**İSTANBUL BİLGİ ÜNİVERSİTESİ**
**LİSANSÜSTÜ PROGRAMLAR ENSTİTÜSÜ**
**HUKUK YÜKSEK LİSANS PROGRAMI**

# KİŞİSEL VERİLERİN KORUNMASI KANUNU ÇERÇEVESİNDE DİJİTAL PLATFORMLARDAKİ KİŞİSEL VERİ İŞLEME UYGULAMALARININ DEĞERLENDİRİLMESİ

**Ceren CEYHAN**
**119615074**

**Dr. Öğr. Üyesi Nilgün BAŞALP YILDIRIM**

**İSTANBUL**
**2024**

Kişisel Verilerin Korunması Kanunu Çerçevesinde Dijital Platformlardaki Kişisel Veri İşleme Uygulamalarının Değerlendirilmesi

Evaluation on Personal Data Processing Activities in Digital Platforms under Personal Data Protection Law

Ceren CEYHAN
119615074

**Tez Danışmanı :** **Dr. Öğr. Üyesi Nilgün BAŞALP YILDIRIM**
İstanbul Bilgi Üniversitesi

**Jüri Üyeleri :** **Doç. Dr. Ece BAŞ SÜZEL**
İstanbul Bilgi Üniversitesi

**Dr. Öğr. Üyesi Çiçek ERSOY KEKEVİ**
İstanbul Teknik Üniversitesi

Tezin Onaylandığı Tarih : 7 Ekim 2024
Toplam Sayfa Sayısı : 137

Anahtar Kelimeler (Türkçe)
1) Kişisel Veri
2) Dijital Platform
3) Veri Sorumlusu
4) Veri Güvenliği
5) Veri İşleme

Anahtar Kelimeler (İngilizce)
1) Personal Data
2) Digital Platform
3) Data Controller
4) Data Security
5) Data Processing

## İÇİNDEKİLER

## KISALTMALAR

| | | |
|---|---|---|
| AB | : | Avrupa Birliği |
| 95/46/AT sayılı Direktif | : | 95/46/EC Kişisel Verilerin İşlenmesi ve Bu Tür Verilerin Serbest Dolaşımına Dair Bireylerin Korunması Direktifi |
| ABAD | : | Avrupa Birliği Adalet Divanı |
| AYUET | : | Aydınlatma Yükümlülüğünün Yerine Getirilmesinde Uyulacak Usul ve Esaslar Hakkında Tebliğ |
| BT | : | Bilgi teknolojileri |
| CNIL | : | Fransız Veri Koruma Otoritesi |
| DHTüz | : | Dijital Hizmetler Tüzüğü |
| DPTüz | : | Dijital Piyasalar Tüzüğü |
| E.T. | : | Erişim Tarihi |
| ETK | : | 6563 sayılı Elektronik Ticaretin Düzenlenmesi Hakkında Kanun |
| GDPR | : | General Data Protection Regulation |
| IEC | : | Uluslararası Elektronik Komisyonu |
| ISO | : | International Organization for Standardization |
| ISO 29100 | : | ISO/IEC 29100 Standardı |
| İntKanunu | : | 5651 sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun |
| Kurul | : | Kişisel Verileri Koruma Kurulu |
| Kurum | : | Kişisel Verileri Koruma Kurumu |
| KVKK | : | 6698 sayılı Kişisel Verilerin Korunması Kanunu |
| OECD | : | Organisation for Economic Co-operation and Development |
| RG | : | Resmî Gazete |
| T.C. | : | Türkiye Cumhuriyeti |

| | | |
|---|---|---|
| Unutulma Hakkı Rehberi | : | Unutulma Hakkının Arama Motorları Özelinde Değerlendirilmesi Rehberi |
| VERBİS | : | Veri Sorumluları Sicili Bilgi Sistemi |
| VERBİS Yönetmeliği | : | Veri Sorumluları Sicili Hakkında Yönetmelik |
| Veri Sorumlusuna Başvuru Tebliğ | : | Veri Sorumlusuna Başvuru Usul ve Esasları Hakkında Tebliğ |

## TABLO LİSTESİ

## ÖZET

Bu tez, dijital platformlarda kişisel verilerin işlenmesi konusunu ele almaktadır. İlk bölümde, kişisel veri kavramı ve özel nitelikli kişisel veriler açıklanarak, kişisel verilerin tanımı yapılmaktadır. Ayrıca, dijital platform kavramı üzerinde durulmakta ve dijital platformların kişisel veri kullanımı incelenmektedir. Dijital platformların 6698 sayılı Kişisel Verilerin Korunması Kanunu ("**KVKK**") uyarınca veri sorumlusu statüsü, veri sorumlularının yükümlülüklerine ilişkin konular ele alınmaktadır.

İkinci bölüm, dijital platformlarda kişisel verilerin işlenmesi bakımından özel konuları kapsamaktadır. Bu bölümde yurt dışına veri aktarımı, çerezler ile kişisel veri işleme faaliyetleri, platformların pazarlama faaliyetleri ve ilgili kişilerin hakları konuları işlenmektedir. Özellikle 12 Mart 2024 değişiklikleri sonrası yurt dışına veri aktarım kuralları ve Avrupa Birliği Genel Veri Koruma Tüzüğü (*General Data Protection Regulation ("**GDPR**")* ile KVKK'daki ilgili kişi haklarının karşılaştırılması yapılmaktadır.

Üçüncü bölümde, dijital platformlarda kişisel veri güvenliği üzerinde durulmaktadır. Bu bölüm, dijital platformlardaki kişisel verilerin güvenliği için alınabilecek teknik ve idari tedbirleri Kişisel Verileri Koruma Kurulu'nun ("**Kurul**") kararları ışığında dijital platformların mahremiyet endişelerini ve kişisel veri ihlal bildirimlerini kapsamaktadır.

Sonuç bölümünde yapılan çalışmaların genel bir değerlendirilmesi yapılmakta ve dijital platformlarda kişisel veri işleme faaliyetleri için öneriler sunulmaktadır.



**Anahtar Kelimeler:** Kişisel Veri, Dijital Platform, Veri Sorumlusu, Veri Güvenliği, Veri İşleme

## ABSTRACT

This thesis addresses the processing of personal data on digital platforms. The first chapter elaborates on the concept of personal data and special categories of personal data, defining personal data comprehensively. It also focuses on the concept of digital platforms and examines their use of personal data. The legal status of digital platforms under the Personal Data Protection Law No. 6698 ("**KVKK**") and the obligations of data controllers are detailed.

The second chapter covers specific issues regarding the processing of personal data on digital platforms. This section addresses cross-border data transfers, the processing of personal data via cookies, the marketing activities of platforms, and the rights of data subjects. In particular, it compares the rules on cross-border data transfer and the rights of data subjects under the General Data Protection Regulation ("**GDPR**") of the European Union and the KVKK following the amendments on March 12, 2024.

The third chapter focuses on personal data security on digital platforms. It discusses technical and administrative measures that can be taken to ensure the security of personal data on these platforms, in light of Personal Data Protection Board ("**Board**") decisions, and addresses privacy concerns and personal data breach notifications.

In the conclusion, a general evaluation of the studies is made, and recommendations for personal data processing activities on digital platforms are presented.



**Keywords:** Personal Data, Digital Platforms, Data Controller, Data Security, Data Processing.

# GİRİŞ

Dijitalleşmenin hızla ilerlediği günümüzde, kişisel verilerin korunması ve işlenmesi, hukuki ve etik açıdan büyük önem taşımaktadır. Özellikle dijital platformların hayatımızda daha fazla rol almasıyla birlikte, kişisel verilerin elde edilmesi, işlenmesi ve saklanması konuları çok boyutlu bir hale gelmiştir. Bu tez, dijital platformlarda kişisel verilerin işlenmesi konusunu ele alarak uygulamada bu konuda karşılaşılan sorunları açıklamayı ve örnek kararlar ışığında çözüm önerileri ortaya koymayı amaçlamaktadır.

Dijital platformlar kullanıcıların geniş bir yelpazede hizmetlere erişim sağlamasına olanak tanırken aynı zamanda büyük miktarda veri toplamaktadır. Bu veriler, kullanıcıların kimlik bilgileri, alışveriş alışkanlıkları, gezinme geçmişi, coğrafi konum bilgileri gibi geniş bir spektrumu kapsar. Kişisel verilerin bu denli geniş kapsamlı olarak işlenmesi, gizlilik ve veri güvenliği endişelerini beraberinde getirmektedir. Bu tez kapsamında dijital platformların veri işleme süreçleri incelenerek, bu süreçlerin hukuki boyutları değerlendirilecektir.

Birinci bölümde, kavramsal olarak kişisel verinin ne olduğu, dijital platformlarda kişisel veri işleme faaliyetlerinin nasıl yürütüldüğü ele alınacaktır. Özel nitelikli kişisel veriler de değerlendirilerek, kişisel verilerin korunmasına ilişkin örneklerle birlikte değerlendirmeler yapılacaktır. Bölümün devamında dijital platformların, kullanıcı verilerini nasıl topladığı, işlediği ve muhafaza ettiği incelenerek; bu süreçlerin KVKK'ya uygun bir şekilde nasıl yürütülmesi gerektiğine yer verilecektir. Özellikle dijital platformların aydınlatma yükümlülüğü, kişisel veri işleme ilkeleri gibi veri sorumlusunun yükümlülükleri ele alınacaktır.

İkinci bölümde, dijital platformlarda kişisel verilerin işlenmesi bakımından belirli konulara odaklanılacaktır. Yurt dışına veri aktarımı, çerezler ile veri işleme faaliyetleri, pazarlama faaliyetleri ve unutulma hakkı dahil dijital platformlarda ilgili kişilerce talep edilebilecek haklara ilişkin konular incelenecektir. Özellikle uluslararası yapıdaki dijital platformları etkileyen, yurt dışına veri aktarımına

ilişkin düzenlemelerdeki değişiklikler analiz edilecektir. Ayrıca, çerezler ve benzeri teknolojiler ile kişisel veri toplama ve işleme faaliyetlerinin hukuka uygunluğu değerlendirilecektir.

Üçüncü bölümde, dijital platformlarda kişisel veri güvenliği için alınması gereken teknik ve idari tedbirler incelenecektir. Bu tedbirler, Kurul kararları ışığında değerlendirilecektir. Ayrıca, dijital platformların profilleme faaliyetleri ve kullanıcı güvenliği de bu bölümde yer alacaktır.

Sonuç bölümünde ise yapılan çalışmaların genel bir değerlendirilmesi yapılacak ve dijital platformlarda kişisel veri işleme faaliyetleri için öneriler sunulacaktır. Bu bölümde tezde ele alınan konuların özet bir değerlendirilmesi yapılacaktır.

Bu tez, dijital platformların kişisel veri işleme faaliyetlerinin mevcut hukuki düzenlemeler ve Kurul kararları ışığında değerlendirilmesi ve bu alanda karşılaşılan sorunlara yönelik çözüm önerileri sunmayı amaçlamaktadır.

# BİRİNCİ BÖLÜM
# DİJİTAL PLATFORMLARDA KİŞİSEL VERİLERİN İŞLENMESİ

## 1.1. DİJİTAL PLATFORM KAVRAMI

Dijital platform kavramı, dijitalleşen dünyada 2020 yılında yaşanan pandeminin de etkisiyle yediden yetmişe herkesin hayatının bir parçası haline gelmiş durumdadır. Bu durumun bir getirisi olarak, 4. Sanayi Devrimi yeniliklerinin en büyük etkilerinden kişisel verilerin konumu oldukça önemlidir.[1]

Alışveriş merkezlerinde saatler harcadığımız zamanlardan, şimdilerde dijital platformları ziyaret ettiğimiz günlere geçiş yaptık. Platform kültürü dijital dünyadan önce aslında gündelik yaşantımızın içerisinde hep vardı; örneğin gazeteler ve dergiler, bir yandan okuyucusuna içerik sunarken diğer yandan tüketicilere ulaşmaya çalışan teşebbüslere reklam mercii olarak hizmet vermekteydi. Diğer bir örnek ise televizyon kanallarının haber, dizi, film gibi içerik sunarken aynı zamanda reklam vermek isteyen teşebbüslere de reklam mecrası olarak hizmet sunmasıdır.[2]

Avrupa Birliği ("**AB**") mevzuatında dijital platformları düzenlemek adına iki önemli düzenleme bulunmaktadır: Dijital Piyasalar Tüzüğü (*Digital Markets Act*)[3] ("**DPTüz**") ve Dijital Hizmetler Tüzüğü (*Digital Services Act*)[4] ("**DHTüz**"). DPTüz, dijital piyasalardaki kapı bekçilerini (*gatekeepers)* düzenlemeye odaklanırken[5], DHTüz ise çevrimiçi hizmetlerin işleyişine ve kullanıcıların

[1] **TIKKINEN-PIRI, Christina / ROHUNEN, Anna / MARKKULA, Jouni;** EU General Data Protection Regulation: Changes and Implications for Personal Data Collecting Companies, Computer Law&Security Reviews, Cilt:34, Sayı.1, Şubat 2018 s.134-153, s.138.
[2] **DOĞAN, Cihan,** Rekabet Hukuku ve İktisadi Bağlamında Dijital Platformlar, İstanbul, On İki Levha Yayıncılık, 2021, s.5, 6, 7.
[3] Dijital Piyasalar Tüzüğü, (*Regulation (EU) 2022/1925 of the European Parliament and of The Council of 14 September 2022 on contestable and fair markets in the digital sector and amending Directives (EU) 2019/1937 and (EU) 2020/1828),* Official Journal, L 265, 12.10.2022, s. 1–66
[4] Dijital Hizmetler Tüzüğü (*Regulation (EU) 2022/2065 of the European Parlıament and of the Council Of 19 October 2022 on a Single Market for Digital Services and Amending Directive 2000/31/EC),* Official Journal, L 277, 27.10.22, s. 1–102.
[5] Dijital Piyasalar Tüzüğü (*Digital Market Act*), dijital sektörde adil ve rekabetçi bir piyasa sağlamak amacıyla, AB içindeki "kapı bekçileri" (gatekeepers) için uyumlaştırılmış kurallar belirlemektedir. Tüzük, AB'de faaliyet gösteren iş kullanıcıları ve son kullanıcılar için temel platform hizmetleri

çevrimiçi haklarının korunmasına[6] odaklanmaktadır. Her iki düzenleme de dijital platformları tanımlamak için belirli kriterler ve tanımlar içermektedir.

DPTüz kapsamında kapı bekçisi olarak nitelendirilen büyük platformlar, belirli yükümlülükler ve kısıtlamalara tabi tutulmaktadır. Bu platformların, pazardaki hâkim durumlarını kötüye kullanarak rekabeti kısıtlamamaları için belirli düzenlemelere uyması gerektiği düzenlenmektedir. Öte yandan, DHTüz, çevrimiçi hizmet sağlayıcılarının, kullanıcıların güvenliğini ve temel haklarını korumak için alması gereken önlemleri belirlemekte ve platformların içerik yönetimi, reklamcılık ve kullanıcıların şikayetlerini ele alma konularında şeffaf ve hesap verebilir olmalarını sağlamayı hedeflemektedir.

DHTüz kapsamında platformlar "çevrimiçi aracılık hizmetleri" (*online intermediary services)* olarak tanımlanmakta olup, bir veya birden fazla üçüncü kişinin hizmetlerini kullanıcılarına sunan hizmet olarak ifade edilmektedir. Bu tanım çevrimiçi pazar yerlerini, sosyal medya platformlarını ve diğer çeşitli çevrimiçi hizmetleri içermektedir.

Türkiye'de dijital platformlara, öncelikle 6563 sayılı Elektronik Ticaretin Düzenlenmesi Hakkında Kanun[7] ("**ETK**") uygulanmaktadır. ETK'nın 2. maddesi kapsamında platform kavramı olarak değerlendirilebilecek "aracı hizmet sağlayıcı" ve "e-ticaret aracı hizmet sağlayıcı" tanımları yapılmaktadır.

ETK'da aracı hizmet sağlayıcıları, "*başkalarına ait bilgileri ileten, bu bilgilere erişimi sağlayan veya saklayan hizmet sağlayıcı"* olarak tanımlanmaktadır. E-ticaret aracı hizmet sağlayıcıları ise, ETK'da "*elektronik ticaret ortamında, mal veya hizmetlerin çevrimiçi olarak sunulması, sipariş*

sunan kapı bekçilerini kapsamaktadır. Ancak, elektronik iletişim ağları ve hizmetleri gibi belirli sektörler bu tüzüğün kapsamı dışında tutulmuştur.

[6] Dijital Hizmetler Tüzüğü (*Digital Services Act*), aracılık hizmetleri için güvenli, öngörülebilir ve güvenilir bir çevrimiçi ortam sağlamak amacıyla uyumlaştırılmış kurallar belirlemektedir. Tüzük, aracılık hizmeti sağlayıcılarının sorumluluktan muafiyetine ilişkin bir çerçeve, belirli hizmet sağlayıcılara yönelik özen yükümlülükleri ve kanunun uygulanması ile ilgili kuralları içermektedir.

[7] RG: 05.11.2014, 29166.

*edilmesi veya satın alınması amacıyla sunulan elektronik ortamlarda hizmet sağlayıcı veya alıcıların bu ortama erişimi sağlayan veya bu ortamda sunulan mal ve hizmetlere ilişkin bilgileri saklayan hizmet sağlayıcı"* olarak tanımlanmaktadır. Bu tanımdan anlaşıldığı üzere e-ticaret hizmet sağlayıcıları, satıcı ve alıcıları bir araya getiren elektronik ticaretin gerçekleşmesine aracılık eden dijital platformları kapsamaktadır.

AB mevzuatı kapsamında DPTüz de ETK da elektronik ortamda hizmet sunan ve aracılık eden dijital platformları benzer şekilde tanımlamaktadır. Ancak, Türk hukukundaki tanımlar daha çok elektronik ticarete yönelik iken, DPTüz daha geniş bir yelpazede çevrimiçi hizmetleri düzenlemektedir.

Türk hukukundaki "e-ticaret aracı hizmet sağlayıcı" tanımı, DPTüz'deki "çevrimiçi aracılık hizmetleri" (*online intermediary services*) tanımına benzer şekilde çevrimiçi pazar yerlerini ve mal veya hizmet sunan diğer elektronik ortamları içermektedir. Ancak, DPTüz daha geniş bir çerçevede arama motorları, sosyal medya platformları dahil olmak üzere diğer çevrim içi hizmet sağlayıcıları ile kullanıcıların çevrimiçi etkileşimlerini düzenlemektedir[8].

Türkiye'de elektronik ticaret platformları dışındaki diğer dijital platformlara yönelik düzenlemeler de günlük hayatımızda "İnternet Kanunu" olarak bilinen 5651 sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun ("**İntKanunu**")[9]

[8] DPTüz madde 2'deki "çevrimiçi aracılık hizmetleri" (*online intermediary services)* tanımı, Avrupa Parlamentosu ve Konseyi'nin çevrimiçi aracılık hizmetlerinin kullanıcılarına yönelik adillik ve transparanlığı teşvik etmeyi amaçlayan 20 Haziran 2019 tarihli 2019/1150 sayılı Tüzüğü'ne atıf yapmaktadır. Bu Tüzüğe göre 'çevrimiçi aracılık hizmetleri', aşağıdaki şartların tamamını karşılayan hizmetleri ifade eder:

1. Avrupa Parlamentosu ve Konseyi'nin 9 Eylül 2015 tarihli ve 2015/1535 sayılı Direktifi'nin 1. maddesinin 1. fıkrasının (b) bendinde tanımlanan anlamda bilgi toplumu hizmetlerini oluşturması;
2. Kullanıcılarının, tüketicilere mal veya hizmet sunmasına ve bu kullanıcılar ile tüketiciler arasında doğrudan işlemlerin başlatılmasını bu işlemlerin nihai olarak nerede sonuçlandığından bağımsız olarak kolaylaştırması;
3. Kullanıcılarına, bu hizmetleri sunan sağlayıcı ile tüketicilere mal veya hizmet sunan kullanıcılar arasındaki sözleşmesel ilişkilere dayalı olarak sağlanması (2019/1150 sayılı Tüzük, Madde 2, bent (2)).

[9] RG: 23.05.2007, 26530.

kapsamında yer almaktadır.

İnt Kanunu'nun 2. maddesinin birinci fıkrasının (f) bendi "içerik sağlayıcı" kavramını, "*kendi oluşturduğu veya üçüncü kişilerden aldığı içeriği internet ortamında kullanıcılara sunan kişi veya kuruluşlar"* olarak tanımlamaktadır. Yine İntKanunu'nun 2. maddesinin birinci fıkrasının (m) bendinde "yer sağlayıcı" kavramı ise "*başkalarına ait içeriklerin internet ortamında yayınlanmasını sağlayan hizmet sağlayıcıları"* olarak tanımlanmaktadır.

Türkiye'de "dijital platform" kavramını tek bir düzenlemeye altında tanımlamak mümkün değildir. İş hukuku düzenlemelerinde platformlar mal, hizmet ve yazılımların bağımsız kişiler arasında, internet üzerinden, ücret karşılığı veya ücretsiz olarak paylaşımını sağlayan dijital ortamlar olarak açıklanmıştır.[10] Bu düzenlemeler kapsamında platformun rolü, sürece müdahil olacak şekilde kurulu altyapısı ile tarafların arz ve talebini bir araya getirmek olduğu belirlenmiştir.[11]

Bu bağlamda dijital platformların, e-ticaret platformları, sosyal medya platformları, ilan platformları gibi çeşitli konularda karşımıza çıkan dijital platformlar, birden fazla tarafın farklı sıfatlar ile gerek içerik sağlayıcı gerek yer sağlayıcı gerek aracı hizmet sağlayıcı gerek hizmet sağlayıcı olacak şekilde bir araya geldiği, karşılıklı bilgi akışında bulunduğu ortamlar olarak tanımlanması doğru bir yaklaşım olacaktır.

