaye, Jane, "Are 'pseudonymised' data always personal data? Implications of the GDPR for administrative data research in the UK", Computer Law & Security Review, Cilt 34, Sayı 2, 2018, s. 222-233

Oğuz, Habip, "Elektronik Ortamda Kişisel verilerin Korunması, Bazı Ülke Uygulamaları ve Ülkemizdeki Durum", Uyuşmazlık Mahkemesi Dergisi, Cilt 0, Sayı 3, 2014, s. 1-38

Özcan, Göknil, Bankacılık İş Ve İşlemlerinde Kişisel Verilerin Korunması, Yayımlanmamış Yüksek Lisans Tezi, İstanbul Üniversitesi, Sosyal Bilimler Enstitüsü, İstanbul, 2019

Pekmez, Cüneyt, "Overview of the Definitons of Data Controller and Data Processor within the Scope of The Turkish Code of Personal Data Protection (TCDP)", Annales de la Faculté de Droit d'Istanbul, Sayı 67, 2019, s. 59-71

Pinsent Masons, "Identifying people on-line violates Data Protection laws, says European Court", (Erişim) https://www.pinsentmasons.com/out-law/news/identifying-people-on-line-violates-data-protection-laws-says-european-court, 13 Ocak 2020

Shastri, Supreeth, Wasserman, Melissa, Chidambaram, Vijay, "The seven sins of personal-data processing systems under GDPR", (Erişim) https://arxiv.org/pdf/1903.09305.pdf, 3 Şubat 2020

Singel, Ryan, "Netflix Spilled Your Brokeback Mountain Secret, Lawsuit Claims", (Erişim) https://www.wired.com/2009/12/netflix-privacy-lawsuit/, 22 Kasım 2019

Solmaz, Eren, "Avrupa İnsan Hakları Mahkemesi Kararları'nın "Kişisel Verilerin Korunması"na Katkısı", İdare Hukuku ve İlimleri Dergisi, Cilt 18, Sayı 1, 2019, s. 61-78

Sullivan, Clare, "EU GDPR or APEC CBPR? A comparative analysis of the approach of the EU and APEC to cross border data transfers and protection of personal data in the IoT era", Computer Law & Security Review, Cilt 35, Sayı 4, 2019, s. 380-397

Tekin, Nurullah, "Kişisel Verilerin Korunması İle İlgili Türkiye'deki Kanun Tasarısının Avrupa Birliği Veri Koruma Direktifi Işığında Değerlendirilmesi", Uyuşmazlık Mahkemesi Dergisi, Cilt 0, Sayı 4, 2014, s. 222-262

The GDPR Group Ltd., "Understanding GDPR Fines", (Erişim) https://www.gdpr.associates/what-is-gdpr/understanding-gdpr-fines/, 20 Ocak 2020

The Office of the Data Protection Authority, "Accountability and Governance ", (Erişim) https://odpa.gg/wp-content/uploads/2018/03/Accountability.pdf, 20 Kasım 2019

Tikkinen-Piri, Christina, Rohunen, Anna, Markkula, Jouni, "EU General Data Protection Regulation: Changes and implications for personal data collecting companies", Computer Law & Security Review, Cilt 34, Sayı 1, 2018, s. 134-153

Torre, Lydia F de la, "Google Spain & the Right to be Forgotten", (Erişim) https://medium.com/golden-data/google-v-spain-the-right-to-be-forgotten-aaee50dae43c, 3 Şubat 2020

Torre, Lydia F de la, "The right to restrict processing under EU data protection law", (Erişim) https://medium.com/golden-data/what-is-the-right-to-restrict-processing-under-eu-data-b6627db1319f, 2020 Ocak 3

Torre, Lydia F de la, "What is 'personal data' under EU data protection law?", (Erişim) https://medium.com/golden-data/what-is-personal-data-under-eu-data-protection-law-a9983fb2e483, 27 Şubat 2020

Torre, Lydia F de la, "What is a 'filing system' under EU data protection law?", (Erişim) https://medium.com/golden-data/what-is-a-filing-system-under-eu-data-protection-law-6e7222743f71, 3 Ocak 2020

Turan, Metin, Karşılaştırmalı Hukukta Kişisel Verilerin Korunması, Seçkin Yayınevi, Ankara, 2019

University of Reading, "Data Protection Glossary", (Erişim) https://www.reading.ac.uk/internal/imps/DataProtection/imps-d-p-glossary.aspx, 5t Şubat 2020

Verdoodt, Valerie, Valcke, P (Supervisor), Lievens, E (Co supervisor), Children's Rights And Advertising Literacy In The Digital Era: Towards An Empowering Regulatory Framework For Commercial Communication, Yayımlanmamış Yüksek Lisans Tezi, Ghent University, Faculty Of Law And Criminology, Ghent, 2018

Voss, W. Gregory, "European Union Data Privacy Law Reform: General Data Protection Regulation, Privacy Shield, and the Right to Delisting", The Business Lawyer, Cilt 72, Sayı 1, 2016, s. 221-234

Wachter, Sandra, "The GDPR and the Internet of Things: a three-step transparency model", Law, Innovation and Technology, Cilt 10, Sayı 2, 2018, s. 266-294

Waem, Heidi, van Essen, Jacqueline, Wellens, Vincent, "Can the GDPR's Main Players still fulfil their Roles Effectively in an Era Characterised by Developments such as the Blockchain and the Internet of Things?", (Erişim) https://www.e-nautadutilh.com/56/2412/landing-pages/part-2---gdpr.asp?sid=c5019f94-05ff-4f2c-a894-a5ba75ac9208, 5 Şubat 2020

Wolters, P.T.J., "The Control by and Rights of the Data Subject Under the GDPR", Journal of Internet Law, Cilt 22, Sayı 1, 2018, s. 7-18

Yargıtay 12. Ceza Dairesi'nin 2015/4348E. ve 2015/4865K. Sayılı Kararı

Yargıtay 12. Ceza Dairesi'nin 2017/150E. ve 2017/6231K. Sayılı Kararı

Yargıtay Ceza Genel Kurulu'nun 2012/1510E. ve 2014/331K. Sayılı Kararı

Yargıtay Ceza Genel Kurulu'nun 2012/1514E. ve 2014/312K. Sayılı Kararı

Yücedağ, Nafiye, "Kişisel verilerin korunması kanunu kapsamında genel ilkeler", Kişisel Verileri Koruma Dergisi, Cilt 1, Sayı 1, 2019, s. 47-63

Yücedağ, Nafiye, "Medeni Hukuk Açısından Kişisel Verilerin Korunması Kanunu'nun Uygulama Alanı Ve Genel Hukuka Uygunluk Sebepleri", İstanbul Üniversitesi Hukuk Fakültesi Mecmuası, Cilt 72, Sayı 2, 2017, s. 765-790

T.C.
KIRIKKALE ÜNİVERSİTESİ
SOSYAL BİLİMLER ENSTİTÜSÜ
HUKUK ANABİLİM DALI
KAMU HUKUKU BİLİM DALI

Kişisel Verilerin KVKK ve GDPR Kapsamında Korunması

Yüksek Lisans Tezi

Hazırlayan

Yüksel TOLUN

Danışman

Doç. Dr. İslam Safa KAYA

Haziran - 2020
KIRIKKALE