## 1.2. DİJİTAL PLATFORMLARDA KİŞİSEL VERİ KAVRAMI

Küreselliğin arttığı bilgi ve iletişim teknolojilerinin kullanımının son derece yaygınlaştığı günümüzde, birçok veri bulut bilişim ile saklanmaya başladı, bireylerin sosyal medya kullanımının yoğunlaşması ile birlikte dijital

[10] ILO: World Employment and Social Outlook The Role of Digital Labour Platforms in Transforming the World of Work, Cenevre 2021, s. 33.
[11] ILO 2018, s. 1; **BAYCIK, Gaye/ CİVAN, Orhan Ersun/ TOLU YILMAZ, Hazal/ BOSNA, Berrin**: "Platform Çalışanlarını Yasal Güvenceye Kavuşturmak: Sorunlar ve Çözüm Önerileri", Galatasaray Üniversitesi Hukuk Fakültesi Dergisi, S:1, 2021, 713-801, s. 716.

platformlarda kişisel veri kavramı ve güvenliğinin önemi gün geçtikçe artmaktadır.[12]

"Kişisel veri" kavramının tanımında Türkiye'de ve dünya üzerinde görüş birliği sağlanmıştır, bu kapsamda bireye yönelik bir bilgi veya bilgi kümesini ifade edecek şekilde düzenlenmektedir.[13] Bu doğrultuda KVKK'nın 3. maddesinin birinci fıkrasının (d) bendinde bu kavram "*kimliği belir veya belirlenebilir gerçek kişiye ilişkin her türlü bilgi*" olarak tanımlanmaktadır.[14] Maddenin gerekçesine baktığımızda ise; gerçek kişiye ait yalnızca ad, soyadı, doğum günü gibi bir kişiyi şüphesiz bir şekilde tanımlanabilir kılan veriler değil; ayrıca gerçek kişiye ait fiziki, ailesine ilişkin, sosyal hayatına ilişkin veya diğer konularda gerçek kişiye ait verilerin de bir kişiyi belirlenebilir kıldığı sürece kişisel veri olarak nitelendirildiği belirtilmektedir.[15]

Bir kişinin belirli veya belirlenebilir olması ifadesi ile mevcut verilerin gerçek kişi ile ilişkilendirilmesi ise o gerçek kişiyi tanımlanabilir hale getirebilmesi niteliği anlaşılmaktadır.[16] Bu noktada doğrudan bir gerçek kişiyi tanımlayacak şekilde somut bir içerik taşımasa da kimlik numarası gibi başka bir kayıt ile ilişkilendirildiğinde bir kişi belirlenebilir hale geliyorsa kişisel veri olarak değerlendirilmektedir.[17]

---

[12] **BAŞALP, Nilgün**; Avrupa Birliği Veri Koruması Genel Regülasyonu'nun Temel Yenilikleri, 2015, 21 Marmara Üniversitesi Hukuk Fakültesi Hukuk Araştırmaları Dergisi, s.85.

[13] **TAŞTAN, Furkan Güven**, Türk Sözleşme Hukukunda Kişisel Verilerin Korunması, On İki Levha Yayıncılık, İstanbul, 2017, s. 35.

[14] Kişisel veri kavramının tanımına ilişkin dünya üzerinde görüş birliği sağlanmıştır. OECD'nin 1980 yılında yayınladığı rehber kapsamında ("Guidelines on the Protection of Privacy and Transborder Flows of Personal Data") (https://www.oecd-ilibrary.org/docserver/9789264196391-en.pdf?expires=1710964015&id=id&accname=guest&checksum=DBF322B08C808FC584FA61E85F578921) (E.T.:16.09.2024), 108 sayılı "*Kişisel Verilerin Otomatik İşlenmesi Karşısında Bireylerin Korunması Sözleşmesi'nin* 2/a maddesinde (https://rm.coe.int/1680078b37) (E.T.:16.09.2024), 95/46/EC sayılı Avrupa Direktifinin 2/a maddesinde (https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A31995L0046) (E.T.:16.09.2024)ve Avrupa Birliği Genel Koruma Tüzüğü'nün 4/1 maddesinde de (https://eur-lex.europa.eu/eli/reg/2016/679/oj) (E.T.:16.09.2024) aynı şekilde tanımlanmıştır.

[15] **KÜZECİ, Elif**, Kişisel Verilerin Korunması, On İki Levha, Ankara, 2020, s.10.

[16] Benzer tanım için Anayasa Mahkemesi'nin 19.01.2012 tarihli, 2010/40 Esas, 2013/8 sayılı Kararı

[17] Kişisel Verileri Koruma Kurumu, Madde ve Gerekçesi İle Kişisel Verilerin Korunması Kanunu (Bilgi Notu) Ve Kişisel Verilerin Korunmasına İlişkin Terimler Sözlüğü, s.9

"Kişisel veri" kavramı tanım ve madde gerekçesinden de açıkça görüldüğü üzere sınırlı sayıda belirlenmemiş, genel bir tanımlama ile açıklanmıştır. Bir kişinin belirli veya belirlenebilir olması, mevcut verilerin doğrudan veya dolaylı bir şekilde o ilgili kişi ile ilişkilendirilmesiyle sağlanmaktadır. Bu; kişinin ismi, doğum tarihi, T.C. kimlik numarası gibi kesin bir şekilde kişiyi tanımlayan bilgiler olabileceği gibi aynı zamanda fiziksel özellikleri, hobileri, ekonomik durumu gibi diğer bilgileri de içerebilmektedir. Bir verinin kişisel veri olması için önemli nitelikte olmasına da gerek yoktur. Bir kişiye ait önemli sayılmayan, gizli nitelikte de olmayan bir bilgi kişisel veridir. Örneğin, banka hesabının şifresi gizli tutulması gereken bir bilgi iken kişinin arabasının rengi herkes tarafından bilinen bir bilgidir. Kişiye ait iki bilgi de kişisel veri niteliğindedir.[18]

Anılan hükümde sınırlı bir tanım yapılmayarak aslında gelişen teknolojiler ile ortaya çıkabilecek yeni veri kategorilerini de kapsayacak bir kişisel veri tanımı verilmiştir.[19] Örneğin geçmişte "alışveriş alışkanlıkları" gibi bir veri kategorisi günlük hayatımızda karşımıza çıkmazken, günümüzde her platform kullanıcısının aşina olduğu bir kategori haline gelmiştir. "Alışveriş alışkanlıkları" kişisel veri kategorisi olarak, bireylerin satın alma davranışlarını, tercihlerini ve harcama eğilimlerini yansıtan bilgilerden oluşmaktadır. Bu veriler, özellikle veri madenciliği teknikleri kullanılarak analiz edilmekte ve müşteri ilişkileri yönetimi (CRM) kapsamında stratejik kararlara temel oluşturmaktadır. Örneğin, bir çalışmada alışveriş alışkanlıkları, müşterilerin demografik özellikleri ile incelenmiş ve alışveriş davranışlarını etkileyen ana değişkenler belirlenmiştir. Bu tür veriler, pazarlama stratejilerinin kişiselleştirilmesi ve tüketici davranışlarının

(https://www.kvkk.gov.tr/Icerik/5388/Madde-ve-Gerekcesi-ile-Kisisel-Verilerin-Korunmasi-Kanunu-Bilgi-Notu-ve-Kisisel-Verilerin-Korunmasina-Iliskin-Terimler-Sozlugu) (E.T.: 16.09.2024).

[18] **AKGÜL, Aydın**, Danıştay ve Avrupa İnsan Hakları Mahkemesi Kararları Işığında Kişisel Verilerin Korunması, Beta Yayınları, İstanbul, 2016.

[19] Kişisel Verileri Koruma Kurumu, 6698 sayılı Kanunda Yer Alan Temel Kavramlar, s.14, 15 (https://www.kvkk.gov.tr/SharedFolderServer/CMSFiles/8110dc3c-2856-4e54-9129-5e2e375469af.pdf) (E.T.: 16.09.2024) ve Küzeci, s.314-315.

daha iyi anlaşılması için kritik bir öneme sahip hale gelmiştir.[20]

Bu doğrultuda, isim, iletişim bilgisi, araç bilgisi, kimlik veya pasaport numarası, fotoğraf, kredi kartı bilgisi, sendika bilgisi gibi doğrudan bilgi taşıyan veriler ile bir araya gelmesi ile kişiyi tanımlanabilir hale getiren verilerden oluşan (doğum tarihi, telefon numarası, araç plakası, vb.) bilgiler kişisel veri kapsamında değerlendirilmektedir.[21]

Özel nitelikli kişisel veri kavramı ise KVKK'nın 6. maddesinde sınırlı sayıda olacak şekilde tanımlanmıştır: "*kişilerin ırkı, etnik kökeni, siyasi düşüncesi, felsefi inancı, dini, mezhebi veya diğer inançları, kılık ve kıyafeti, dernek, vakıf ya da sendika üyeliği, sağlığı, cinsel hayatı, ceza mahkumiyeti ve güvenlik tedbirleriyle ilgili verileri ile biyometrik ve genetik verileri özel nitelikli kişisel veridir.*"

Madde gerekçesi incelendiğinde, bu maddede sayılan kişisel verilerin, üçüncü kişilerce öğrenilmesi halinde ilgili kişinin ayrımcılığa uğramasına, mağdur olmasına sebep olabileceğinden özel nitelikli olarak sınıflandırıldığı belirtilmektedir.[22]

Dijital platformlar, geleneksel olarak bilinen kişisel verilerin ötesinde kullanıcıların davranışları ve işlemleri ile ilişkili kişisel verilerini de kapsayan kullanıcı hareketleri de dahil olacak şekilde çok geniş bir kişisel veri türünü işlemektedir. Yapay zekâ, makine öğrenimi gibi ileri teknolojiler ile olan bu etkileşim, kişileri dolaylı olarak tanımlayabilen veya etkileyebilen verilerin dijital platformlar aracılığıyla toplanmasına imkân sağlamaktadır. Böylece kişisel veri tanımı da oldukça genişlemektedir. Dijital platformlar tarafından yaratılan bu karmaşık veri ekosistemi ve hızla gelişen teknolojik gelişmelere ayak uydurmak

[20] Umman Tuğba Şimşek, "Veri madenciliği ve müşteri ilişkileri yönetiminde (CRM) bir uygulama," Doktora Tezi, İstanbul Üniversitesi, Sosyal Bilimler Enstitüsü, Sayısal Yöntemler Bilim Dalı, 2006. Tez bağlantısı: https://tez.yok.gov.tr/UlusalTezMerkezi/tezDetay.jsp?id=SHQeQrNLBdDS_RADHJThrg&no=PdfR5WEOenvfhwwSCkL6Vw (E.T.: 16.09.2024).

[21] **BAŞALP, Nilgün**, Kişisel Verilerin Korunması ve Saklanması, Ankara, Yetkin Yayınları, 2004, s.33, 34.

[22] Özel nitelikli kişisel verilerin işlenmesine ilişkin açıklamalar "1.2" başlığında yer verilmektedir.

geleneksel veri hukuku düzenlemelerinin gelişimi için oldukça önemlidir.[23]

Dijital platformların faaliyetlerini geliştirmesi, kullanıcı tecrübesini iyileştirmesi gibi amaçlarla geleneksel veri hukukunda karşılaştığımız kişisel veri kategorileri de genişlemeye başladığı görülmektedir. Örneğin bir sosyal medya platformunda hesap oluşturulurken kullanıcı adı, e-posta adresi, profil resmi gibi kullanıcı verileri temel veri kategorileri arasında yer almaktadır. Bu kişisel verilerin işlenmesi kullanıcı profili oluşturularak kişiselleştirilmiş içeriklerin sunulmasına yardımcı olmaktadır. Kullanıcı davranışlarını analiz etmeye ve kişilerin tercihlerine yönelik içerik oluşturmaya izin veren davranışsal veriler ise platformdaki kullanıcının beğendiği yorumlar, içerikler veya yaptığı paylaşımlar gibi kullanıcı hareketlerini takip ederek işlenmektedir. Ayrıca, dijital platformlar, kullanıcıların arkadaş listesi, takipçileri, üye olduğu gruplar gibi sosyal bağlantılarını da içeren bağlantı verilerini işlemektedir. Bu bilgilerle sosyal grafik oluşturarak bağlantı (*network)* etkisinin gelişmesini sağlayabilmektedirler. Dijital platformların performanslarının ve güvenliğinin optimizasyonu için otomatik olarak işlenen cihaz ve kullanım verileri ise cihazların kullanım hizmetleri sırasında işlenen IP adresi, cihaz tipi, hesaba giriş yapma sıklığı, çevrimiçi kalma uzunluğu gibi hareketlerin takip edilmesi ile elde edilmektedir.[24]

## 1.3. DİJİTAL PLATFORMLARDA KİŞİSEL VERİ İŞLEME FAALİYETLERİ

Dijital platformlar, sundukları hizmetlerin temelini oluşturan kişisel verileri çeşitli amaçlarla kullanabilmektedirler. Bu kullanım şekilleri genellikle platformun hizmet türüne, iş modeline ve kullanıcı sözleşmesine bağlı olarak değişmektedir.

[23] **GELLERT, Raphael;** Personal data's ever-expanding scope in smart environments and possible path(s) for regulating emerging digital technologies, International Data Privacy Law, 2021, Vol.11, No.2, Oxford University Press, s.196-208.
[24] **KUENZLER, Adrian;** On (some aspects of) social privacy in the social media space, 2022, Vol.12, No:1, Oxford University Press, s. 63-73.

Dijital platformlar, uygulamada genelde kullanıcı deneyimini geliştirmek ve kişiselleştirmek aynı zamanda hizmet sunumunu optimize ederek üyelik oluşturmak gibi amaçlarla kullanıcıların hesap bilgilerini, e-posta adreslerini, tercihlerini, alışveriş geçmişini veya etkileşimlerini elde etmekte, analiz etmekte ve kullanmaktadır. Reklam ve pazarlama faaliyetleri bağlamında ise kişisel veriler, kullanıcıların ilgi alanlarına, tercihlerine ve hareketlerine uygun hedeflenmiş reklamların gösterilmesinde kritik bir rol oynamaktadır. Bu uygulama, reklam verenlerin verimliliğini artırma noktasında etki ederken kullanıcılar bakımından da ilgisini çekebilecek içeriklere erişmelerini kolaylaştırmaktadır.

Ayrıca, dijital platformlar analiz ve iyileştirme çalışmaların, kullanıcı davranışlarını inceleyerek hizmetlerini geliştirmek ve yeni özellikler, eklentileri kullanıcılarına sunmak amacıyla da kullanıcıların kişisel verilerinden yararlanmaktadır. Bir başka amaç da dijital platformun güvenliğini sağlayarak dolandırıcılıkların önüne geçmektir.

Öte yandan dijital platformlar yasal yükümlülükleri çerçevesinde de kullanıcıların belirli kişisel verilerini toplayarak belirli bir süre muhafaza edebilmektedir. Diğer yaygın kullanım şeklide de kullanıcılardan elde edilen kişisel verilerin anonimleştirerek veya kümeleştirerek kullanıcıyı tanımlanamaz hale getirmek suretiyle yeni teknolojilerin geliştirilmesi ve pazar yönelimlerinin anlaşılması gibi amaçlarla da kullanılabilmektedir.

Yukarıda örnek verdiğimiz kişisel veriler üzerindeki tüm faaliyetler "kişisel verilerin işlenmesi" olarak tanımlanmaktadır. KVKK'nın 3. maddesinin birinci fıkrasının (e) bendinde "kişisel verilerin işlenmesi" kavramı şu şekilde tanımlanmaktadır; "*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 işlem*".[25]

Dijital platformların veri işleme faaliyetlerini çözümleyebilmek adına bu tanımda yer alan "otomatik işleme" ile otomatik olmayan işleme" arasındaki farkın belirlenmesi önemli bir referans noktası oluşturacaktır.

Otomatik işlemeye dair KVKK'da herhangi bir tanım yer almamaktadır.[26] Organisation for Economic Co-operation and Development'ın ("**OECD**") yaptığı tanıma göre; "*insan müdahalesine veya etkine olan ihtiyacı en az seviyeye düşüren, birbirlerine bağlantılı ve birbirlerinden etkileşim alan elektrikli veya elektronik bir sistemin gerçekleştirdiği veri işleme faaliyetidir"*.[27] Kurum'a göre ise otomatik işleme, kendi işlemcisi olan cihazların, sahip olduğu yazılım veya donanımlar sayesinde insan etkisi olmaksızın daha önceden hazırlanan algoritmaları kullanarak yürüttüğü faaliyettir.[28]

Otomatik olmayan işleme faaliyetinin KVKK kapsamında değerlendirilebilmesi için ise bir "veri kayıt sistemi" aracılığıyla işlenmesi gerekmektedir. KVKK'nın 3. maddesinin birinci fıkrasının (h) bendinde veri kayıt sistemi, *kişisel verilerin belirli kriterlere göre yapılandırılarak işlendiği kayıt sistemi* olarak tanımlanmaktadır. Buna göre verilerin elden işlenmesi hali gerekli olacaktır, örneğin bir işyeri ziyaretlerini takip amacıyla tutulan ziyaretçi defterinde yer alan kişisel verileri otomatik olmayan veri işleme faaliyeti olarak değerlendirilmektedir.[29]

Bu tanımlamalar kapsamında baktığımızda dijital platformlar, ilk defa elde etme anında başlayarak devamındaki düzenleme, yapılandırma, uyumlaştırma,

---

[25] Küzeci, s. 107.
[26] **OĞUZ, Sefer**, Kişisel Verilerin Korunması Hukukunun Genel İlkeleri, BEYDER. 2018, C. 13, S.2, s.121-138, s.128.
[27] OECD Glossary of Statistical Terms, (https://read.oecd-ilibrary.org/economics/oecd-glossary-of-statistical-terms_9789264055087-en#page39). (E.T.: 16.09.2024)
[28] Kişisel Verileri Koruma Kurumu, 6698 sayılı Kanunda Yer Alan Temel Kavramlar, s. 18. (https://www.kvkk.gov.tr/SharedFolderServer/CMSFiles/8110dc3c-2856-4e54-9129-5e2e375469af.pdf) (E.T.: 16.09.2024)
[29] Başalp, Kişisel Verilerin Korunması, s.33.

silme gibi her türlü işlemler ile kişisel verileri işleyebilmektedir.[30] Dijital platform kullanıcısı olarak kişisel verisi işlenen ilgili kişiler de dijital platformda satış yapan gerçek kişi veya tüzel kişinin gerçek kişi yetkilisi olabileceği gibi ürün ve hizmetlerden faydalanan son kullanıcı da olabilmektedir.

## 1.4. DİJİTAL PLATFORMLARIN KVKK KAPSAMINDA HUKUKİ STATÜSÜ: VERİ SORUMLUSU MU? VERİ İŞLEYEN Mİ?

Dijital platformların KVKK'dan doğan yükümlülüklerini belirlemek adına belirli veri işleme faaliyeti kapsamında veri sorumlusu veya veri işleyen olarak hangi hukuki statüye sahip olduğunu belirlemek önemlidir. Sundukları hizmetlerin niteliğine ve kişisel veriler üzerindeki kontrol düzeylerine, yani bir başka kişiden alınan yetkiye göre hareket etmesine, bağlı olarak ya veri sorumlusu ya da veri işleyen olarak değerlendirilmektedir. [31]

KVKK'nın 3. maddesinin birinci fıkrasının (ı) bendi "veri sorumlusu*"* kavramını, *"kişisel verilerin işlenme amaçlarını ve araçlarını belirleyen, veri kayıt sisteminin kurulmasından ve yönetilmesinden sorumlu olan gerçek veya tüzel kişi"* olarak tanımlamaktadır. Bu kapsamda veri üzerinden uygulanacak her türlü işleme yönelik karar mekanizması veri sorumlusudur.[32] Bir dijital platformun veri sorumlusu olup olmadığı, veri işleme faaliyetlerindeki kontrol derecesine bağlıdır. Eğer söz konusu dijital platform, kullanıcı verilerinin hangi amaçla ve nasıl işleneceğine karar verebiliyorsa, bu durumda veri sorumlusu olarak kabul edilebilecektir.

"Veri işleyen" kavramı ise KVKK'da "*veri sorumlusunun verdiği talimatlar doğrultusunda ve onun adına kişisel verileri işleyen gerçek veya tüzel kişi"* olarak tanımlanmaktadır. Bir platformun veri işleyen olup olmadığı, veri işleme

[30] Başalp, Kişisel Verilerin Korunması, s.33; KVKK, Madde Gerekçesi: m.3; **ÇEKİN, Mesut Serdar**, Avrupa Birliği Hukukuyla Mukayeseli Olarak 6609 Sayılı Kişisel Verilerin Korunması Kanunu, İstanbul, 2020 s.39.
[31] Küzeci, s.319.
[32] ÇELİKEL, Serdar, "Kişisel Verilerin Korunması Hukuku Kapsamında Veri Sorumlusu ve Veri Sorumlusunun Yükümlülükleri", Doktora Tezi, Ankara Üniversitesi, 2021, s. 84.

faaliyetindeki yetki ve sorumluluk düzeyine bağlıdır.

Kurul'un 2020/71 sayılı Kararı[33], dijital platformların veri sorumlusu ve veri işleyen olarak değerlendirilmesinde dikkat edilmesi gereken hususlar için yol gösterici niteliktedir.

Bir dijital platformun veri sorumlusu olarak değerlendirilmesi için platformun neden, ne zaman ve ne kadar süreyle bu faaliyetin yürütüleceği, kimlerin bundan sorumlu olacağı gibi konularda karar verme yetkisine sahip olması gerekmektedir. Bu noktada belirleyici kriterler aşağıdaki gibidir:

- Toplama Yöntemi: Veri sorumlusu olan taraf hangi kişisel verilerin nasıl toplanacağına karar veren taraftır.

- Toplanacak Kişisel Veri Türleri: Hangi türdeki kişisel verilerin toplanacağına veri sorumlusu karar vermektedir.

- Kimlerin Kişisel Verisinin Toplanacağı: Veri sorumlusu hangi ilgili kişi gruplarının kişisel verilerinin toplanacağını belirlemektedir.

- Kişisel Verinin Kimin İşleyeceğine Karar Verme: Veri sorumlusu, kişisel verilerin kim tarafından işleneceğine karar vermektedir.

- İşleme Faaliyetinin Temel Unsurlarına Karar Verme: Veri sorumlusu olan taraf kişisel verilerin işlenme amaç ve araçları, süresi ve saklama yeri gibi işlemenin temel unsurlarına karar vermektedir.

- Kişisel Verilerin Aktarımına Karar Verme: Veri sorumlusu olan taraf elde edilen kişisel verilerin bir üçüncü tarafa aktarılıp aktarılmayacağına, aktarılacaksa hangi taraflara aktarılacağına karar vermektedir.

[33] Veri sorumlusu ve veri işleyenin tespitinde göz önünde bulundurulması gereken hususlar ile aydınlatma yükümlülüğünün kim tarafından yerine getirileceğine ilişkin Kişisel Verileri Koruma Kurulunun 30/01/2020 tarihli ve 2020/71 sayılı Karar Özeti (https://www.kvkk.gov.tr/Icerik/6874/2020-71) (E.T.: 16.09.2024).

- Kişisel Verilerin İşlenmesine Yönelik Özerk Karar Verme Yetkisi: Veri sorumlusu olan taraf, kişisel verilerin işlenmesi konusunda bağımsız kararlar alabilmektedir. Bu kararlarında herhangi bir üçüncü tarafından talimatlarına tabi değildir.

- İlgili Kişilerle Doğrudan Muhatap Olma: Veri sorumlusu, ilgili kişilerle doğrudan iletişim kurarak onların KVKK madde 11'deki haklarını kullanmalarını sağlamaktadır

- Veri İşleyen Atama Yetkisi: Veri sorumlusu, bir veri işleyen atayarak kendi adına veri işleme faaliyetlerin yürüttürebilir.

- Kişisel Veri İşleme Faaliyetinden Menfaat Sağlama: Veri sorumlusu olan taraf, kişisel verilerin işlenmesinden doğrudan veya dolaylı olarak menfaat sağlamaktadır.

Bu kriterler ışığında, veri sorumlusunun tespiti için kişisel verilerin işlenmesinde temel karar mekanizmasının kim olduğu belirleyici olmaktadır. Yapılan değerlendirme sonucunda, yukarıda sayılan kriterlerde yer alan karar mekanizmalarından çoğuna sahip olan taraf veri sorumlusu olarak kabul edilmektedir. Yukarıda anılan Kurul'un 2020/71 sayılı Kararı[34] uyarınca uygulamada karşılaştığımız veri sorumlusu olarak değerlendirilebilecek dijital platform aktörleri şöyledir;

a. Hizmet Sağlayıcılar: Dijital platformlar, kendi ticari amaçları doğrultusunda kullanıcılara ait verileri topluyor, analiz ediyor ve bu verileri kendi stratejilerini geliştirmek için kullanıyorsa, bu durumda ilgili dijital platformlar böyle faaliyet için veri sorumlusu olarak kabul edilebilecektir. Trendyol gibi bir e-ticaret platformu, müşteri alışveriş tercihlerini analiz ederek ürün önerileri sunuyorsa, bu platform veri sorumlusu olarak değerlendirilmektedir.

[34] Bkz. dn. 33.

b. İçerik Yayınlayıcılar: Sosyal medya platformları, kullanıcıların paylaştığı içerikleri depolayıp yayınlıyorsa ve bu içerikler kişisel veri içeriyorsa, platform bu kişisel verilerin işlenmesinden dolayı veri sorumlusu olarak kabul edilecektir. Dijital platform, kullanıcıların içeriklerini yönetme ve denetleme yetkisine sahip olduğu için veri sorumlusu olarak kabul edilebilecektir. Popüler uygulama olan *Instagram* bu tip dijital platforma bir örnektir.

c. Veri Toplayıcılar: Anket ve araştırma platformları gibi, kullanıcılardan doğrudan kişisel veri toplayan ve bu verileri analiz eden dijital platformlar, veri sorumlusu olarak değerlendirilebilecektir. *SurveyMonkey, Google Forms* gibi platformlar, topladıkları verileri, işleme amaçlarını ve araçlarını belirlemektedirler.

d. Ödeme Hizmeti Sağlayıcıları: Bir e-ticaret sırasında satış işlemleri için uygulamada genelde satıcı ödeme hizmet şirketi ile anlaşmaktadır. Böyle bir durumda ödeme hizmeti sağlayıcı şirket, ödemelerin tam ve eksiksiz yapılmasını sağlamak için müşterilerin hangi kişisel verilerine ihtiyacı olduğuna, bu verilerin hangi amaç çerçevesinde kullanılacağına karar vermektedir. Bu doğrultuda, e-ticaret sitesindeki satıcıdan ayrı ve bağımsız bir şekilde hareket ettiği için veri sorumlusu statüsündedir.[35] *İyzico* bu tip platforma bir örnektir.

Özetle, veri sorumlusu olarak değerlendirilmek, ilgili dijital platformun veri işleme faaliyetlerindeki kontrol düzeyine ve veriler üzerindeki etkisine bağlıdır. Bir dijital platform, kişisel verilerin işlenme amaçlarını ve araçlarını belirliyor ve bu kişisel veriler üzerinde önemli ölçüde bir kontrol sahibi ise, veri sorumlusu olarak kabul edilebileceklerdir.

[35] Kişisel Verileri Koruma Kurumu, Veri Sorumlusu Veri İşleyen, s.7. (https://www.kvkk.gov.tr/SharedFolderServer/CMSFiles/31d9c444-27a5-4a75-95b1-1ca9bdb81ea5.pdf) (E.T.: 16.09.2024).

## 1.5. VERİ SORUMLUSU DİJİTAL PLATFORMLARIN YÜKÜMLÜLÜKLERİ

Dijital platformlar, KVKK kapsamında veri sorumlusu olarak kabul edildiklerinde belirli yükümlülüklere tabi olurlar.

**a. Veri Sorumluları Sicili Bilgi Sistemine ("VERBİS") Kayıt:** KVKK'nın 16. maddesinin ikinci fıkrası uyarınca kişisel veri işleyen gerçek ve tüzel kişilerin veri işleme faaliyetine başlamadan önce, Veri Sorumluları Siciline kaydolma zorunluluğu bulunmaktadır. Bu doğrultuda Veri Sorumluları Sicili Bilgisi Sistemi oluşturulmuş ve sicil hakkındaki usul ve esasların detayları da Veri Sorumluları Sicili Hakkında Yönetmelik ("**VERBİS Yönetmeliği**") ile düzenlenmiştir.[36]

Kurul tarafından belirlenen ve duyurulan bazı kriterler ışığında bu yükümlülüğe işlenen kişisel verilerin niteliği, sayısı, veri işlemenin kanundan kaynaklanması veya aktarım yapılan taraflar gibi somut kriterlere dayanarak istisnalar getirilmiştir.[37] Bu yetki çerçevesinde VERBİS kayıt yükümlülüğüne 19.07.2018 tarihli ve 2018/87 sayılı Kurul kararı ile "yıllık mali bilanço toplamı" tutarı kriter olarak belirlenmiş[38], ilgili kriter Kurul'un 06.07.2023 tarihli ve 2023/1154 sayılı Kararı[39] ile güncellenmiştir. Bu doğrultuda, yıllık elliden az çalışanı olan ve yıllık mali bilanço toplanı yüz milyon Türk lirasından düşük olan veri sorumlularının, eğer ana faaliyet konusu özel nitelikli kişisel veri işleme de değilse, VERBİS'e kaydolma yükümlülüğü bulunmamaktadır.

Türkiye'de yerleşik olmayan yabancı veri sorumluları bakımındansa herhangi bir istisna tanınmamıştır. Kurul'un 23/07/2019 tarihli ve 2019/225 sayılı

[36] RG: 30.12.2017, 30286. Yürürlük Tarihi: 01.01.2018.
[37] Küzeci, s.369.
[38] Veri Sorumluları Siciline Kayıt Yükümlülüğünden İstisna Tutulacak Veri Sorumluları ile ilgili Kişisel Verileri Koruma Kurulunun 19/07/2018 Tarihli ve 2018/87 Sayılı Kararı (https://www.kvkk.gov.tr/Icerik/5271/2018-87) (E.T.: 16.09.2024).
[39] Veri Sorumluları Siciline Kayıt Yükümlülüğüne İlişkin İstisna Kriterinde Değişiklik Yapılması Hakkında Kişisel Verileri Koruma Kurulunun 06/07/2023 Tarihli ve 2023/1154 Sayılı Kararı (https://www.kvkk.gov.tr/Icerik/7647/2023-1154) (E.T.: 16.09.2024).

Kararı'ndan[40] anlaşıldığı üzere KVKK, Türkiye'de doğrudan veya şubeleri aracılığıyla kişisel veri işleme faaliyetinde bulunan yurt dışında yerleşik veri sorumlularına da uygulanmaktadır. Dolayısıyla, küresel yapıdaki birçok yabancı platform, Türk vatandaşı veya Türkiye'de yerleşik kişilere hizmet verirken kişisel veri işlemesi halinde KVKK'nın uygulama alanına girecek olup bu doğrultuda veri işleme faaliyetlerine başlamadan önce VERBİS'e kayıt yükümlülüğünü yerine getirerek KVKK'dan doğan diğer yükümlülüklerini uyması gerekmektedir.

Yurt dışında yerleşik veri sorumluları, VERBİS'e kaydolurken Türk bir veri sorumlusu temsilcisi ataması gerekmektedir. VERBİS Yönetmeliği'nin 4. maddesinin birinci fıkrasının (p) bendi uyarınca veri sorumlusu temsilcisi, bu veri sorumlularını VERBİS Yönetmeliği ile düzenlenen belirli konularda temsile yetkili Türkiye'de yerleşik tüzel kişi ya da T.C. vatandaşı gerçek kişidir.

VERBİS Yönetmeliği madde 11 kapsamında açıklanan yabancı veri sorumlusu temsilcisi temel olarak Kurul ile yurt dışında yerleşik veri sorumlusu arasındaki iletişimi sürdürmekle görevlidir. Yurt dışında yerleşik veri sorumlusunun karar vermeye yetkili bir organı tarafından verilecek atama kararının Kurul'a sunulması ile VERBİS'e kayıt işlemi tamamlanmaktadır. Daha sonrasında temsilci tarafından atanacak irtibat kişisi tarafından ilgili veri sorumlusunun Türkiye'deki kişisel veri işleme faaliyetlerini VERBİS'e kaydetmesi gerekmektedir.

VERBİS Yönetmeliği'nin 13. maddesine göre veri sorumlusu dijital platformların VERBİS'e daha önce bildirilen bilgilerde herhangi bir değişiklik olması halinde bu değişiklikleri, meydana geldiği tarihten itibaren yedi gün içerisinde Kurum'a bildirmelidir, yine bu bildirim irtibat kişisi aracılığıyla yapılabilmektedir.

[40] Yurtdışında yerleşik Tüzel kişilerin Türkiye'deki Şubeleri ile İrtibat Bürolarının Sicile Kayıt Yükümlülüğü Hakkındaki Görüş Talebi ile ilgili Kişisel Verileri Koruma Kurulunun 23/07/2019 tarih ve 2019/225 sayılı Karar Özeti (https://www.kvkk.gov.tr/Icerik/5545/2019-225) (E.T.: 16.09.2024).

VERBİS kaydı, veri sorumlusu dijital platformların veri işleme faaliyetlerini kamuoyu ile paylaşarak ilgili kişilere karşı şeffaflığı sağlamaktadır. VERBİS kayıt yükümlülüğünü ihlal eden veri sorumlularının 2024 yılı için Kurul'un 119.436 TL ile 5.972.040 TL arasında idari para cezası uygulama yetkisi bulunmaktadır.[41]

**b. Aydınlatma Yükümlülüğü:** KVKK'nın 10. maddesi uyarınca, veri sorumluları kişisel verileri işlerken ilgili kişilere kişisel verilerin işleneceği amaçları, aktarılacak tarafları ve amaçlarını, veri toplama yöntemi ve hukuki sebebini açık ve sade bir dil ile bildirmek zorundadır.[42]

**c. Kişisel Verileri Hukuka Uygun İşleme:** Veri sorumlularının kişisel veri işleme faaliyetini yürütebilmesi için KVKK'nın 5. ve 6. maddeleri kapsamında belirtilen hukuki sebeplerinden bir veya birkaçına sahip olması gerekmektedir.[43]

**d. Kişisel Verilerin Güvenliğinin Sağlanması:** KVKK'nın 12. maddesinde, veri sorumları, kişisel verilerin hukuka aykırı olarak işlenmesini, erişilmesini önlemek ve kişisel verilerin muhafazasını sağlamak amacıyla uygun güvenlik düzeyini temin etmeye yönelik gerekli her türlü teknik ve idari tedbirleri almak zorundadır.[44]

**e. İlgili Kişilerin Haklarını Karşılamak:** KVKK'nın 11. maddesi uyarınca ilgili kişiler haklarını kullanmak için veri sorumlusuna başvuruda bulunabilir. Bu takdirde, Veri Sorumlusuna Başvuru Usul ve Esasları Hakkında Tebliğ[45] ("**Veri Sorumlusuna Başvuru Tebliğ**") uyarınca veri sorumlusu ilgili kişinin taleplerini, talebin niteliğine göre en kısa sürede ve en geç otuz gün içinde sonuçlandırmak

[41] 6698 sayılı Kişisel Verilerin Korunması Kanunu'nun 18'inci maddesinde düzenlenen İdari Para Cezalarının 5326 sayılı Kabahatler Kanunu'nun 17'nci maddesinin yedinci fıkrasına göre her takvim yılı başından geçerli olmak üzere o yıl için 213 sayılı Vergi Usul Kanunu'nun mükerrer 298'inci maddesi hükümleri uyarınca 2017-2024 yılları için tespit ve ilan edilen yeniden değerleme oranında arttırılmış tutarlarını gösteren tablo:(https://www.kvkk.gov.tr/SharedFolderServer/CMSFiles/8833aad2-62c2-4a01-b147-fe97062678f3.pdf) (E.T.: 16.09.2024)
[42] Veri sorumluların bu yükümlülüğü 1.4 numaralı bölümde kapsamlı bir şekilde incelenmektedir.
[43] Veri sorumlularının bu yükümlülüğü 1.5 numaralı başlıkta kapsamlı bir şekilde incelenmektedir.
[44] Veri sorumlusu dijital platformların bu yükümlülüğü Bölüm 3 kapsamında incelenmektedir.
[45] RG: 10.03.2018, 30356.

zorundadır.[46]

## 1.6. DİJİTAL PLATFORMLARIN AYDINLATMA YÜKÜMLÜLÜĞÜ

Aydınlatma yükümlülüğünün mevzuat kapsamında öngörüldüğü şekilde ifa edilmesi ile kişisel verilerin korunması hakkının amacına uygun ve etkin bir şekilde kullanılmasına imkân yaratılmaktadır.[47] Kişisel verilerin dijital platformlar tarafından nasıl kullanıldığı genellikle aydınlatma metni veya uygulamada bilinen yaygın ifade ediliş şekli ile gizlilik politikalarında açıklanmaktadır. KVKK'nın 10. maddesi aydınlatma yükümlülüğünü düzenlemektedir, bu yükümlülüğü yerine getirmek üzere dijital platformlar genellikle gizlilik politikalarını kullanıcıların platforma kaydı veya alışveriş sırasında okunmasını ve okunduğunun onaylanmasını sağlayacak şekilde internet sitesinde veya mobil uygulamada konumlandırılmasını sağlamaktadır.

Dijital platformların KVKK uyarınca yerine getirmeleri gereken aydınlatma yükümlülüğü, kullanıcıların kişisel verilerinin işlenmesi konusunda bilgilendirilmesini ve böylece veri sahibi ilgili kişilerin kişisel verilerinin geleceğini belirleme hakkının da sunulmasını sağlanmaktadır.[48] Bunun sonucu olarak da ilgili kişiler nezdinde güven tesis edecek şekilde şeffaflık ve hesap verilebilirlik ilkeleri uygulanabilmektedir.[49]

Aydınlatma Yükümlülüğünün Yerine Getirilmesinde Uyulacak Usul ve Esaslar Hakkında Tebliğ'in[50] ("**AYUET**") 4. maddesinde aydınlatma yükümlülüğü kapsamında ilgili kişiye aktarılması gereken bilgilere yer verilmiştir. Bu kapsamda, dijital platformlar, aydınlatma metnini hazırlarken, öncelikle veri

[46] Veri sorumlusu dijital platformların bu yükümlülüğü 2.5 numaralı bölümde kapsamlı bir şekilde incelenmektedir.
[47] **DÜLGER, Murat Volkan;** Kişisel Verilerin Korunması Hukuku, Hukuk Akademisi Yayınları, İstanbul, 2020 s. 297.
[48] Küzeci, s. 359
[49] Kişisel Verileri Koruma Kurumu, Aydınlatma Yükümlülüğünün Yerine Getirilmesi Rehberi, s.7. (https://www.kvkk.gov.tr/SharedFolderServer/CMSFiles/a569a068-c079-4189-b134-f57bc727af7d.pdf) (E.T.: 16.09.2024).
[50] R.G: 10.03.2018, 30356.

sorumlusunun kimliğini ve yurt dışında yerleşik bir dijital platform ise veri sorumlusu temsilcisini açıkça belirtmelidir. Özellikle şeffaflığı ve hesap verilebilirlik ilkesini uygulamak adına bu oldukça önem arz eden bir noktadır. Zira küresel dijital platformlarda ilgili kişinin kendi kişisel verilerini kimin aldığını, veri sorumlusunu Türkiye'de kimin temsil ettiğini bilmesi, ilgili kişinin haklarını kullanabilmesi açısından önemlidir.[51]

Kişisel veriler işlenirken kişinin kendisi yerine bir başkasından kişisel verilerin elde edilmesi halinde de veri sorumlusunun bu yükümlülüğünü yerine getirmesi gerekmektedir. AYUET'nin 6. maddesi kapsamında bu durumda veri sorumlusu kişisel veriyi elde ederek işlemeye başladıktan sonra makul bir süre içerisinde ilgili kişiyi bilgilendirmelidir. Veri sorumlusu, elde ettiği bu kişisel verileri ilgili kişi ile iletişim kurmak için kullanacak ise ilk iletişim sırasında aydınlatma yükümlülüğünü yerine getirmelidir. Eğer kişisel verilerin aktarımı söz konusu olacak ise en geç aktarılacağı esnada bu yükümlülük yerine getirilmelidir.

GDPR'ın 14. maddesinin üçüncü fıkrasında da benzer şekilde bu konu düzenlemektedir: "*Kişisel verilerin ilgili kişiden temin edilmediği hallerde, veri sorumlusu, kişisel verileri temin ettiği andan itibaren makul süre içinde, kişisel verileri işleme koşullarını da göz önünde bulundurarak, en geç bir ay içinde; ilgili kişi ile iletişim kurulacaksa en geç ilk iletişim anında veya kişisel verilerin aktarımı söz konusu olacaksa en geç ilk aktarım anında ilgili kişi bilgilendirilmelidir."* GDPR ile KVKK arasındaki "makul süre" noktasındaki farklılık GDPR'da netliğe kavuşturulmuştur. Kurul'un genel yaklaşımında KVKK'yı yorumlarken GDPR atıflarına yer veriyor olması sebebiyle kişisel verilerin ilgili kişi yerine bir başkasından temin edildiği durumlarda veri sorumlusunun aydınlatma yükümlülüğünü en geç bir ay içinde yerine getirmesinin faydalı olacağı kanaatindeyim.

Veri sorumlularının aydınlatma yükümlülüğünü yerine getirmesi için mevzuat kapsamında belirlenen bir şekil şartı bulunmamaktadır. AYUET'nin 5.

[51] Küzeci, s.360.

maddesi kapsamında bu yükümlülük sözlü, yazılı, ses kaydı, çağrı merkezi gibi fiziksel veya elektronik ortam kullanılmak suretiyle yerine getirilebilir. Tek şart verilen bilgilerin anlaşılabilir bir şekilde sunulmasıdır, bu kapsamda açık ve sade bir dil kullanılması ve şeffaflığın sağlanması gerekmektedir.[52] Kanaatimce, mevzuat kapsamında belirtilmemişse de açık ve anlaşılabilir olmasını sağlamak adına, aydınlatma metninin kullanıcıların anadilinde ve kolayca anlayabilecekleri şekilde sunulması gerekmektedir.

Aydınlatma metninin kullanıcıların kolaylıkla erişebileceği ve anlayabileceği bir biçimde sunulması, dijital platformların KVKK'nın gerektirdiği şekilde aydınlatma yükümlülüğünü yerine getirebilmesi açısından kritik bir öneme sahiptir. Metnin açık, anlaşılabilir ve erişilebilir olması, kullanıcıların kişisel verilerini nasıl işlendiğini ve bu süreçte hangi haklara sahip olduklarını net bir şekilde anlamalarını sağlamaktadır.[53] Ayrıca veri sorumlusu dijital platformlar veri işleme faaliyetlerine yönelik sunduğu bilgileri düzenli olarak güncel tutmalı, işlediği kişisel verilerin doğru ve güncel olmasını sağlama yükümlülüğünü yerine getirmelidir.[54]

Dijital platformların aydınlatma yükümlülüğünü veri işleme hukuki sebebi fark etmeksizin her durumda yerine getirmesi gerekmektir. AYUET'nin 5. maddesinde açıklandığı üzere kişisel veri işleme faaliyeti KVKK'daki hukuki sebeplerden "açık rıza" şartına dayalı olarak yürütülüyor ise aydınlatma yükümlülüğü kapsamındaki bilgilerin sunulması işlemi ile veri işleme faaliyetine ilişkin ilgili kişinin açık rızasının talep edilmesi işlemleri birbirlerinden ayrı bir şekilde yerine getirilmelidir. Bu doğrultuda dijital platformların, kişisel verilerin işlenmesi için açık rızaya dayanması gerektiğinde, bu açık rızayı almadan önce aydınlatma yükümlülüğünü yerine getirmeleri ve ilgili kişilerin verilen rızanın bilincinde olmalarını sağlamaları gerekmektedir.

---

[52] Küzeci, s.202, Akgül, Kişisel Verileri, s.126.
[53] **AŞIKOĞLU, Şehriban İpek**; Avrupa Birliği ve Türk Hukukunda Kişisel Verilerin Korunması ve Büyük Veri, On İki Levha Yayıncılık, İstanbul, 2018 s.42.
[54] Dülger, s.298.

Aynı hüküm ile ayrıca bu yükümlülüğünün yerine getirmenin ispatının veri sorumlusuna ait olduğu düzenlenmiştir. Böylece, dijital platformlar uygulamada genellikle, öncelikle aydınlatma metnini hazırlayarak herhangi üyelik, satış veya kişisel veri işlemesi gereken işlemden önce okunmasını zorunlu tutarak; "*okudum, anladım"* şeklinde bir ifade ile ispat yükümlülüğünü açıklıkla ifa ettiklerini göstermeye çalışırlar. Bu amaçla eğer onay kutucuğu konulduysa okunduğuna ilişkin onay kutucuğunun işaretlenmesini zorunlu tutulmaktadır ki bu yükümlülüğünün yerine getirildiğine ilişkin ispat edilmiş olsun. Ardından açık rıza alması gereken bir durum varsa ayrı bir onay kutucuğu konumlandırarak açık rıza gerektiren veri işleme faaliyeti için kullanıcının açık rızasının talep edilmesi gerekmektedir.

Bu konuda Kurul'un *Amazon Turkey* hakkında 2020 yılında verdiği kararı oldukça aydınlatıcıdır.[55] Bu karar kapsamında tespit edilen ihlallerden birisi de *Amazon Turkey*'in Gizlilik Bildirimi'nde yer alan "*amazon.com.tr'yi ziyaret ederek işbu Gizlilik Bildiriminde belirtilen uygulamaları kabul etmekte ve onaylamaktasınız*" ifadesi ile ilgili kişilerin kişisel verilerinin işlendiğine ilişkin bilgi verilmiştir. Kurul'un incelemesi neticesinde bu ifade ile aydınlatma yükümlülüğü yerine getirirken eş zamanlı olarak kişilerden açık rıza alındığı izlenimi yaratıldığı belirtilmiştir. Ayrıca, bir veri işleme faaliyetinde bu faaliyete açık rıza dışındaki diğer veri işleme sebeplerinin mevcut olması halinde hala açık rıza talep edilmesinin dürüstlük kuralına aykırı olduğunu ve açık rıza alınması gereken haller için de aydınlatma yükümlülüğü ve açık rıza alınmasının ayrı ayrı yerine getirilmesi gerektiği prensibine aykırı olduğunu tespit etmiştir. Dolayısıyla dijital platformların aydınlatma yükümlülüğünü yerine getirirken hazırlayacağı metinler ile açık rıza gerektiren haller için hazırladığı metinlerin birbirinden ayrı olması gerektiğine hükmetmiştir.

[55] Amazon Turkey Perakende Hizmetleri Limited Şirketi hakkındaki başvuru ile ilgili Kişisel Verileri Koruma Kurulunun 27/02/2020 Tarihli ve 2020/173 Sayılı Karar Özeti: https://www.kvkk.gov.tr/Icerik/6739/2020-173 (E.T.: 16.09.2024) (Bundan sonra "*Amazon Turkey* Kararı" olarak anılacaktır.)

## 1.7. DİJİTAL PLATFORMLARDA KİŞİSEL VERİ İŞLEME İLKE VE ŞARTLARI

### 1.7.1. Kişisel Veri İşleme İlkeleri

Dijital platformlar, kişisel veri işleme faaliyetlerini KVKK'da öngörülen ilkeler çerçevesinde ve şartların varlığı halinde yürütmelidir. KVKK'da veri işleme faaliyetlerinde dikkat edilmesi gereken ilkeler madde 4 uyarınca düzenlenmiştir. Bu doğrultuda bir kişisel veri işleme faaliyeti "*hukuka ve dürüstlük kurallarına uygun olmalı*", "*belirli, açık ve meşru amaçlar kapsamında gerçekleştirilmelidir*, "*işleme amacıyla bağlantılı, sınırlı ve ölçülü olmalı*", "*mevzuatta öngörülen veya amaçla bağlantılı olarak belirlenecek bir süre kadar saklama koşulunu sağlamalı"* ve "*doğru ve gerektiğinde güncel veriler içermeli"*dir.[56]

Bu doğrultuda dijital platformların öncelikle kişisel veri işleme faaliyetlerini hukuka ve dürüstlük kurallarına uygun bir şekilde yürütmesi gerekmektedir. Bu en temel ilke ile *"hukuka uygunluk"* ilkesi kapsamlı bir şekilde değerlendirilmiştir.[57] Dijital platformların veri işleme faaliyetlerini tüm kanunlar ve ikincil düzenlemelerden kaynaklanan ilke ve yükümlülüklere uygun bir şekilde gerçekleştirilmesini gerektirmektedir.[58] Örneğin, söz konusu dijital platformun ana hizmet alanı sigortacılık faaliyeti ise bu mevzuat kapsamında diğer tüm düzenlemelere de uygun bir şekilde ilgili platformu tasarlaması gerekmektedir.

Dürüstlük kuralına uygunluk ise Türk Medeni Kanunu madde 2'de[59] düzenlenen dürüstlük kuralının kişisel veriler işlenirken ihlal edilmemesidir.[60] Bu

---

[56] Çekin, s. 61; Nafiye Yücedağ, Kişisel Verilerin Korunması Kanunu Kapsamında Genel İlkeler, KVKD, 2019, C.1, S.1, s.47-63, s.48.

[57] Beste Ekin, Kişisel Verilerin Korunması ve Rekabet Hukuku Boyutuyla Büyük Veri, İstanbul, On İki Levha, s.55., Küzeci, s.200; Taştan, s.45.

[58] Kişisel Verileri Koruma Kurumu, Kişisel Verilerin İşlenmesine İlişkin Temel İlkeler, s. 2. (https://www.kvkk.gov.tr/SharedFolderServer/CMSFiles/32ff74f6-9798-405a-b3d2-b42d28423fde.pdf) (E.T.: 16.09.2024).

[59] *"Herkes, haklarını kullanırken ve borçlarını yerine getirirken dürüstlük kurallarına uymak zorundadır. Bir hakkın açıkça kötüye kullanılmasını hukuk düzeni korumaz."*

[60] Taştan, s.49; **ÖZDEMİR, Hayrunnisa**, Elektronik Haberleşme Alanında Kişisel Verilerin Özel Hukuk Hükümlerine Göre Korunması, Seçkin Yayıncılık, 2009 s.138; 71-72; **YÜCEDAĞ, Nafiye**, "Kişisel Verilerin Korunması Kanunu Kapsamında Genel İlkeler", Kişisel Verileri Koruma Dergisi,

ilke, her somut olayın özelinde objektif olarak bir kimseden beklenen şekilde davranılması olup tarafların çatışan menfaatlerinin dengelenmesi açısından önemlidir.[61] Bu bağlamda, örneğin dijital platformların aydınlatma metinlerinde belirttiği kişisel veri kategorilerinden farklı bir veri işleme faaliyeti yürüterek kullanıcıların kişisel veri işlemesi halinde dürüstlük kuralı ihlal edilmiş olacaktır.

Diğer bir ilke ise, KVKK madde 4'te yer alan doğruluk ve güncellik ilkesidir. Bu ilke kapsamında dijital platformlar, işledikleri kişisel verilerin doğru ve gerektiğinde güncel olmasını sağlamakla yükümlüdür.[62] Yanlış veya eksik verilerin işlenmesi, kişisel hakların ihlaline neden olabilecektir.[63]

Kurul'un 22/12/2020 tarihli ve 2020/966 sayılı İlke Kararı[64] kapsamında da kişisel verilerin işlenmesinde doğruluk ve güncellik ilkesine uyulmasının gerektiği, veri sorumlularının işlediği kişisel verilerin doğruluğunu ve güncelliğini sağlamak için gerekli önlemleri almakla yükümlü olduğu vurgulanmaktadır.[65] Bu İlke Karar kapsamında dijital platformların kişisel veri toplarken ilgili kişilerin beyan ettiği iletişim bilgilerinin doğruluğunun teyit edilmesi amacıyla doğrulma kodu veya bağlantı gibi yöntemleri kullanması, hatalı veya eksik bilgilerin işlenmesini önlemeleri gerekmektedir. Ayrıca kullanıcıların kendi kişisel verileri üzerinde kontrol sahibi olmalarını sağlayacak araçlar sunarak, kullanıcıların verilerini güncelleyebilmelerine olanak tanıması da bu ilkeye uygunluk noktasında

---

Cilt:1, Sayı:1 s.a.47-63, s.49. Farklı görüş için bkz Çekin, s.64: bu ilkenin Türk Medeni Kanunu'nda anılan dürüstlük ilkesinden farklı olarak veri sorumlularının ilgili kişilere adil davranma yükümlülüğü kapsamında olduğu belirtilmektedir.

[61] Küzeci, s.230; Information Commissioner's Office, Guide to the General Data Protection Regulation, s.23-24; GDPR'ın 58 ve 60 numaralı resitali.

[62] Çekin, s. 71, Yücedağ, Genel İlkeler, s.51

[63] **DEVELİOĞLU, Hüseyin Murat;** 6698 sayılı Kişisel Verilerin Korunması Kanunu ile Karşılaştırmalı Olarak Avrupa Birliği Genel Veri Koruma Tüzüğü Uyarınca Kişisel Verilerin Korunması Hukuku, On İki Levha Yayınları, İstanbul, 2017 s.48; Yücedağ Genel İlkeler, s.50; Küzeci, s.213.

[64] Veri sorumluları tarafından kişilerin telefon numarası, e-posta adresi gibi iletişim kanallarına Kanuna aykırı şekilde gönderilen üçün kişilere ait kişisel veriler hakkında Kişisel Verileri Koruma Kurulu'nun 22/12/2020 tarihli ve 2020/966 sayılı İlke Kararı, (https://www.kvkk.gov.tr/Icerik/6858/2020-966) (E.T.: 16.09.2024).

[65] Veri sorumluları tarafından kişilerin telefon numarası, e-posta adresi gibi iletişim kanallarına Kanuna aykırı şekilde gönderilen üçün kişilere ait kişisel veriler hakkında Kişisel Verileri Koruma Kurulu'nun 22/12/2020 tarihli ve 2020/966 sayılı İlke Kararı, (https://www.kvkk.gov.tr/Icerik/6858/2020-966) (E.T.: 16.09.2024).

önemlidir. Ancak bu kapsamda alınacak önlemlerin kişisel verilerin kullanılması gerektiğinde güncelliğinin sağlanmasına ilişkin olduğu unutulmamalıdır, sürekli bir şekilde güncelliğinin sağlanması makul bir beklenti olmayacaktır.[66]

Kişisel verilerin işlenme amacının belirli, açık ve meşru olması ilkesi kapsamında ise dijital platformların kişisel verileri toplama ve işleme nedenlerini net bir şekilde belirlemelerini ve bu amaçların meşru olmasını gerektirmektedir.[67] Bu ilkenin tüm veri işleme sürecini kapsaması gerekmektedir.[68] Örneğin, bir sosyal medya platformu, kullanıcı deneyimini iyileştirmek veya hizmetlerini kişiselleştirmek amacıyla aydınlatma metninde gerekli bilgileri sunarak kullanıcının belirli kişisel verilerini işleyebilir. Ancak, bu amaç ile ilgisi olmayan, gelecekte ortaya çıkabilecek olası amaçlar[69] doğrultusunda daha fazla kişisel veri işlemesi bu ilkeye ayrılık teşkil edecektir. Örneğin bir e-ticaret platformunun müşterilerine ait telefon numaralarını kaydetmesindeki amacının meşru olduğu değerlendirilebilirken, kan grubu bilgisinin işlenmesi aynı şekilde değerlendirilemez.[70]

Diğer bir ilke olan amaçla bağlantılılık, sınırlılık ve ölçülülük ilkesi ışığında işlenen verilerin belirlenen amaçla gerçekleştirilmesi için yeterli olmasını gerektirmektedir.[71] Örneğin, bir e-ticaret platformunun, sipariş işlemlerini gerçekleştirmek için kullanıcıların adı, soyadı, adresi, telefon numarası gibi iletişim bilgilerine ihtiyacı olabilir, ancak kullanıcıların din, ırk, üye olduğu siyasi parti gibi özel nitelikli kişisel verini toplaması ve işlemesi gereksiz ve ölçüsüz olarak değerlendirilecektir.

KVKK kapsamında yer alan temel ilkelerden biri de kişisel verilerin işlendikleri amaçla sınırlı bir şekilde veya mevzuatta daha uzun bir süre

[66] Küzeci, s.214, Yücedağ, Genel İlkeler, s.51.
[67] Develioğlu, s.45-46; Yücedağ, Genel İlkeler, s.52.
[68] Küzeci, s. 230.
[69] Aynı yönde bkz. Başalp, Kişisel Verilerin Korunması s. 37.
[70] Kişisel Verileri Koruma Kurumu, KVKK Yayınları, Örnekler, s.7.
[71] KVKK, Gerekçe, m.4.

öngörülüyorsa bu süre ile sınırlı bir şekilde muhafaza edilmesidir.[72] Bu doğrultuda dijital platformların işleme amacı sona eren veya mevzuatta bir süre belirlenmişse bu saklama süresinin dolması halinde, kişisel verileri silmesi, yok etmesi veya anonim hale getirmesi gerekmektedir. Bu ilke doğrultusunda dijital platformların işleme amacı ve yasal gerekliliklerine göre kişisel verilerin saklama sürelerini belirlediği açık ve anlaşılır saklama ve imha politikası geliştirmelidir.

### 1.7.2. Dijital Platformlarda Kişisel Veri İşleme Şartları

Kişisel veri işleme faaliyetinin mevzuat çerçevesinde yürütülebilmesi için KVKK'da sayılan şartlardan en az birinin bulunması gerekmektedir. Kişisel veri işleme şartları kişisel verinin özel nitelikli ve genel nitelikli olmasına göre değişmektedir.[73]

#### 1.7.2.1. Dijital Platformlarda Genel Nitelikli Kişisel Verilerin İşlenmesi

Kişisel veri işlemek için temel şart ilgili kişinin açık rızasını sunmasıdır.[74] Aşağıda açıklanan diğer veri işleme şartları ise istisna olarak düzenlenmiştir.[75]

Açık rıza kavramı ilgili kişilerin belirli bir konuda edindiği bilgi neticesinde kendi hür iradesi ile verdiği rıza olarak açıklanmaktadır. KVKK'nın gerekçesinde bu kavram için ilgili kişinin kendisi hakkında yürütülecek veri işleme faaliyetine yeterli bilgi sahibi olduktan sonra hür bir şekilde sunduğu olumlu beyan olarak açıklanmıştır.[76] Özgürce verilme unsuru bu rızanın dijital platformların uygulamasında *opt-in,* diğer bir deyişle önceden işaretli bir şekilde sunulmamasını da gerektirmektedir.

Kurul'un *Amazon Turkey* Kararı'nda iletişim verilerinin pazarlama amacıyla kullanılabilmesi için pazarlama iletileri gönderilmeden önce veya en geç elektronik ileti gönderilmesine ilişkin onayın alınması esnasında işlenmesi halinde

[72] Yücedağ, Genel İlkeler, s.60.
[73] Aşıkoğlu, s.117
[74] Aşıkoğlu, s.119.
[75] Yücedağ, Medeni Hukuk Açısından, s.773.
[76] KVKK, 3 ve 5. Madde Gerekçeleri

KVKK'nın 5. maddesinde anılan kişisel veri işleme şartlarından sayılan açık rızanın bulunması gerektiği değerlendirilmiştir. Bu doğrultuda, bir ticari nitelikli elektronik ileti gönderilecek ise bunun ilgili e-ticaret mevzuatına uygun olması gerekmektedir. Ancak, bu süreçte aynı zamanda kişisel veriler de kullanıldığından kişisel verilerin korunmasına ilişkin düzenlemelere de uygun olmalıdır.

Bu karar kapsamında açık rıza beyanlarında *opt-out* ve *opt-in* ayrımına gidilmiştir. *Opt-out* şeklinde açık rıza beyanında ilgili kişilerden önceden onay alınmaz, ilgili kişinin otomatik bir şekilde onay verdikleri kabul edilir ve ilgili kişilere onayı kaldırmalarına yönelik imkân tanıyan sistemdir. Karar kapsamında *opt-out* şeklinde beyanın değil, *opt-in* şeklindeki bireyin özgür iradesini de ortaya koyacak şekilde aktif bir eylem ile kişisel verilerin işlenmesine rıza gösterebileceği sistemin mevcudiyetinin gerekliliği netleşmiştir. Dolayısıyla dijital platformların ilgili kişilerin aktif irade beyanını içerecek şekilde *opt-in* rıza sistemini benimsemesi gerekmektedir.

Ayrıca, bir veri sorumlusunun kişisel verileri açık rıza dışında aşağıda belirtilen başka şartlara dayandırarak işleyebiliyorken açık rızaya dayandırmaya çalışması "*aldatıcı ve hakkın kötüye kullanımı"* niteliğindedir.[77] Bu doğrultuda dijital platformların açık rıza gereken halleri hassasiyetle belirlemesi gerekmektedir.

KVKK'nın 5. maddesinin ikinci fıkrasında sayılan işleme şartlarından en az birinin varlığı halinde ise ilgili kişinin açık rıza olmadan kişisel veri işleme faaliyeti mevzuata uygun bir şekilde yürütülebilecektir. Sayılan uygunluk şartları şöyledir;

i. Kanunlarda açıkça yer alıyorsa; örneğin bir e-ticaret platformunun, vergi mevzuatına uygun olarak müşterilerinin fatura bilgilerini saklaması,

[77] Küzeci, s.342.

ii. Fiili imkânsızlık halinde kendisinin veya başkasının hayati tehlikesi varsa; örneğin acil durum hizmetleri sunan bir platformun, kullanıcının rızasını alamayacak durumda olması halinde, hayatını kurtarmak amacıyla kullanması,

iii. Sözleşmenin kurulması veya ifası kapsamında; örneğin bir çevrimiçi alışveriş platformunun, sipariş teslimi için gerekli olan müşterinin adres ve iletişim bilgilerini işlemesi,

iv. Hukuki yükümlülüklerin ifası için mutlaka gerekliyse; örneğin, e-ticaret platformu, e-fatura hizmeti sunabilmek için müşterilerinin adı, soyadı, vergi / T.C. kimlik numarası, adres bilgilerini işlemesi,

v. İlgili kişinin kendisinin kişisel verisini alenileştirmiş olması halinde; örneğin iş ilişkisi kurma ve iş arama hizmetleri sunan bir platformda (örneğin, Kariyer.net) kullanıcılar, kendi profillerinde eğitim bilgilerini, iş deneyimlerini, becerilerini ve diğer özlük bilgilerini paylaşarak aleni hale getirilmesi. Önemle belirtmek gerekir ki ilgili kişinin alenileştirdiği kişisel verilerini bilinçli bir şekilde ve rızasıyla kamuyla paylaşmış olmalıdır[78],

vi. Bir hakkın tesisi, kullanılması veya korunması için mutlaka gerekliyse; örneğin bir sigorta platformu, kullanıcının sigorta poliçesi kapsamındaki haklarını tesis etmek ve korumak için verilerini işleyebilmektedir. Bu kapsamda söz konusu dijital platform hasarın boyutunu belirleyerek, tazminat hesaplayarak kullanıcının hak ettiği tazminatı sağlamak için kullanıcının kişisel verilerini kullanabilmektedir.

vii. Veri sorumlusunun meşru menfaati için zorunlu olması halinde; örneğin, bir video paylaşım platformu, içerik önerilerini iyileştirmek

[78] Yücedağ, Medeni Hukuk Açısından, s.779.

için kullanıcıların izleme geçmişini işleyebilmektedir. Ancak bu durumda ilgili kişinin temel hak ve özgürlüklerinin korunması gerektiği için denge testi[79] yapılması gerekmektedir.

KVKK'da denge testinin yürütülmesi açık ve zorunlu bir şekilde belirtilmemiş olsa da Kurul'un 2019/78 sayılı Kararı'nda standartları belirtilmiştir. Bu standartlar, veri işlemenin gerekli ve orantılı olmasını, meşru menfaatin halihazırda mevcut, belirli ve açık olmasını, alternatif yöntemlerin değerlendirilmesini, şeffaf ve hesap verilebilir nitelikte olması ve veri güvenliği için gerekli teknik ve idari tedbirlerin alınmasını vurgulamaktadır.[80]

Örnek uygulama olarak bir video paylaşım platformunu değerlendirdiğimizde, video paylaşım platformunun, kullanıcı deneyimini iyileştirmek ve içerik önerilerini kişiselleştirmek için kullanıcıların izleme geçmişini işleyebilmektedir. Bu durumda, söz konusu platformun meşru menfaati, kullanıcı deneyimini iyileştirmek ve platformun kullanımını artırmak olarak değerlendirilebilecektir.

- Birinci adım; meşru menfaatlerin belirlenmesi: İlgili platform, kullanıcı deneyimini iyileştirmek ve içerik önerilerini kişiselleştirmek amacıyla kullanıcıların izleme geçmişini işlemek istemektedir. Bu veri işleme faaliyeti, ilgili platformun kullanımını ve kullanıcı memnuniyetini artırabilecektir.

- İkinci adım; hak ve özgürlüklerin değerlendirilmesi: Kullanıcıların özel hayatın gizliliği hakkının ve kişisel verilerin korunması hakkının korunması gerekmektedir. İzleme geçmişinin işlenmesi, kullanıcının özel

[79] Kişisel veri işleme şartının veri sorumlusunun meşru menfaatine dayandığı hallerde mutlaka denge testinin yürütülmesi gerekmektedir. Denge testi, veri sorumlusunun meşru menfaatlerinin, ilgili kişinin temel hak ve özgürlüklerine potansiyel olarak verebileceği zarar ile dengelenip dengelenmediğini değerlendirmek için kullanılan bir yöntemdir. Bu test, veri işlemenin meşru menfaatler temelinde yapılabilmesi için şartların getirilip getirilmediğinin belirlenmesini sağlar.
[80] Kişisel Verileri Koruma Kurulu. (2019) Karar No:2019/78 Erişim adresi: https://www.kvkk.gov.tr/Icerik/5434/2019-78 (E.T.: 16.09.2024).

hayatının gizliliğine müdahale olarak değerlendirilebilecektir.

- Üçüncü adım; denge kurulması: İlgili platform, kullanıcıların izleme geçmişini işlemenin, kullanıcı deneyimini iyileştirmek amacıyla gerekli ve orantılı olup olmadığını değerlendirmelidir. Eğer veri işleme, kullanıcıların gizlilik haklarına orantısız bir şekilde müdahale ediyorsa, bu veri işleme faaliyeti yürütülmemelidir. Ayrıca, kullanıcı deneyimini iyileştirmek için izleme geçmişini işlemek yerine daha az müdahaleci alternatif yöntemlerin olup olmadığı incelenmelidir. Örneğin, kullanıcıların izleme tercihlerini açıkça belirmelerine olanak tanıyan bir sistem kullanılabilecektir.

- Dördüncü adım; aydınlatma yükümlülüğü: İlgili platform kullanıcıları veri işleme faaliyetleri hakkında şeffaflığı sağlamak adına açık ve net bir şekilde bilgilendirilmelidir. Kullanıcılar, veri işlemenin amacı, işlenen veri türleri ve veri işlemenin nasıl gerçekleştirileceği konusunda net bilgi sahibi olmalıdır.

KVKK uyarınca henüz denge testinin hesap verilebilirliği sağlaması adına her zaman yapılması yükümlülük olarak düzenlenmemiş olsa da GDPR uygulamalarına ve Kurul kararlarına baktığımızda kişisel veri işleme faaliyetlerinin veri sorumlusunun meşru menfaati hukuki sebebine dayandırıldığında denge testinin yürütülüp yürütülmediği incelenmektedir.

Kurul incelediği kararlarda doğrudan denge testi yapmamıştır. Çünkü denge testi veri sorumlusunun kendisi tarafından yürütülmesi gerekmektedir. Bu konuda Kurul tarafından denge testinin nasıl yürütülebileceğine yönelik standartların belirlenmesi veri sorumlularına daha yol gösterici nitelikte olacaktır.[81]

Bu kapsamda, her ne kadar kesin standartlar olmasa da eğer dijital platformların bir kişisel veriyi meşru menfaat hukuki sebebine dayanarak işlemesi

[81] (Yayınlanmayan Tez) **SEPİCİ GÜLEŞGEN**, Şive, Kişisel Verilerin Korunması Hukuku Açısından Meşru Menfaat Kavramının Değerlendirilmesi, İstanbul Bilgi Üniversitesi, Lisansüstü Programları Enstitüsü Bilişim ve Teknoloji Hukuku Yüksek Lisans Programı, İstanbul, 2021, s.73.

halinde denge testini anılan Kurul kararındaki standartlar ışığında yürütmesi ve kayıtlarında denge testi raporlarını muhafaza etmeleri önemlidir.

#### 1.7.2.2. Dijital Platformlarda Özel Nitelikli Kişisel Verilerin İşlenmesi

Özel nitelikli kişisel veriler, ilgili kişilerin en fazla mahremiyet ihtiyacı duyduğu kişisel bilgilerini içerdiği için bu verilerin işlenmesi ve muhafazası sıkı kurallara tabidir.

KVKK, özel nitelikli kişisel verilerin işlenmesini temelde yasaklamaktadır. Ancak belirli istisnai durumların mevcut olması halinde bu verilerin işlenmesine izin vermektedir. KVKK yürürlüğe girdiğinde madde 6 çok daha sınırlı uygulama alanına sahip bir hükümdü ve neredeyse özel nitelik veri işleme faaliyetini açık rıza şartına hapsederek ciddi aksaklıklara neden olmuştu.[82]

Maddenin eski halinde özel nitelikli kişisel verilerin işlenmesi için temel kural ilgili kişinin açık rızasının varlığıydı. Bununla birlikte bazı istisnalar da tanınmıştı, bu kapsamda sağlık ve cinsel hayat dışındaki özel nitelikli kişisel verilerin, kanunlarda öngörülen hallerde ilgili kişinin açık rızası aranmaksızın işlenebileceğini, sağlık ve cinsel hayata ilişkin özel nitelikli kişisel verilerin ise ancak kamu sağlığının korunması, koruyucu hekimlik, tıbbi 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 ilgili kişinin açık rızası aranmaksızın işlenebileceğini düzenlemekteydi. Madde bu haliyle uygulamada zorluklar yaratmakta, açık rıza yoğunluğuna neden olmaktaydı.

Örneğin, Kurul'un 2020/667 sayılı Kararı kapsamında Kurul'a gönderilen bir şikâyet incelenmiştir.[83] İlgili kişi şikâyeti kapsamında ailesi adına düzenlettiği

[82] Kaya, Mehmet Bedii (2024) KVKK Reformu: 2024 Değişiklikler, (Dijital Baskı v.1.0), s.8. https://mbkaya.com/hukuk/kvkk-reformu.pdf E.T.: 16.09.2024).
[83] Bir sigorta şirketinin ilgili kişiye vereceği hizmeti açık rıza şartına bağlaması sebebiyle Kuruma iletilen şikâyet hakkında Kişisel Verileri Koruma Kurulunun 03/09/2020 tarihli ve 2020/667 sayılı Karar Özeti, https://www.kvkk.gov.tr/Icerik/6878/2020-667 (E.T.: 16.09.2024).

sağlık sigorta poliçesini yenilemek istediğinde, sigorta şirketinin kendisinden poliçeyi yenilemek için açık rıza talep ettiğini ileri sürmüştür. Şikayetçi, bu durumun KVKK'ya aykırı olduğunu iddia ederek şikâyette bulunmuştur. Kurul, yaptığı incelemede KVKK'nın 6. maddesi uyarınca özel nitelikli kişisel verilerin işlenmesinin kural olarak yasak olduğunu, dolayısıyla bu verilerin işlenmesi için ilgili kişinin açık rızasının alınması gerektiğini belirtmiştir. Sağlık sigorta poliçesi özel nitelikli kişisel veri niteliğinde sağlık verilerini içerdiğinden bir sigorta şirketi tarafından bu verilerin işlenmesi ancak ilgili kişiden açık rıza alınmasıyla mümkün olduğu değerlendirilmiştir. Sonuç olarak Kurul, veri sorumlusu sigorta şirketinin, poliçeyi yenilerken sağlık verilerini işlemek için ilgili kişiden açık rıza talep etmesinin KVKK'ya aykırılık olmadığına hükmetmiştir.

İlgili karar kapsamında değerlendirildiğinde, bir hizmetin sunulabilmesinin sağlık verilerinin sunulması için açık rıza verilmesi koşuluna bağlandığı değerlendirilecektir. Dolayısıyla, kanaatimce açık rızanın "özgür irade" unsurunun böyle bir olayda uygulanabilir olduğundan bahsedilemeyecektir.

Sigorta hizmeti sunan platformlar gibi birçok platformun işleyişini kısıtlayan hükmün yeni hali 12 Mart 2024 tarihinde Resmî Gazete yayımlanmış[84] ve daha özgür bir yapıya ulaşmıştır.

KVKK'nın 6. maddesinde yapılan yeni düzenleme ile özel nitelikli kişisel verilerin tanımı aynı şekilde kalmış ancak veri işleme şartlarında önemli ölçüde esneklik sağlanmıştır. Yeni düzenleme ile özel nitelikli kişisel verilerin işlenmesine ilişkin maddenin sistematiği değiştirilerek tamamen yasaklanmış ve açık rızanın varlığı diğer veri işleme şartları ile değerlendirilmiştir. [85]

Bu doğrultuda, ilgili kişinin açık rızasının olması halinde özel nitelikli kişisel verileri işlenebilmektedir. Bu durum, dijital platformların madde devamında sayılan tahdidi hallerin olmaması halinde, özel nitelikli kişisel verilerini işlemeden

[84] 12 Mart 2024 tarih ve 32487 sarılı Resmî Gazete yayımlanan 7499 sayılı Ceza Muhakemesi Kanunu ile Bazı Kanunlarda Değişiklik Yapılmasına Dair Kanun ile değişiklik yapılmıştır.
[85] Kaya, s.13.

önce bilgilendirmeye dayalı, özgür irade ile verilen, belirli bir konuya yönelik açık rızalarını almasını gerektirmektedir.

Dijital platformlar, eğer tahdidi olarak sayılan diğer özel nitelikli kişisel veri işleme şartı varsa ilgili kişinin açık rızası olmaksızın veri işleme faaliyetini yürütebileceklerdir:

i. Kanunlarda açıkça yer alıyorsa; maddenin yeni haliyle kanunlarda öngörülmesi şartına "açıkça" ibaresi eklenerek sağlık ve cinsel hayat dışındaki kişisel verilere ilişkin herhangi bir kısıt kalmamıştır.[86] Böylece örneğin, Kişisel Sağlık Verileri Hakkında Yönetmeliğin[87] 4. maddesinin birinci fıkrasının (d) bendinde "*ilgili kişilerin sağlık verilerine kendilerinin, hekimlerin veya yetki verdikleri üçüncü kişilerin erişimini sağlayan, e-Devlet uygulamasına uygun olarak Bakanlık tarafında kurulan sistem*" olarak tanımlanan e-Nabız platformunun özel nitelikli kişisel veri işleme faaliyeti kanunlarda açıkça öngörülme şartını sağlamaktadır.

ii. Fiili imkânsızlık halinde kendisinin veya başkasının hayati tehlikesi varsa; sağlık durumu takibi ve acil durum bildirimi sunan bir dijital platformun, ilgili kişinin yaşadığı ani bir sağlık sorunu ve bilinç kaybını tespit etmesiyle birlikte ambulansı veya acil durum kişisini arayarak bilgi paylaşması bir örnektir.

iii. İlgili kişinin kendisinin kişisel verisini alenileştirmiş olması halinde; madde kapsamında ayrıca alenileştirme amacıyla kullanılması gerektiğinin de altı çizilmiştir. Bu kapsamda bir ilgili kişinin, örneğin iş arama platformunda üye olduğu sendikayı belirtmesi halinde ilgili platform da bu doğrultuda işçinin profilini oluşturabilecektir.

[86] Kaya, s.13.
[87] RG: 21.06.2019, 30808.

iv. Bir hakkın tesisi, kullanılması veya korunması için mutlaka gerekliyse; örneğin bir doktor randevu hizmeti sunan platformun hastanın randevusunu oluşturabilmek amacıyla hangi şikayetinin olduğuna ilişkin özel nitelikli kişisel verileri işleyebilecektir.

v. Sır saklama yükümlülüğü altında bulunan kişiler veya yetkili kurum ve kuruluşlarca kamu sağlığının korunması, koruyucu hekimlik, tıbbi teşhis, tedavi ve bakım hizmetlerinin yürütülmesi ile sağlık hizmetlerinin planlanması, yönetimi ve finansmanı amacıyla gerekli olması halinde; veri işleme şartı maddenin ilk halinde de var olan bir şarttır.

Dijital platformlar bakımından örnek olarak Covid-19 salgını sırasında "Evde Kal Kampanyası" kapsamında kullanılan "Hayat Eve Sığar" uygulaması salgının takibi ve kontrolü için geliştirilmiş bir mobil uygulamaydı. Bu uygulama ile vatandaşların sağlık verileri işlenerek salgının yayılması, Covid-19 test sonuçları ve olası temasları bu veri işleme şartı kapsamında takip edilmekteydi.

vi. İstihdam, iş sağlığı ve güvenliği, iş ve sosyal güvenlik veya sosyal hizmetler ile sosyal yardım alanındaki hukuki yükümlülükler kapsamında gerekli olması hali; uygulamada en çok karşılaşılan sorunlardan biri olarak bu veri işleme şartı madde gerekçesinde de açıklandığı üzere 4857 sayılı İş Kanunu[88] çerçevesinde işverenlerin çalışanlarına karşı hukuki yükümlülüklerini yerine getirilmesi sırasında değerlendirilebilecektir.

vii. Siyasi, felsefi, dini veya sendikal amaçlarla kurulan vakıf, dernek ve diğer kâr amacı gütmeyen kuruluş ya da oluşumların, tabi oldukları mevzuata ve amaçlarına uygun olmak, faaliyet alanlarıyla sınırlı olmak ve üçüncü kişilere açıklamamak kaydıyla; mevcut

[88] RG: 10.06.2003, 25134.

veya eski üyelerine ve mensuplarına veyahut bu kuruluş ve oluşumlarla düzenli olarak temasta olan kişilere yönelik olması; veri işleme şartı için örneğin bir dijital sosyal yardım platformunun bir dini vakıf veya dernek ile ortaklık kurarak, üyelerin dini inançlarına veya sosyal yardım ihtiyaçlarına ilişkin bilgileri işleyebilecektir.

Yeni düzenleme, dijital platformların özel nitelikli kişisel verileri işleme biçimlerini ve kullanıcıların bu veriler üzerindeki kontrolünü önemli ölçüde etkilemektedir. Özellikle konusu özel nitelikli kişisel verilerin işlenmesi olan dijital platformlar, kullanıcıların yukarıdaki hukuki sebeplerin varlığında veri güvenliğini sağlayarak operasyonlarını sürdürmeleri kolaylaşacaktır.

# İKİNCİ BÖLÜM
# DİJİTAL PLATFORMLARDA KİŞİSEL VERİLERİN İŞLENMESİ BAKIMINDAN ÖZEL KONULAR

## 2.1. YURT DIŞINA VERİ AKTARIMI

Küreselleşmenin ve bilişim çağının bir getirisi olarak, dijital platformlar günümüzde hayatımızın ayrılmaz bir parçası haline gelmiştir. Bu platformlar, kullanıcıların gerek yurt içi gerek yurt dışı boyutta bilgi alışverişinde bulunduğu, iletişim kurduğu ve hizmetlerinden faydalandığı önemli araçlardır. Söz konusu platformlar, küresel yapıları veya sundukları hizmetin küresel niteliği sebebiyle sıklıkla yurt dışına veri aktarabilmektedir. Gerek yurt içinde olsun gerek yurt dışında olsun kişisel veri aktarımı da bir kişisel veri işleme faaliyetidir.[89]

İlgili kişilerin kişisel verilerinin mahremiyetine ve veri güvenliğine ilişkin yurt dışına veri aktarımının hukuki boyutları önemli bir noktadır. Türkiye gibi birçok ülke, bu konuda çeşitli düzenlemeler yaparak kişisel verilerin uluslararası aktarımı sırasında korunması konusunda adımlar atmıştır. Ancak, uluslararası boyutta veri aktarımı, KVKK'nın yürürlüğe girdiği ilk günden itibaren sorunlara neden olmuştur.

Bu bölümde, dijital platformların yurt dışına veri aktarımı KVKK çerçevesinde incelenmekte ve dijital platformlar bakımından kişisel veri güvenliğini sağlamak için etkili politika ve düzenlemelerin geliştirilmesine yönelik öneriler sunulmaktadır.

[89] Küzeci, s.354.

## 2.2. GEÇMİŞTEN GÜNÜMÜZE YURT DIŞINA VERİ AKTARIM KURALLARI

### 2.2.1. 12 Mart 2024 Değişikliği Öncesi Yurt Dışına Veri Aktarım Kuralları

KVKK, 2016 yılında yürürlüğe girdiği zamandan sonra ilk defa 12 Mart 2024 tarihinde değiştirilmiştir.[90] Bu değişiklik kapsamında temel olarak özel nitelikli kişisel verilerin işlenmesi ve yurt dışına veri aktarım konularında daha özgürlükçü bir sistematik getirilmiştir.

KVKK'nın mülga halinde kural olarak ilgili kişinin aktarıma ilişkin açık rızası olmaksızın yurt dışına kişisel veri aktarımı yasaklanmıştı.[91] Bir sonraki uygunluk koşulu olan yeterlilik kararına baktığımızda ise Kurul'un yeterlilik kararında dikkate alınacak hususlara ilişkin bir karar yayınlamış[92] olmasına rağmen bugüne kadar ne Türkiye tarafından verilmiş ne de bir başka ülkenin Türkiye hakkında verdiği bir yeterlilik kararı bulunmaktadır.[93]

Böylece bir dijital platformun yurt dışına veri aktarımı için elinde iki seçenek kalmaktaydı; açık rıza ve taahhütname uygulaması. Taahhütname uygulaması ise Türkiye'deki ve verinin aktarılacağı yabancı ülkedeki veri sorumlularının kişisel verilerin güvenliği için yeterli bir korumayı yazılı olarak taahhüt etmelerini ve bu taahhütnameye Kurul'un izninin bulunmasını gerektirmektedir. Bu tez tarihi

[90] 12 Mart 2024 tarih ve 32487 sarılı Resmî Gazete yayımlanan 7499 sayılı Ceza Muhakemesi Kanunu ile Bazı Kanunlarda Değişiklik Yapılmasına Dair Kanun ile değişiklik yapılmıştır.
[91] KVKK, m.9/1.
[92] "Yeterli korumanın bulunduğu ülkelerin tayininde kullanılmak üzere oluşturulan form" hakkındaki Kişisel Verileri Koruma Kurulu'nun 02/05/2019 tarihli ve 2019/125 sayılı Karar Özet: (https://www.kvkk.gov.tr/Icerik/5469/-Yeterli-korumanin-bulundugu-ulkelerin-tayininde-kullanilmak-uzere-olusturulan-form-hakkindaki-02-05-2019-tarihli-ve-2019-125-sayili-Kurul-Karari) (E.T.: 16.09.2024).
[93] Avrupa Komisyonu, Türkiye'nin veri koruma yeterliliğini reddetmiş ve Türkiye'nin veri koruma yasalarının AB'nin GDPR standartlarıyla yeterince uyumlu olmadığını belirtmiştir. Bu karar, Türkiye ile AB arasındaki veri transferlerini zorlaştırmıştır. Türkiye'nin, uluslararası standartlarla uyum sağlamak için ek reformlar yapması ve geçici olarak Veri Koruma Anlaşmaları veya Standart Sözleşme Hükümleri gibi mekanizmaları kullanması önerilmiştir. https://marpatas.com/en/european-commission-rejects-turkeys-data-protection-adequacy-impacts-and-future/ (E.T.: 16.09.2024).

itibariyle dokuz tane taahhütname başvurusu onaylanmıştır. [94]

Süreç içerisinde dijital platformları temelden etkileyecek bazı kararlar Kurul tarafından internet sitesinde yayımlanmıştır. Bunlardan birisi ise yurt dışı tabanlı server kullanımının yurt dışına veri aktarımı olarak kabul edildiğine ilişkin karardır.[95]

Bu karar kapsamında, kurumsal olarak kullanılan e-posta adreslerinin Google (*gmail*) üzerinden kullanılmasının uygun olup olmadığına ilişkin bir veri sorumlusu tarafından bilgi talebinde bulunulmuştur. Yapılan incelemeler sonucunda Kurul tarafından, *g-mail* e-posta hizmeti alt yapısının kullanılması halinde e-postaların dünyanın çeşitli yerlerinde bulunan veri merkezlerinde tutulacağından bu faaliyetin kişisel verilerin yurt dışına aktarımı olarak değerlendirileceğini ve bu kapsamda KVKK'nın 9. maddesine uygun davranılması gerektiğini belirtmiştir. Ayrıca "*server*"ları yurt dışında bulunan veri sorumlularından/veri işleyenlerden temin edilen saklama hizmetlerinin de benzer şekilde değerlendirdiğini anılan karar ile vurgulamıştır.

Bu karar ile yurt dışına veri aktarımının aktif bir şekilde görüldüğü dijital platformların küresel yapısını sürdürmesini oldukça zora sokmuştur. Bu

---

[94] TEB Arval: https://www.kvkk.gov.tr/Icerik/6867/TAAHHUTNAME-BASVURUSU-HAKKINDA-DUYURU, (E.T.: 16.09.2024).
Amazon Turkey: https://www.kvkk.gov.tr/Icerik/6898/TAAHHUTNAME-BASVURUSU-HAKKINDA-DUYURU, (E.T.:16.09.2024).
Decathlon Türkiye: https://www.kvkk.gov.tr/Icerik/6985/TAAHHUTNAME-BASVURUSU-HAKKINDA-DUYURU; (E.T.: 16.09.2024).
Türkiye Futbol Federasyonu: https://www.kvkk.gov.tr/Icerik/7161/Taahhutname-Basvurusu-Hakkinda-Duyuru (E.T.: 16.09.2024).
Otokoç: https://www.kvkk.gov.tr/Icerik/7546/-Taahhutname-Basvurusu-Hakkinda-Duyuru; (E.T.: 16.09.2024).
Google: https://www.kvkk.gov.tr/Icerik/7700/Taahhutname-Basvurusu-Hakkinda-Duyuru (E.T.: 16.09.2024).
Celltrion: https://www.kvkk.gov.tr/Icerik/7814/Taahhutname-Basvurusu-Hakkinda-Duyuru (E.T.: 16.09.2024).
Bosh Termoteknik: https://www.kvkk.gov.tr/Icerik/7899/Taahhutname-Basvurusu-Hakkinda-Duyuru (E.T.: 16.09.2024).
Huawei: https://www.kvkk.gov.tr/Icerik/7915/Taahhutname-Basvurusu-Hakkinda-Duyuru (E.T.: 12.09.2024).

[95] Kurumsal e-posta hizmetinin, Google (gmail) üzerinden yine aynı uzantıya sahip olarak kullanılıp kullanılamayacağı ilişkin Kişisel Verileri Koruma Kurulu'nun 31/05/2019 Tarihli ve 2019/157 Sayılı Karar Özeti https://www.kvkk.gov.tr/Icerik/5493/2019-157(E.T.: 16.09.2024).

doğrultuda ilgili kişinin açık rızasının alınması veya taahhütname başvurusunun onaylanmasına dayanan yurt dışına aktarımın uygulamada tıkandığı değerlendirilmiştir.[96]

Hem bu tıkanıklığa bir dijital platformun faaliyetlerinden örnek olması adına hem de Kurul'un dijital platformlara olan yaklaşımını anlamak adına *Amazon Turkey* Kararı oldukça önemlidir.

*Amazon Turkey* Kararında, Kurum bir ihbar dilekçesinden hareketle re'sen inceleme başlatmıştır. Karar kapsamında ihbarın elektronik ticari elektronik iletilere yönelik öncelik Ticaret Bakanlığı'na yapıldığı, Bakanlık tarafından Kurum'a iletildiği anlaşılmaktadır. İhbarın iki temel konusu vardır, usulüne uygun bir rıza almaksızın ticari elektronik ileti gönderimi ile "http://amazon.com.tr" adresinde yer alan "Gizlilik Bildirimi" isimli metindeki kişisel verilerin AB'ye ve AB'den Amerika Birleşik Devletleri'ne aktarılabileceğine ilişkin ifadedir.

İlgili karar kapsamından anlaşıldığı üzere Kurul ihbara ilişkin başlattığı inceleme sırasında *Amazon Turkey* tarafından yurt dışına veri aktarımının yürütülmesi için taahhütname metinlerini hazırlamış ve Kurul'un onayına sunmuştur. Ancak Kurul tarafından henüz başvuru neticelendirilmediğinden ayrıca yeterli korumayı sağlayan ülkelerinde belirlenmemiş olduğundan yurt dışına veri aktarımının hukuka uygun bir şekilde yürütülmesi için tek yöntemin ilgili kişinin açık rızasının alınması olduğu belirtilmiştir. Bu karar mevzuatın uygulanmasına ilişkin taahhütname ve açık rıza uygulaması arasında yaşanan tıkanıklığın somut bir halidir.

Karara konu süreçte *Amazon Turkey* ilgili kişi tarafından "Gizlilik Bildirimi"nin kabul edilmesi ile Gizlilik Bildirimi metninde yer alan hususların da kabul edildiğini ileri sürmüştür. Bu noktada, Kurul belirli konu ile sınırlandırılmayan, genel ifadeler içeren açık rızaların "battaniye rıza" olarak kabul edildiğini belirtmiştir. Battaniye rızalar hukuken geçersiz olduğundan herhangi bir

[96] Kaya, s.26.

veri işleme şartı olmaksızın kişisel veri işleme faaliyeti yürütüldüğü değerlendirilmiştir.

Anılan gizlilik bildirimine verilen onay "veri işleme" faaliyeti kapsamına giren çerezler vasıtasıyla izleme, verileri aktarma, paylaşma, depolama gibi tek bir rıza ile birden çok konuya ilişkin olacak şekilde tasarlanmıştır. Bu yapının hukuka uygun olmadığına, kişisel verilerin yurt dışına aktarılmasına yönelik ilgili kişinin geçerli açık rızasının bulunması gerektiğine kanaat getirilmiştir.

Yapılan incelemeler neticesinde Kurul, halihazırda yeterli korumayı sağlayan ülkelerin henüz belirlenmediği, veri sorumlusu *Amazon Turkey*'in sunduğu taahhütnamenin de henüz Kurum tarafından onaylanmadığı vurgulanmıştır. Bu doğrultuda yurt dışına veri aktarımı için ilgili kişilerin açık rızasının varlığının gerektiği, ancak somut olayda usulüne uygun bir açık rıza da alınmadığından hareketle *Amazon Turkey* hakkında idari para cezası uygulamıştır.

### 2.2.2. 12 Mart 2024 Değişikliği Sonrası Yurt Dışına Veri Aktarım Kuralları

12 Mart 2024 tarihinde yapılan değişiklik ile yurt dışına veri aktarımı kurallarına yönelik GDPR'a benzer şekilde daha fazla esneklik ve tüm veri sorumluları bakımından uygulanabilir bir sistem geliştirilmiştir. Bu da tabii ki küresel yapıdaki dijital platformların faaliyetlerini de oldukça kolaylaştırmıştır. Bu düzenlemeler 1 Eylül 2024 tarihinde yürürlüğe girmiştir.

KVKK'nın yapısı temel olarak sorumluluğun "veri sorumlusuna" ait olduğu yönündedir. Ancak, değişiklikler kapsamındaki yurt dışına veri aktarımını düzenleyen 9. maddenin yeni halinde sorumluluk veri sorumlusunun yanı sıra veri işleyen de dahil edilmiştir. Bu konu hakkında böylece hukuki güvenlik sağlanmıştır.[97] Uygulamada yurt dışı tabanlı bulut sistemlerinin de, veri işleyen sıfatını taşısalar dahi, bu aktarım sırasında mevzuata uyumdan sorumlu olmaları gerekecektir.

[97] Kaya, s.31.

Söz konusu mevzuata uyum için aşamalı ve seçenekli bir aktarım sistemi oluşturulmuştur. Kişisel verilerin yurt dışına aktarımı için (i) yeterlilik kararına dayalı aktarım, (ii) uygun güvencelere dayalı aktarım ve (iii) arızi durumlara dayalı aktarım olmak üzere üç farklı alternatif getirilmiştir.[98]

#### 2.2.2.1. Yeterlilik Kararına Dayalı Aktarım

Maddenin mülga halinde temel kural olan açık rıza yerini yeterlilik kararına bırakmıştır. Bu kapsamda eğer ki veri işleme şartlarını düzenleyen KVKK'nın 5. ve 6. maddelerine uygunluk var ise ve aktarımın yapılacağı ülke, uluslararası kuruluş veya ülke içerisindeki sektörler hakkında kişisel verilerin güvenliğine ilişkin yeterlilik kararı var ise, veri sorumlusu veya veri işleyen kişisel verileri yurt dışına aktarabilecektir.

Eski halinde sadece ülkelere yeterlilik kararı tanınabilirken artık bir ülkenin tamamına olmasa da uluslararası kuruluşlara, bölge içerisindeki belli bir sektöre ayrıca yeterlilik tanınabileceği düzenlenmiştir. Dolayısıyla, mevzuat değişikliğinin temeli olan ticareti sekteye uğratan sorunların bertaraf edilmesi kapsamında önemli bir adım atılmıştır. Bu doğrultuda, örneğin bir ülkenin tamamı için yeterlilik kararı verilmese de e-ticaretin aktif bir şekilde yürütülüyor olması sebebiyle o ülke içerisindeki e-ticaret sektörüne yeterlilik kararı tanınabilecektir. Bu kapsamda bir karar verilmesi halinde ise dijital platformlar bakımından da uygulama kolaylaşacaktır.

#### 2.2.2.2. Güvencelere dayalı aktarım

Değişiklik kapsamında ilk koşul için gerekli olan yeterlilik kararı yoksa belirli güvencelerin mevcut olması gerektiği düzenlenmektedir. Güvencelere dayalı aktarım kapsamında üç ön koşul aranmaktadır:[99]

1- KVKK kapsamında belirtilen kişisel veri işleme şartlarından birinin mutlaka

[98] Kaya, s.30
[99] Kaya, s.36

mevcut olması gerekmektedir;

2- İlgili kişi haklarının aktarım yapılacak ülkede de kullanılabilmesinin mümkün olması gerekmektedir; ve

3- Kişisel verilerin aktarılacağı ülkede kişisel verilerin korunmasına dair etkin ve aktif kanun yollarına başvuru imkânı olmalıdır.

Bu üç ön koşulun sağlanıp sağlanmadığının anlaşılabilmesi için veri sorumlusu veya veri işleyen olacak şekilde veriyi aktaran tarafın kişisel veri aktaracağı ülkeye veya uluslararası kuruluş veya sektör kapsamında aktarım yapılacaksa bunlara ilişkin bilgi sahibi olmaları gerekmektedir.[100] Bunun tespiti için de adeta AB mevzuatına Avrupa Birliği Adalet Divanı'nın ("**ABAD**") Schrems II kararı ile giren "uluslararası kişisel veri transfer etki analizi" (*transfer impact assessment*) yapılması gerekecektir.

**a) Bağlayıcı Şirket Kuralları**

Bağlayıcı şirket kuralları yöntemi her ne kadar mülga KVKK döneminde uygulamada var olsa da KVKK bünyesinde yer almamaktaydı. Kurul'un 10 Nisan 2020 yılında yaptığı Bağlayıcı Şirket Kuralları Hakkında Duyuru[101] ile taahhütname sunma yönteminin bir çeşidi olarak mevzuata kazandırılmıştır. İlgili duyuru kapsamında Taahhütname sunma yönteminin, iki taraflı veri aktarımları bakımından kolay olsa da birden fazla ülkede bulunan grup şirketleri arasındaki gerçekleşen kişisel veri aktarımları bakımından yetersiz kaldığı kabul edilmiştir. Bu sebeple, Kurul tarafından bu tip şirketler bünyesinde gerçekleştirilecek yurt dışı veri aktarımları için kullanılacak yöntem olarak "Bağlayıcı Şirket Kuralları" (*binding corporate rules)* belirlenmiş ve bu yöntem ancak veri sorumlularının

[100] Kaya, s.37.
[101] Kişisel Verileri Koruma Kurulu'nun Bağlayıcı Şirket Kuralları Hakkında Duyurusu: (https://www.kvkk.gov.tr/Icerik/6728/YURT-DISINA-KISISEL-VERI-AKTARIMINDA-BAGLAYICI-SIRKET-KURALLARI-HAKKINDA-DUYURU) (E.T.: 16.09.2024).

kullanabileceği bir yöntem olarak düzenlemişti.[102]

Küreselleşmenin getirisi olarak uluslararası veri koruma standartlarına da ihtiyaç duyulmaktadır. Bağlayıcı Şirket Kuralları uygulaması ile küresel yapıdaki şirketlerin tamamında, verilerinin hangi ülkede işlendiği fark etmeksizin tüm ülkelerde aynı niteliklerin benimsenmesi gerekmektedir. Böylece küresel düzeyde belirlenecek olası veri koruma standartlarında AB mevzuatında yer alan *Binding Corporate Rules* uygulamasına benzer birçok ülkede etkili olan taahhütler uygulama alanı bulacaktır. Böylece AB standartlarına yakın veri koruma standartları için bu yöntemin uygulanması önemlidir. [103]

Bu aktarım yöntemi ile ortak ekonomik faaliyet yürüten bir teşebbüs grubundaki veri sorumluları veya veri işleyenlerin uymak zorunda olduğu kişisel veri güvenliğine ilişkin düzenlemeler belirlenmekte ve Kurul tarafından bu hükümleri içeren bağlayıcı şirket kurallarına onay alınmaktadır [104]

**b) Standart Sözleşme Yöntemi**

Güvencelere dayalı yurt dışına aktarım yapılabileceği üçüncü durum standart sözleşmelerin kullanılmasıdır. AB mevzuatında yer alan Avrupa Komisyonu tarafından yayımlanan "*standard contractual clauses"* sistemine benzer bir yapı oluşturulmuştur. Bu yöntemde, bağlayıcı şirket kurallarından farklı olarak ayrıca Kurul'un onayının alınması gerekmemektedir.

Daha önce mevzuatımızda yer almayan yeni bir araç olan standart sözleşmelerin içeriği ve temel unsurları bu değişiklik ile somutlaşmıştır. Standart sözleşme ile iki taraf arasında sözleşmesel ilişki kurularak kişisel verilerin korunması sağlanmaktadır. Dolayısıyla sözleşme hukukuyla kişisel verilerin korunması hukukunun kesiştiği özel bir araçtır.[105]

---

[102] TOPARLAK, Rüya Tuna Veri Koruması Hukukunda Bağlayıcı Şirket Kuralları: 2016/679 Sayılı Genel Veri Koruma Tüzüğü ve 6698 Sayılı Kişisel Verilerin Korunması Kanunu Karşılaştırması, On İki Levha Yayıncılık, Baskı 1, 2021, s.116.
[103] Toparlak, s.119.
[104] Kaya, s.39.
[105] Kaya, s.40.

Değişik madde aynı zamanda yapılan standart sözleşmelerin imzalanmasından itibaren 5 iş günü içerisinde Kurul'a bildirimini öngörmektedir. Ancak, AB mevzuatında kullanılan standart sözleşmelerin herhangi bir otoriteye bildirilmesine gerek yoktur.[106] Kurul'a bildirim yükümlülüğünün yerine getirilmemesi halinde 50.000 TL'den 1.000.0000 Türk lirasında kadar idari para cezası öngörülmüştür.

Bu noktada, dijital platformların standart sözleşme yöntemini seçtiği takdirde imzadan itibaren başlayan 5 iş günü içinde bildirim yükümlülüğünün yerine getirilmesi önemli bir iş yükü olabileceği kanaatindeyim.

Bu kapsamda çok uluslu şirketleri barındıran dijital platformların, yeterlilik kararı bulunmayan hallerde, veri işleme şartlarının yer aldığı KVKK'da veri işleme şartlarından birinin mevcut olduğu hallerde, aktarımın yapılacağı ülkede ilgili kişinin kişisel verilerine ilişkin haklarını kullanabilmesi ve etkin ve aktif bir şekilde kanun yollarına başvurabilecek olması şartıyla, ilk hal olan bağlayıcı şirket kurallarını benimsemesi, sürekli ancak belirli bir şirkete aktarım söz konusu ise, örneğin bulut hizmet sağlayıcısına yapılan kişisel veri aktarımı gibi, standart sözleşme yönteminin benimsenmesi gerekmektedir.

### c) Taahhütname Sunma Yöntemi

Taahhütname sunmaya ilişkin yöntem değişik KVKK kapsamında da aynı şekilde muhafaza edilmiştir. Bu doğrultuda Türkiye'de yerleşik veri sorumlusu olan bir dijital platformun kişisel verileri, veri güvenliğine yönelik yeterli olarak tanınmayan ülkelerdeki veri sorumlusu veya veri işleyene aktarabilmesi için aktarıma taraf olacakların kişisel verilerin güvenliğini sağlayacağını yazılı olarak taahhüt etmesini sağlamaktadır. İlgili taahhütname metinlerinin asgari unsurları Kurul tarafından ilan edilmiş olup[107], veri sorumlularınca buna uygun sunulan

[106] Kaya, s.41.
[107] Kişisel Verileri Koruma Kurulu, Yurtdışına Veri Aktarımında Veri Sorumlularınca Hazırlanacak Taahhütnamede Yer Alacak Asgari Unsurlar: (https://www.kvkk.gov.tr/Icerik/4236/Yurtdisina-Veri-Aktariminda-Veri-Sorumlularinca-Hazirlanacak-Taahhutnamede-Yer-Alacak-Asgari-Unsurlar) (E.T.: 16.09.202.4)

taahhütname metinlerinin Kurul tarafından da onaylanması gerekmektedir.

#### 2.2.2.3. Arızi Aktarım Yöntemleri

Arızi aktarım yöntemleri; öncelikle aktarım yapılacak ülke, uluslararası kuruluş veya sektör için yeterlilik kararının bulunmadığı hallerde, güvencelere dayalı aktarım da yapılamıyorsa istisnai olarak uygulanabilecektir.[108] Arızi aktarımdan anlaşılması gereken düzenli ve sistematik veri aktarımının gerçekleştirilmemesidir.

Arızi aktarım tek veya birkaç sefer yani süreklilik içermeyen aktarımlarda başvurulabilecek bir yöntemdir.[109] Dolayısıyla dijital platformların bu arızi aktarım yöntemlerinden birine dayanacak olması halinde her somut olay özelinde araştırması gerekir. Bu bölümde bu arızi aktarımlara ve dijital platformların hangi hallerde bu yöntemlerden yararlanabileceği değerlendirilecektir.

**a) Açık Rızaya Dayalı Yurt Dışına Veri Aktarımı**

Açık rıza daha önce neredeyse temel bir hukuki sebep iken yeni düzenleme ile istisnai bir yurt dışına veri aktarım yöntemi haline gelmiştir. Yeni düzenlemede ayrıca açık rızaya dayalı yapılacak yurt dışına veri aktarım halinde muhtemel riskler hakkında ilgili kişinin bilgilendirilmesi gerektiği eklenmiş, böylece veri sorumlusu ile veri işleyen arasındaki bilgi asimetrisinin azaltılması hedeflenmiştir.[110]

Arızi bir yöntem olduğu için dijital platform daha önce olduğu gibi sürekli aktarım gerektiren, örneğin üyelik süreçleri sırasında dijital platformun yurt dışındaki bir ayağıyla paylaşım yapılması, hallerde açık rızaya dayanılamayacaktır. Bir dijital platformun açık rıza arızi yöntemine dayanabileceği bir örnek olarak düzenlenecek tek seferlik çevrimiçi

[108] Kaya, s.44.
[109] GDPR madde 49'da düzenlenen "Özel Durumlara Yönelik Derogasyonlar" (*Derogations for specific situations)* başlıklı maddesinde arızi durumlar tekrar etmeyen anlamına gelen "*if the transfer is not repetitive*" ifadesi kullanılmaktadır.
[110] Kaya, s.46.

konferans verilebilir. Yurt dışı tabanlı teknik bir alt yapı kullanılarak yapılacak bu konferansta katılımcı ve konuşmacılara ait kişisel veriler tek seferlik bir işlem olarak yeterli koruma kararı verilmemiş üçüncü bir ülkeye aktarılacaktır. Güvencelere dayalı aktarımı da içerebilecek bir aktarım mevcut olmadığından bu tek seferlik aktarım için katılımcı ve konuşmacıların açık rızalarına dayanılabilecektir.

Bir başka örnek olarak bir e-ticaret platformunun, Türkiye'deki faaliyetlerinde müşteri memnuniyetini ve hizmet kalitesini artırmak üzere belirli bir anket çalışması yürütmek isteyebilir. Türkiye dışında yer alan bir anket ve geri bildirim platformundan hizmet alınması halinde müşteri e-posta adreslerinin ve anket sonuçlarının bu belirli anket süresi boyunca kullanılmak üzere yurt dışına aktarılacağı bir senaryoda e-ticaret platformunun bu anket çalışması için müşterilerine bilgi vermesi ve yurt dışında hizmet sağlayıcıya kişisel verilerinin aktarılacağını bildirerek açık rızalarını talep etmesi gerekecektir.

**b) Yurt Dışına Aktarımın Bir Sözleşmenin İfası veya İlgili Kişinin Talebi Üzerine Alınan Sözleşme Öncesi Tedbirlerin Uygulanması Kapsamında Gerçekleşmesi**

Bu yönteme dayanılabilmesi için aktarımın hem tekrar etmeyen şekilde arızi olması aynı zamanda da zorunlu olması gerekmektedir.[111]

Örneğin, bir öğrencinin, yurt dışındaki eğitim süresi için sağlık sigortası yapmak üzere Türkiye'de bir sigorta platformundan en uygun poliçeyi talep ettiğinde Türkiye'deki sigorta platformu öğrenciye en uygun poliçeyi sunabilmek için ilgili ülkedeki sigorta şirketi ile çalışması gerekecektir. İlgili kişinin talebi üzerine yurt dışındaki sigorta şirketine teklif alınması amacıyla kişisel verilerin aktarılması bu hukuki sebep kapsamında değerlendirilecektir.

[111] Kaya, s.48.

**c) Yurt Dışına Aktarımın Bir Sözleşmenin Kurulması veya İfası İçin Zorunlu Olması Durumunda Gerçekleşmesi:**

Bu halde yapılacak aktarımda ilgili kişinin sözleşmenin tarafı olmaması gerekmektedir. Örneğin; e-ticaret platformu, dünya genelinde hizmet vermekte ve ilgili kişi müşterinin başka bir ülkedeki siparişini kendisine ulaştırmak ister. Bu kapsamda siparişi istediği ve yeterli korumanın bulunmadığı ülkeden ürünün kargo firması aracılığı ile taşınması gerekecektir. Bu takdirde siparişi veren ilgili kişinin kimlik ve adres bilgisi, ürünün satın alındığı satıcı ile ve kargo şirketi ile paylaşılması halinde bu yönteme dayanılabilecektir.

**d) Yurt Dışına Aktarımın Üstün Bir Kamu Yararı İçin Zorunlu Olduğu Halde Gerçekleşmesi:**

Bu yöntem kapsamında uluslararası düzeyde kurulmuş bir yardım platformu örnek verilebilir. Kamu yararına yapılacak bir kişisel veri aktarımı halinde, örneğin bir salgın hastalığın uluslararası tehdit oluşturması halinde Türkiye salgının etkilerini azaltmak ve küresel sağlık güvenliğini sağlamak amacıyla, hastalığın yayılımını izlemek ve etkili tedavi yöntemleri geliştirmek için Dünya Sağlık Örgütü ile iş birliği yapabilir. Bu kapsamda Türkiye'deki sağlık teşebbüsleri, hastalıkla ilgili kişisel verileri (örneğin, vaka sayıları, hasta listeleri, hastaların sağlık durumları) Dünya Sağlık Örgütü'ne bu kapsamda aktarabilecektir.

**e) Yurt Dışına Aktarımın Bir Hakkın Tesisi, Kullanılması veya Korunması İçin Zorunlu Olması Halinde Gerçekleşmesi:**

Bu yöntemde hakkın sözleşmeden mi yoksa kanundan mı doğduğu önemli değildir.[112] Önemli olan hukuken somut hakka dayanak oluşturacak hukuki bir temelin bulunmasıdır.

**f) Yurt Dışına Veri Aktarımın Fiili İmkânsızlık Hallerinde Gerçekleşmesi:**

Yurt dışına veri aktarım için bu istisnai halde; fiili imkânsızlık nedeniyle

[112] Kaya, s.49.

rızasını açıklayamayacak veya rızasına hukuki geçerlilik tanınamayan bir kişinin mevcut olması ve bu kişinin kendisinin ya da bir başkasının hayatı veya beden bütünlüğünün korunması için gerekli olmalıdır.[113]

**g) Yurt Dışına Aktarımın Aktarımda Meşru Menfaati Olan Kişinin Talebi Üzerine Gerçekleşmesi:**

Bu istisnai yöntemde aktarılacak kişisel verinin tamamen kamuya açık olan veya meşru menfaati bulunan kişilere açık olan bir sicilde bulunması gerekmektedir. Meşru menfaati olan kişi talep ederse yurt dışına veri aktarımı yapılabilecektir. Talep ilgili kişi tarafından yapılmalıdır. [114]

## 2.3. DİJİTAL PLATFORMLARDA ÇEREZLER İLE KİŞİSEL VERİ İŞLEME FAALİYETLERİ

### 2.3.1. Çerez Nedir?

Çerez, internet sitelerinin ziyaret edilmesi sırasında toplanan ve Üstün Metin Transfer Protokolü (*Hyper Text Transfer Protocol – HTTP)* kapsamında iletilen metin parçasıdır. Çerezler, bir internet tarayıcısı (Google Chrome, Internet Explorer gibi) aracılığıyla elde edilen çeşitli bilgi parçalarıdır.[115]

Çerezlerin temel amacı, bir internet sitesinin kullanıcın cihazını tanıması ve kullanıcının tercihleri veya geçmişteki eylemleri hakkında bilgileri saklamasıdır.[116] Bu sayede, internet siteleri kullanıcının sonraki ziyaretlerinde kişisel tercihlerini anımsayarak kişiye özel ve kullanıcı dostu bir deneyimi sunabilmektedir.

Çerezler sürelerine ve kullanım amaçlarına göre belirli kriterlere göre sınıflandırılmaktadır. Oturum çerezleri (*session cookies*) geçici olup, genellikle

[113] Kaya, s.50.
[114] Kaya, s.50.
[115] Castelluccia, C. ve Narayanan, A. (2012). Privacy considerations of online behavioural tracking. The European Network and Information Security Agency (ENISA), s.6.
[116] Jules, A. Jakobsson, M., & Jagatic, T. N. (2006). Cache cookies for browser authentication. 2006 IEEE *Symposium* on Security and Privacy (S&P'06). Doi: 10.1109/SP.2006.8, s.1.

kullanıcı oturum açtığında çalışır ve oturum kapatıldığında silinir. Kullanıcı tercihlerini ve internet sitesindeki gezintilerini saklamak için kullanılmaktadırlar. Kalıcı çerezler (*persistent cookies)* kullanıcıların kimlik bilgilerini, kimlik doğrulama araçlarını saklamak için kullanılan kalıcı çerezlerdir. Tarayıcıda, kullanıcı tarafından silinene veya süresi dolana kadar karlılar. Üçüncü taraf çerezleri ise (*third-party cookies)* başka bir alan adı tarafından ayarlanan bileşenler (görüntüler, bağlantılar, bulgular, vb.) tarafından oluşturulabilir. Reklam şirketleri gibi bazı siteler, bu çerezleri kullanıcıları birden fazla site üzerinden izlemek için kullanmaktadırlar.[117]

Kurum'un Haziran 2022'de yayımladığı "Çerez Uygulamaları Hakkında Rehber"[118] kullanım amaçlarına göre aşağıdaki şekilde sınıflandırmıştır[119]:

i. Kesinlikle gerekli (zorunlu) çerezler: internet sitesinin düzgün çalışması için gereklidir.

ii. İşlevsel Çerezler: internet sitesinin kişiselleştirilmesi veya kullanıcıların tercihlerinin hatırlanması için gereklidir.

iii. Performans-Analitik Çerezler: internet sitesinin kullanıcılarının ziyareti sırasındaki davranışlarını analiz edebilmek ve istatistiki ölçüm yapabilmek için gereklidir.

iv. Reklam ve Pazarlama Çerezleri: internet ortamında kullanıcıların çevrimiçi hareketlerine dayalı olarak kişisel ilgi alanları belirlenip bu ilgi alanlarına yönelik reklamlar gösterilmektedir.

Çerezlerin mahremiyet açısından endişe yaratıp yaratmayacağı kullanım amaçlarına ve uygulamalara bağlı olarak değişmektedir. Hukuka uygun iyi niyetli kullanımlarda önemli işlevlere sahip olan çerezler, kötü niyetli kullanılması

[117] Castelluccia ve Narayanan, s.6.
[118] Kişisel Verileri Koruma Kurumu, Çerez Uygulamaları Hakkında Rehber: (https://www.kvkk.gov.tr/SharedFolderServer/CMSFiles/fb193dbb-b159-4221-8a7b-3addc083d33f.pdf) (E.T.: 16.09.2024).
[119] Kurum, Çerez Uygulamaları Hakkında Rehber, s.8.

halinde önemli mahremiyet riskleri taşıyabilmektedir.

Çerezler, tek başına kişisel veri olmamakla birlikte, çerezler içinde kişisel veriler yer alabilmektedir. Çerezler aracılığıyla işlenen veriler, kullanıcı tarafından seçilen örneğin dil ayarı gibi doğrudan kişiyi tanımlayamayacak nitelikte olabileceği gibi isim ve soy isimden oluşan bir kullanıcı adı, e-posta adres gibi kişiyi doğrudan tanımlayan nitelikte de olabilecektir.[120]

Çerez Uygulamaları Hakkında Rehber kapsamında çerezler yoluyla kişisel veri işleyen internet sitesi işleticileri için önerilerde bulunmaktadır. Rehber, çerezlerin hangi kişisel veri işleme şartına dayanılarak kullanılabileceğini ele almakta ve çerezler vasıtasıyla kişisel verilerin işlenmesi için KVKK'da öngörülen hukuki sebeplerin bulunması gerekmektedir. [121]

Çerezlerin kullanımı ile ilgili olarak, öncelikle temel yükümlülük olarak aydınlatma yükümlülüğünü yerine getirmesi gerekmektedir. Ayrıca, kullanıcıların çerezlerin kullanımı için açık rıza verdiği hallerde kişisel verilerinin kullanımı üzerinde yönetimi sağlayabilmesi adına çerez panelinin mevcut olması gerekmektedir. Böyle bir panel, kullanıcıların çerez tercihlerini özgür iradeleriyle yönetebilmelerine imkân sunmaktadır. [122]

### 2.3.2. Dijital Platformlarda Çerez Kullanımı

Çerezler kullanımı, dijital platformlarda kişisel verilerin kullanımı açısından önemli bir rol oynamaktadır. İlk olarak 1994 yılında kullanılmaya başlanan çerezler, zamanla mahremiyet konusunda endişelere yol açmıştır.[123]

Dijital platformlarda, çerez kullanımı etkileri hem olumsuz (örneğin, ilgili kişinin açık rızasını almadan kişiyi takip etme veya bir zafiyet tespit ederek ilgili

[120] Çekin, s.188.
[121] Kurum, Çerez Uygulamaları Hakkında Rehber, s.7.
[122] Kurum, Çerez Uygulamaları Hakkında Rehber, s.30.
[123] Cahn, A., Alfred, S., Barford, P., & Muthukrishnan, S. (2016). An Empirical Study of Web Cookies. In *25th International Conference on World Wide Web (WWW'16).* Republic and Canton of Geneva, CHE: International World Wide Web Conferences Steering Committee. https://doi.org/10.1145/2872427.2882991 s. 891-901 (E.T.: 16.09.2024).

kişinin cihazına saldırmak) hem de olumlu (örneğin, kullanıcı ara yüzünü ilgili kişiye göre kişiselleştirmek, web sitesi performansının iyileştirilmesi veya çevrimiçi hizmetlerin güvenliğinin güçlendirilmesi) olabilmektedir. Bu nedenle, dijital platformlarda kişisel verilerin kullanılmasında mevzuata uyum oldukça önem arz etmektedir.

Bu konu Kurul tarafından da birkaç kararında incelenmiştir. Kurul'un 23.12.2022 tarihli ve 2022/1358 numaralı Karar[124] kapsamında e-ticaret sektöründe faaliyet gösteren bir şirketin internet sitesi ve mobil uygulamalarında çerezler aracılığıyla kişisel veri işlemesiyle ilgili şikâyet üzerine Kurul, ilgili e-ticaret sitesini incelemiştir. Karar kapsamında Kurul yaptığı inceleme sonucunda internet sitelerinin olması gerektiği şekilde çalışması için mutlaka bulunması gereken "kesinlikle gerekli çerezler" için ilgili kişilerin açık rızasının varlığına gerek olmadığını belirtmiş, "reklam, pazarlama ve performans amacıyla çalışan çerezlerin" kullanılması için ilgili kişilerin açık rızasının mevcut olması gerektiğini vurgulamıştır. Veri sorumlusu e-ticaret firmasının kesinlikle gerekli olmayan çerezler kullanması ancak usulüne uygun "*opt-in*" açık rıza mekanizmasının bulunmaması, çerezlere özgülenmiş bir çerez politikasının olmaması, yurt dışına veri aktarım yaptığını tespit ederek 800.000 TL tutarında idari para cezası uygulamıştır.

Dünyadan örneklere baktığımızda Fransız Veri Koruma Otoritesi'nin ("***CNIL**") Google LLC* ve *Google Ireland Limited'e* 31 Aralık 2021 tarihinde uyguladığı 150 milyon Euro tutarındaki idari para cezası, dijital platformlarda çerez kullanımına yönelik önemli bir emsal teşkil etmektedir.[125] Buradaki temel mahremiyet endişesi ise Google'ın web sitelerinde (google.fr ve youtube.com)

[124] Bir internet sitesinde yer alan çerezlere ilişkin aydınlatma ve açık rıza metinlerinin sunulmaması" hakkında Kişisel Verileri Koruma Kurulunun 23/12/2022 tarihli ve 2022/1358 sayılı Karar Özeti: https://www.kvkk.gov.tr/Icerik/7595/2022-1358 (E.T.: 16.09.2024).

[125] CNIL, Deliberation of the restricted committee No. SAN-2021-023 of 31 December 2021 concerning GOOGLE LLC and GOOGLE IRELAND LIMITED, https://www.cnil.fr/sites/cnil/files/atoms/files/deliberation_of_the_restricted_committee_no._san-2021-023_of_31_december_2021_concerning_google_llc_and_google_ireland_limited.pdf (E.T.: 16.09.2024).

çerezlerin kabul edilmesinin reddedilmesinden çok daha kolay hale getirmiş olması olarak belirlenmiştir. Kullanıcıların çerezleri reddetmesi, kabul etmesine kıyasla daha fazla tıklama gerektirmesi sebebiyle kullanıcıların özgür iradesini zedelediği vurgulanmıştır. CNIL'in 13 Temmuz 2023 tarihindeki kararına göre Google kendisine uyum için verilen üç aylık süre içerisinde çerezleri reddetme işlemini kabul etme işlemi kadar kolaylaştırdığını duyurmuştur.[126] Böylece, Google ilgili web sitelerinde "yalnızca gerekli çerezlere izin ver" butonunu kabul butonlarının yanında göstermeye başlamıştır.

ABAD'ın *Planet49* hakkında kullanıcıların dijital platformlarda çerez kullanımına rıza göstermesi konusunda önemli bir ilke karar vermiştir.[127] Anılan kararda *Planet49*, çevrimiçi yarışma düzenleyen bir şirkettir ve yarışmaya katılmak isteyen kullanıcıların cihazlarına çerez yerleştirilmesine dair bir onay kutusu sunmuştur. Ancak bu onay kutusu önceden işaretli bir şekilde *opt-out* olarak kullanıcıya sunulmuştur. Federal Alman Tüketici Birliği (*Bundesverband der Verbraucherzentralen und Verbraucherverbände — Verbraucherzentrale Bundesverband e.V.*) bu uygulamanın etkin bir şekilde kullanıcıların rıza vermesine imkân tanımadığından veri mahremiyeti haklarını ihlal ettiği gerekçesiyle mahkemeye başvurmuştur. Yapılan incelemeler neticesinde kullanıcı rızasının sadece aktif bir eylem ile, yani kullanıcı tarafından onay kutusunun işaretlenmesi şeklinde verilmesi halinde geçerli olacağı, önceden işaretlenmiş onay kutuları geçerli bir rıza olarak kabul edilmediğini belirtmiştir.

## 2.4. DİJİTAL PLATFORMLARIN PAZARLAMA FAALİYETLERİ

Günümüzde dijital platformlar sundukları hizmetler için genelde ayrıca ücret almadan kendilerini kullanıcının karşısına çıkardıkları reklamlar ile finanse

[126] CNIL, Closure of the injunction issued against GOOGLE, https://www.cnil.fr/en/closure-injunction-issued-against-google (E.T.: 16.09.2024).

[127] Verbraucherzentrale Bundesverband eV v. Planet49 GmbH (C-673/17) https://curia.europa.eu/juris/document/document.jsf;jsessionid=0A3A5F81BE1A7718127D2689B3033679?text=&docid=218462&pageIndex=0&doclang=en&mode=lst&dir=&occ=first&part=1&cid=590749 (E.T.: 16.09.2024).

etmektedirler.[128] Dijital platformların hedef kitlesi kullanıcıları olduğu gibi, hedef kitlesini oluşturulan verileri elde ettiği kaynağı da yine kullanıcılarıdır. Bu nedenle bu kullanıcılar üreten tüketiciler *(producer consumer – procumer)* olarak nitelendirilmektedir.[129]

Dijital platformların kullanımı sırasında kullanıcının yaşı, cinsiyeti, hangi reklamla ilgilendiği, kullanıcının IP adresi, ilgili dijital platformdaki alışveriş geçmişi gibi kişisel verilerin işlenmesi sayesinde kullanıcıya ait davranışsal profilleri oluşturulmaktadır.[130] Bu davranışsal profiller kullanılarak, kullanıcının karşısına tercihlerine yönelik o kullanıcıya özel kişileştirilmiş reklamlar çıkarılabilmektedir.[131]

Teknolojinin gelişmesi ile davranışsal profilleme faaliyetlerinin artması, kullanıcıların kişisel veri işleme faaliyetlerinin hız kazanması kullanıcılar bünyesinde mahremiyet endişesi yaratmıştır. Böylece kişisel verilerin korunmasına ilişkin kuralların uygulanmasına daha çok özen gösterilmeye başlanmıştır.[132]

Kişisel verilerin korunmasına ilişkin kuralların uygulanması için dijital platformlarda pazarlama amacıyla kişisel veri işleme faaliyeti yürütürken veri sorumlusu olarak KVKK'nın 4. maddesinde yer alan genel ilkelere uyması gerekmektedir.[133] Ayrıca, veri sorumlusunun bu veri işleme faaliyeti için veri işleme şartlarından birine dayanması gerekmektedir. Öğretide "*sözleşmenin kurulması veya ifası için gereklilik*", "*veri sorumlusunun meşru menfaatlerinin korunması için gerekli olması*" veya "*açık rıza*" şartlarından hangisine

[128] ÇOLAK, Betül / TEVETOĞLU, Mete, "Dijital Reklamcılığın Yol Açtığı Hukuki Sorunlar ve Çözüm Önerileri", Maltepe Üniversitesi Hukuk Fakültesi Dergisi, 2021, S. 1, s. 43-86, s. 68
[129] Cambridge Dictionary, 2021, https://dictionary.cambridge.org/dictionary/english/prosumer (E.T.: 16.09.2024).
[130] Salih Polater, 'Kişisel Verilerin Reklam Amaçlı İşlenmesinde Hukuka Uygunluk Sebepleri', Kişisel Verileri Koruma Dergisi, Sayı: 1, Yıl: 2019, https://dergipark.org.tr/tr/download/articlefile/741785 (E.T.: 16.09.2024), s. 2.
[131] Tiffany Barnett White / Debra Zahay / Helge Thorbjørnsen / Sharon Shavitt, 'Getting Too Personal: Reactance to Highly Personalized Email Solicitations', Marketing Letters, Sayı: 19(1), Yıl: 2008, https://www.researchgate.net/publication/5153026 (E.T.: 16.09.2024).
[132] Çolak ve Tevetoğlu, s. 69.
[133] Detaylı bilgi için bölüm 1.6'ya bakınız.

dayanılacağına yönelik herhangi bir görüş birliği bulunmamaktadır.[134] Kurul'un vermiş olduğu kararlar ışığında ilgili kişinin "*açık rıza*" sunması gerektiği belirtilirken, AB mevzuatı çerçevesinde "*veri sorumlusunun meşru menfaatlerinin korunması için gerekli olması*" şartına yönelik yaklaşım mevcuttur.[135]

Bu doğrultuda dijital platformların, pazarlama faaliyeti yürütmek için genel ilkelere uygun davranması ve herhangi bir veri işleme faaliyetine başlamadan önce KVKK madde 10 uyarınca ilgili kişilere karşı aydınlatma yükümlülüğünü yerine getirmesi gerekmektedir. Bu kapsamda, platformlarında kullanıcılarına, hangi kişisel verilerinin hangi amaçla işleneceği, verilerin kimlere ve hangi amaçlarla aktarılabileceği, veri toplama yöntemi ve hukuki sebebi hakkında bilgi vermesi gerekmektedir.[136]

Daha sonra bu veri işleme faaliyetine yönelik kullanıcının açık rızasını talep etmesi gerekecektir. Açık rızanın temel unsurları belirli bir konuya ilişkin olma, bilgilendirmeye dayanma ve özgür iradeyle açıklanmasıdır. Dolayısıyla dijital platformların açık rıza talep ederken bu unsurlara mutlaka dikkat etmesi gerekmektedir.[137]

Dijital platformların açık rıza talep ederken özgür iradenin sağlanması noktasında Kurul, ilgili kişinin açık rızası istenirken bu teklifin bir hizmetin ya da sözleşmenin kurulması için gerekli olacak şekilde sunulmasının açık rızadaki özgür irade unsurunu sakatlayacağı görüşündedir. Kurul'un *Amazon Turkey* hakkında verdiği kararında[138] *Amazon Turkey*'in internet sitesinde çerezlerin çalışmasının engellenmesi veya çalışmasına izin verilmemesi halinde alışveriş yapamayacağını belirtmesi kişisel verilerin işlenmesi için sunulan hizmetin bir şartı niteliğinde olduğunu değerlendirmiştir. Açık rızanın hizmetin sunulması

[134] Çolak, Tevetoğlu, s.69.
[135] Polater, s.1.
[136] Dülger, s.397.
[137] Dülger, s.140.
[138] Amazon Turkey Perakende Hizmetleri Limited Şirketi hakkındaki başvuru ile ilgili Kişisel Verileri Koruma Kurulunun 27/02/2020 Tarihli ve 2020/173 Sayılı Karar Özeti: https://www.kvkk.gov.tr/Icerik/6739/2020-173 (E.T.: 16.09.2024).

şartına bağlanması halinde de özgür irade unsurunun sakatlanacağı için geçerli bir açık rızanın söz konusu olmadığını vurgulamıştır.

## 2.5. İLGİLİ KİŞİNİN HAKLARI

İlgili kişi hakları veri koruma hukukunun en temel noktasıdır. Kişisel verilerin korunması hakkı da bireylerin verilerinin tehlike altında olduğu düşüncesiyle beraber gündeme gelmiştir.[139] Dijitalleşmenin hız kazandığı günümüzde, kişisel verilerin korunması giderek daha da büyük bir önem kazanmıştır.

Dijital platformlar, kullanıcıların kişisel verilerini toplamak, işlemek ve depolamak için yaygın bir şekilde kullanılmaktadır. Bu sebeple dijital platformların kişisel verilerin etkili bir şekilde korunması ve işlenmesine ilişkin olarak önemli sorumlulukları bulunmaktadır.

İlgili kişilerin kişisel verileri üzerinden daha fazla kontrol sahibi olmalarının sağlanması dijital platformların ilgili kişi tarafından yapılan başvurulan cevaplandırması ile mümkündür. Bu yükümlülük ilgili kişinin kendi kişisel verileri hakkında bilgi edinme hakkı ile bağlantılıdır. Bu doğrultuda ilgili kişiye verilecek cevapların açık, anlaşılır ve sade olması önem arz etmektedir.[140]

Bu bölümde KVKK ve GDPR'da belirlenen ilgili kişi haklarının karşılaştırmalı bir çalışması yapılarak dijital platformlardaki işleyişi ve bu hakların etkili bir şekilde nasıl uygulanabileceği değerlendirilecektir.

### 2.5.1. KVKK Madde 11 Uyarınca İlgili Kişi Hakları

KVKK kapsamında ilgili kişi hakları madde 11'de düzenlenmektedir. Buna göre ilgili kişiler, "*kişisel veri işlenip işlenmediğini öğrenme, kişisel verileri işlenmişse buna ilişkin bilgi talep etme, kişisel verilerin işlenme amacını ve bunların amacına uygun kullanıp kullanılmadığını öğrenme, yurt içinde veya yurt*

[139] Dülger, s.347.
[140] Başalp, Kişisel Verilerin Korunması, s.49.

*dışında kişisel verilerin aktarıldığı üçüncü kişileri bilme, kişisel verilerin eksik veya yanlış işlenmiş olması halinde bunların düzeltilmesini isteme, 7 nci maddede öngörülen şartlar çerçevesinde kişisel verilerin silinmesini veya yok edilmesini isteme, yapılan işlemlerin, kişisel verilerin aktarıldığı üçüncü kişileri bildirilmesini isteme, işlenen verilerin münhasıran otomatik sistemler vasıtasıyla analiz edilmesi suretiyle kişinin kendisi aleyhine bir sonucun ortaya çıkmasına itiraz etme, kişisel verilerin kanuna aykırı olarak işlenmesi sebebiyle zarara uğraması halinde zararın giderilmesini talep etme haklarına sahiptir."*

İlgili kişilerin hakkını kullanımı KVKK madde 13'te düzenlenmiş ve bu maddeye dayanak alınarak veri sorumlusuna başvuru sırasında dikkat edilmesi gereken hususlar ise Veri Sorumlusuna Başvuru Usul ve Esasları Hakkında Tebliğ[141] ("**Veri Sorumlusuna Başvuru Tebliğ**") kapsamında yayımlanmıştır. Dijital platformların ilgili kişilerin bu haklarını kullanırken dikkat etmesi gereken temel hususların başında Veri Sorumlusuna Başvuru Tebliğ madde 4 uyarınca ilgili kişilerin başvurularının Türkçe olma zorunluluğu gelmektedir. Bu konu özellikle küresel dijital platformlar bakımından da önem arz etmektedir.

KVKK'nın 13. maddesine göre ilgili kişilerin bu haklarını kullanmak için veri sorumlusuna yazılı olarak başvuru yapmaları gerekmektedir. Veri Sorumlusuna Başvuru Tebliği'nin 5. maddesi uyarınca bu başvuruyu veri sorumlusunun sistemlerinde kayıtlı olan elektronik e-posta adresi, güvenlik elektronik imza, mobil imza ya da kayıtlı elektronik posta adresi aracılığıyla gerçekleştirebilmektedir.

Bir dijital platform için en sağlıklı yöntem platformun içerisinde ilgili kişilerin haklarını kullanmasını sağlayacağı ayrı bir sekme geliştirmesidir. Anılan sekme vasıtası ile gerekli olan bilgi ve belgelerin de teyidi kolaylaşacak, doğruluğunu kontrol eden mekanizmalar geliştirilebilecektir.

KVKK madde 13 uyarınca veri sorumlusu olarak dijital platformlar

[141] RG: 10.03.2018, 03356.

mevzuata uygun bir başvuruyu teslim aldıktan sonra talebi incelemeli, talep konusuna göre bu başvuruyu en kısa sürede ve en geç otuz gün içinde cevaplandırmalıdır.

Veri Sorumlusuna Başvuru Tebliği'nin 6. maddesi uyarınca dijital platformların başvuruları etkin bir şekilde sonuçlandırmalıdır ve bunun için de gerekli her türlü idari ve teknik tedbirleri alması gerekmektedir. Dijital platformların alabileceği tedbirin yapılarına ve faaliyetlerine göre değişebilecek olsa da en önemlisi başvuruları ilgili kişi başvurularına özgülenmiş bir e-posta adresinin aydınlatma metinlerinde yer verilmesi olduğu değerlendirilebilecektir. Uygulamada pek çok dijital platform ilgili kişi haklarını bu yöntemle kullanılmasını sağlamaktadır, ayrıca bu hesapları aktif bir şekilde takip ve kontrol ediliyor olması oldukça önemlidir. Çok fazla ilgili kişi başvurusu alan bazı dijital platformların bu başvuruları gerek yapay zekâ gerek akıllı yazılımlar vasıtasıyla yönettikleri yöntemler de uygulanmasına engel bulunmamaktadır.

### 2.5.2. GDPR'da İlgili Kişi Hakları

İlgili kişi hakları, GDPR Bölüm 3 İlgili Kişinin Hakları (*Rights of the Data Subject)* başlığı altında 12 ile 23. maddelerini kapsamaktadır. Bu haklar KVKK'dan farklı[142] olarak veri sorumlusu ile veri işleyenlere de sorumluluk doğurmaktadır ve temel olarak ilgili kişileri haklarını korumak ve nasıl kullanılacağına ilişkin kapsamlı bir çerçeve oluşturmaktadır.

GDPR'ın 12., 13. ve 14. maddelerinde ilgili kişilerin kişisel verilerinin açık bir şekilde işlenmesini ve bilgi verme yükümlülüğüne ilişkin gerekli hükümlere

[142] KVKK'nın 12. maddesi ikinci fıkrası kapsamında veri sorumlusunun, kişisel verilerin kendi adına başka bir gerçek veya tüzel kişi tarafından işlenmesi halinde *(i)* kişisel verilerin hukuka aykırı olarak işlenmesini önlemek, (ii) kişisel verilere hukuka aykırı olarak erişilmesini önlemek, kişisel verilerin muhafazasını sağlamak, amacıyla uygun güvelik düzeyini temin etmeye yönelik her türlü teknik ve tedbirlerin alınması hususunda bu kişilerle birlikte müştereken sorumlu kabul edilmiştir. Dolayısıyla her ne kadar ilgili kişilerin haklarının kullanılmasına ilişkin açık bir düzenleme olmasa da bu hüküm gereğince veri işleyenler de ilgili kişilerin kişisel verilerinin güvenliğini sağlamakla yükümlüdür. Ayrıca ilgili maddenin dördüncü fıkrasında da veri sorumluları ile veri işleyen kişilerin, öğrendikleri kişisel verileri KVKK hükümlerine aykırı olarak başkasına açıklayamayacağı ve işleme amacı dışına kullanamayacağını düzenlemektedir.

yer vermektedir. Bu maddeler, kişisel verilerin işlenmesi sırasında ilgili kişilerin haklarına ilişkin temel ilkeleri ve kişisel verilerin hukuka uygun olarak işlenmesi gerektiğini düzenlemektedir. Ayrıca bilgi vermeye ilişkin düzenlemeler kapsamında kişisel verileri doğrudan ilgilisinden elde edilebileceği gibi üçüncü bir kişiden de elde edilebilir. Bu maddelerde düzenlenen hususlar, KVKK uyarınca ilgili kişinin haklarından hemen önce "Veri sorumlusunun aydınlatma yükümlülüğü" başlıklı 10. maddede düzenlenmiştir.[143]

Temel olarak GDPR 15 ile 22. maddelerinde ise ilgili kişilere çeşitli haklar tanımlanmaktadır. Bu haklar sırasıyla, kişisel verilere erişim hakkı (*right to access by data subject),* düzeltme hakkı (*right rectification),* silinme hakkı "unutulma hakkı" (*right to erasure "right to be forgotten"),* işlemenin sınırlanması hakkı (*right to restriction of processing),* veri işleme faaliyetinin sınırlandırılmasının veya kişisel verilerin silinmesinin veya düzeltilmesinin bildirim yükümlülüğü (*notification obligation regarding rectification or erasure of personal data or restriction of processing),* veri taşınabilirliği hakkı *(right to portability),* itiraz hakkı *(right to object),* profilleme gibi otomatik karar veri işleme faaliyetlerine ilişkin haklar *(automated individual decision-making including profiling )* olmak üzere haklara sahiptirler. Madde 23 ise GDPR'ın 12 ile 22. Maddelerinde belirtilen hakların ve yükümlülüklerin, AB veya üye devletlerin kanunları uyarınca sınırlanabileceğini belirtmektedir. Ancak, bu sınırlamanın demokratik bir toplumda temel hak ve özgürlüklere saygı gösterirken ulusal güvenlik, savunma, kamu güvenliği gibi konular için gerekli ve orantılı bir önlem olmalıdır.

### 2.5.3. GDPR ve KVKK'daki İlgili Kişi Haklarının Karşılaştırması

GDPR ve KVKK, temelde kişisel verilerin işlenmesi ve korunmasıyla ilgili benzer prensipleri benimsemektedir. Ancak, bu iki düzenleme arasında belirli farklılıklar bulunmaktadır. Özellikle, küresel boyutta faaliyet gösteren dijital platformlar bakımından farklı ülkelerden aldıkları başvurular bakımından bu

[143] Dülger, s. 348.

farklılıkların bilinmesi ve değerlendirilmesi büyük önem taşımaktadır.

GDPR kapsamında ilgili kişi hakları ayrı bir bölüm altında sekiz ayrı madde kapsamında düzenlenirken KVKK'da ilgili kişi hakları madde 11'de düzenlenmektedir. Bu hakların karşılaştırmalı olarak yer verildiği bir tablo aşağıdadır:

**Tablo 2. 1.** Karşılaştırmalı İlgili Kişi Hakları

| **Haklar** | **GDPR Bölüm 3** | **KVKK Madde 11** |
|---|---|---|
| Erişim Hakkı | İlgili kişiler veri sorumlusu bünyesinde işlenen kişisel verilerine erişme hakkına sahiptirler. | Kişisel verilerin işlenip işlenmediğini öğrenme,<br><br>Kişisel verileri işlenmişse buna ilişkin bilgi talep etme,<br><br>Kişisel verileri işlenme amacını ve bunların amacına uygun kullanılıp kullanılmadığını öğrenme,<br><br>Yurt içinde veya yurt dışında kişisel verilerin aktarıldığı üçüncü kişileri bilme hakkına sahiptirler. |
| Düzeltme | İlgili kişiler, yanlış veya eksik kişisel verilerin düzeltilmesini | Kişisel verilerin eksik veya yanlış işlenmiş |

| | | |
|---|---|---|
| Hakkı | talep etme hakkına sahiptirler. | olması halinde bunların düzeltilmesini talep etme hakkına sahiptirler. |
| Silme Hakkı | GDPR kapsamında ayrıca "Unutulma Hakkı" (*right to erasure ("right to be forgotten")* da belirtilmektedir. İlgili kişiler, kişisel verilerinin silinmesini veya kaldırılmasını talep etme hakkına sahiptirler. | Gerekli şartların varlığı halinde kişisel verilerin silinmesini veya yok edilmesini isteme hakkına sahiptirler. |
| Veri İşleme Faaliyetini Kısıtlama Hakkı | İlgili kişi, madde metninde belirtilen belirli durumların varlığı halinde veri sorumlusunda veri işleme faaliyetinin kısıtlanmasını isteme hakkına sahiptir. | Mevcut değil. |
| Bildirim Yükümlülüğü | Veri sorumluları, ilgili kişinin veri işleme faaliyetinin sınırlandırılmasının veya kişisel verilerin silinmesinin veya düzeltilmesi talebini verilerin aktarıldığı taraflara bildirmekle yükümlüdür. | Kişisel verilerin düzeltilmesi veya silinmesine, yok edilmesine ilişkin taleplerin kişisel verilerin aktarıldığı üçüncü kişilere bildirilmesini talep etme hakkına sahiptirler. |
| Veri | Veri Taşınabilirliği Hakkı: İlgili | Mevcut değil. |

| | | |
|---|---|---|
| Taşınabilirliği | kişiler, kişisel verilerini başka bir veri sorumlusuna aktarma veya kopyalama hakkına sahiptir. | |
| İtiraz Hakkı | İlgili kişi, kişisel verilerin doğruluğuna ilişkin şüphelerin olması gibi belirli durumlarda veri işleme faaliyetinin yürütülmesine itiraz edebilir. | Mevcut değil. |
| Otomatik Veri İşleme Faaliyetine Yönelik Haklar | İlgili kişiler profilleme gibi otomatik karar veri işleme faaliyetlerine itiraz hakkına sahiptir. | İşlenen verilerin münhasıran otomatik sistemler vasıtasıyla[144] analiz edilmesi suretiyle kişinin kendisi aleyhine bir sonucun ortaya çıkmasına itiraz etme hakkına sahiptirler. |
| Zararın Giderilmesini İsteme Hakkı | Mevcut değil. | Kişisel verilerin kanuna aykırı olarak işlenmesi sebebiyle zarara uğraması halinde zararın giderilmesini talep etme hakkına |

[144] Otomatik karar alma kavramı GDPR ile gelen bir kavramdır. KVKK'da bu kavram açıklanmamaktır. Bu kavramın mantığı ise, erişim talebinde bulunan ilgili kişinin yalnızca otomatik işlemede gerçekleşen ve kendisiyle ilgili olarak hukuku veya benzer etkiler yaratan herhangi bir otomatik karar verme sürecine dahil olan mantık hakkında anlamlı bilgiler alma hakkına sahip olması gerektiğidir. İlgili kişi, bu karar vermedeki etkenlerin yanı sıra kararın önemi ve öngörülen sonuçları hakkında da bilgilendirilme hakkına sahiptir. Bkz. Lloyd-Jones/Carey, s.132.

| | | |
|---|---|---|
| | | sahiptirler. |

Yukarıdaki tablodan görüldüğü üzere GDPR ve KVKK kapsamında ilgili kişi hakları hemen hemen benzer olsa da GDPR tahtına daha detaylı bir şekilde ele alındığı anlaşılmaktadır.

### 2.5.3.1. Erişim Hakkı

GDPR ile erişim hakkının kapsamı oldukça genişletilerek bireylere kişisel verileri ile ilgili her türlü bilgiyi elde edebileceği imkanlar sağlamıştır. KVKK'da ise açıkça erişim hakkından söz edilmese de erişim hakkı kapsamında talep edilebilecek bilgiler sayılmıştır. [145]

Erişim hakkı değerlendirilirken dijital platformların başvuruya yönelik olarak ellerinde tuttukları kendileri tarafından anlaşılabilecek şekilde kodlanmış ya da özel bir yöntem ya da dille işlenmiş olması durumunda, ilgili kişiye bu yöntem ya da dilin açıklanması gerekmektedir. Verilerin bilgisayar ortamında herhangi bir ortalama kişi tarafından anlamlandırılamayacak surette işleniyor olması durumunda veri sorumlusu tarafından verilerin işlenmesi ve amaçlarına yönelik makul ölçüde açıklama yapılmalıdır. [146]

Dijital platformların bu düzenleme çerçevesinde, ilgili kişinin erişim hakkını kullanırken aynı zamanda veri güvenliğine ilişkin yükümlülükleri de göz önünde bulundurması gerektiği belirtilmelidir. KVKK'da bu hak, kişisel verilerin doğrudan erişim hakkını değil, verinin içeriğine makul şekilde ulaşabilmesini sağlayacak bilgiyi talep etme hakkını içermektedir.

İlgili kişinin erişim hakkının değerlendirildiği 14.01.2020 tarihli ve 2020/13 sayılı Karar Özeti[147] kapsamında, ilgili kişi, sermaye piyasası mevzuatı

[145] Dülger, s.352.
[146] Dülger, s.354.
[147] "İlgili kişi ile veri sorumlusu şirket arasında gerçekleştirilen telefon görüşmelerine ilişkin kayıtların ilgili kişiye verilmesi yönündeki talebin reddedilmesi hakkında" Kişisel Verileri Koruma

kapsamında veri sorumlusu ile akdedilen sözleşme uyarınca işlenen kişisel verileri arasında yer alan telefon görüşmesi kayıtlarına erişim talebinin reddedilmesine ilişkin Kurum'a şikâyette bulunmuştur. Kurul, Türkiye Cumhuriyeti Anayasası'nın "*Özel Hayatın Gizliliği*" başlıklı 20. maddesi ve KVKK'nın 11. maddesine yaptığı atıf ile ilgili kişinin kişisel verilerine erişim hakkının kişisel veri güvenliğine yönelik tedbirleri ile değerlendirilerek sağlanması gerektiği belirtilmiştir. Erişim talebi, ses kaydının şikayetçiden başka telefon görüşmesinde olan gerçek kişilerin kişisel verisini içeren ses kayıtlarını içermesi sebebiyle yasal makamlar tarafından talep edilmesi halinde teslim edebileceğini belirtmesini makul olduğunu, ancak doğrudan teslim etmek yerine ses kayıt dökümlerinin ilgili kişi tarafından tam olarak anlaşılmasının mümkün olacağı şekilde, erişim hakkı sağlanabileceğine karar vermiştir.

Benzer bir diğer karar olan 30.06.2020 tarihli ve 2020/504 sayılı Karar Özeti[148] kapsamında da şikayetçi ilgili kişi bir havayolu şirketinin çağrı merkezi ile bir görüşme gerçekleştirmiş, bu görüşme sırasındaki ses kaydını talep etmiştir. Veri sorumlusu şirket ise şirket politikalarına göre ses kayıtlarının sadece yasal mercilerce talep edilmesi halinde mümkün olacağı belirtilmiş ve ilgili kişinin bu başvurusu reddedilmiştir. Ancak, ses kaydının transkripti ise maskeleme tedbiri de uygulanarak ilgili kişi ile paylaşılmıştır. Yukarıda özetlenen diğer karara da atıf yaparak Kurul tarafından bu konu hakkında yapılacak bir işlem olmadığına karar verilmiştir. [149]

Uygulamada dijital platformlarında karşılaşacağı her türlü erişim talebini veri güvenliği tedbirlerini alarak yaklaşması oldukça önem arz etmektedir. Bu noktada veri minimizasyonu ilkesi ile erişim talep edilen kişisel verilerin diğer

Kurulunun 14/01/2020 Tarihli ve 2020/13 Sayılı Karar Özeti, https://www.kvkk.gov.tr/Icerik/6698/2020-13 (E.T.: 16.09.2024).

[148] "Veri sorumlusu bir havayolu şirketi tarafından ilgili kişiye ait çağrı merkezi görüşme kayıtlarının transkriptinin teslim edilmemesi" hakkında Kişisel Verileri Koruma Kurulunun 30/06/2020 tarihli ve 2020/504 sayılı Karar Özeti, https://www.kvkk.gov.tr/Icerik/6932/2020-504 (E.T.: 16.09.2024).

[149] Aynı konuda bir başka karar için bkz. https://kvkk.gov.tr/Icerik/7769/2023-1050 (E.T.: 16.09.2024).

üçüncü kişileri de etkileyip etkilemediğinin değerlendirilmesi gerekmektedir.

### 2.5.3.2. Düzeltme Hakkı

Düzeltme hakkı, veri sorumlusuna yüklenen kişisel verilerin doğru ve gerektiğinde güncel olması ilkesiyle doğrudan bağlantılı olduğu değerlendirilmektedir.[150] GDPR ve KVKK neredeyse aynı düzenleme ile kişisel verilerin doğru ve güncel tutulması konusunda veri sorumlusuna bir yükümlülük yüklerken aynı zamanda ilgili kişinin de bunu talep edebileceğini düzenlemiştir.

Bu hak kapsamında dijital platformlar, öncelikli yükümlülüğü olarak verilerin doğru ve güncel tutulmasında sorumlu olup, eğer bir ilgili kişinin düzeltme hakkını kullanmak üzere talepte bulunması halinde de bu talebi yerine getirmesi gerekmektedir.

### 2.5.3.3. Silme ve Unutulma Hakkı

Silme hakkı GDPR ve KVKK'da benzer şekilde düzenlense de GDPR madde 17 ayrıca unutulma hakkına da değinmiştir. Ancak, KVKK kapsamında ilgili kişi hakları düzenlenirken "unutulma hakkı" belirtilmemiştir.[151]

GDPR'a göre ilgili kişi veri sorumlusuna başvurarak kişisel verilerinin silinmesini talep edebilmektedir. Maddenin ikinci paragrafında ise unutulma hakkına değinmiştir. Bu kapsamda veri sorumlusu kişisel verileri kamuya sunmuşsa ve bu verilerin silinmesine ilişkin ilgili kişi tarafından talepte bulunulursa, veri sorumlusu mevcut teknolojiyi ve uygulama maliyetini göz önünde bulundurarak makul adımlar atmalıdır. Ayrıca, kişisel verileri kamunun erişimine sunan veri sorumlusu, bu kişisel verileri işleyen diğer veri sorumlularına, kişisel verilere ait herhangi bir bağlantıyı veya kopyalarını silmeleri konusunda bilgilendirmelidir. Bu kapsamda veri sorumlusu diğer veri sorumlularını

[150] Dülger, s.360.
[151] **USTA, Dr. Oğuz**, Kişilik Hakkı Bağlamında Unutulma Hakkı, Adalet Yayınevi, Ankara, 2023\ s.88.

bilgilendirmek üzere makul adımların atılmasından sorumludur.[152]

Unutulma hakkı teknolojinin gelişmesiyle karşımıza çıkan bir hak olup, öğretide ve uygulamada mutabık kalınan bir tanımı yoktur.[153] Bir görüş unutulma hakkının internet ortamında yer alan kişisel verilerin kamuya sunulmasının kısıtlanması olarak tanımlamaktadır.[154] Bir görüşe göre ise bu tanıma ek olarak bu hak kapsamındaki kişisel verileri üçüncü kişilerin bilmesini istemediği kamuya açık olmayan verileri kapsayacak şekilde belirtilmiştir.[155] Başka bir görüşe göre ise *"kişisel verilerin belirli bir süre geçtikten sonra arama motorları aracılığıyla üçüncü kişilere ulaşmasının engellenmesi"* olarak tanımlanmıştır.[156]

Türkiye'de de "unutulma hakkı" başlığı altında doğrudan bir hukuki düzenleme bulunmamakla birlikte çeşitli hükümler bu hakkın gerçekleştirilmesini mümkün kılmaktadır. Öncelikle Anayasa'nın 20. maddesinin üçüncü fıkrasında düzenlenmiştir. KVKK kapsamında ise 4., 7. ve 11. maddeleri ile Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi Hakkında Yönetmelik'in 8. maddesinde unutulma hakkının kullanılabileceğine dair düzenlemeler yer almaktadır[157]

Kurul her ne kadar ayrıca tanımlanmamış olsa da Unutulma Hakkının Arama Motorları Özelinde Değerlendirilmesi Rehberi'nde ("**Unutulma Hakkı Rehberi**")[158] unutulma hakkının "silinme hakkı" çerçevesinde nasıl

---

[152] GDPR, Recital 66, Right to be Forgotten: https://gdpr-info.eu/recitals/no-66/ (E.T.: 16.09.2024)
[153] Usta, s.96, 97.
[154] Olgun Değirmenci, "Yargısal İçtihatların Ortaya Çıkardığı Bir Hak: Unutulma Hakkı (Çerçevesi ve Hak Üzerine Düşünceler)", THD, 2018, C.13, s.144, 153-263.
[155] **ÖNOK, Murat,** "Kişisel Verilerin Korunması Bağlamında "Unutulma Hakkı" ve Türkiye Açısından Değerlendirmeler", 2017, İKÜHFD, C.16, S.1, s.155-188
[156] **YAVUZ, Can**, İnternet'teki Arama Sonuçlarından Kişisel Verilerin Kaldırılması Unutulma Hakkı, 2018, Ankara, 2. Baskı, s.57.
[157] Kişisel Verilerin İşlenmesi ve Bu Tür Verileri Serbest Dolaşımına Dair Bireylerin Korunması Hakkında 95/46/EC sayılı Avrupa Birliği Direktifi'nde meşru amaçlarla uyumsuz bir biçimde depolanan veya eksik/yanlış olan verilerin engellenmesi veya silinmesi talebi ilgili kişiye tanınmakla birlikte ayrıca "Unutulma Hakkı" ile ilgili bir düzenleme bulunmamaktadır.
[158] Kişisel Verileri Koruma Kurulu, Unutulma Hakkı (Unutulma Hakkının Arama Motorları Özelinde Değerlendirilmesi), Ankara: https://www.kvkk.gov.tr/SharedFolderServer/CMSFiles/11b6fd99-d42a-45b1-a009-21f2d36ded21.pdf (E.T.: 16.09.2024).

kullanılacağını açıklamaktadır. Unutulma Hakkı Rehberi kapsamında, arama motorlarında yürütülen aramalarda gerçek kişilere ait ad ve soyadı ve diğer sonuçların indeksten çıkarılmasına dair talepleri hakkındaki Kurul'un 23/06/2020 tarihli ve 2020/481 sayılı Kararı[159] çerçevesinde, arama motorlarında unutulma hakkının kullanılmasını açıklamaktadır.[160]

Unutulma Hakkı Rehberi'nde öncelikle gelişen teknoloji sayesinde verilerin kolay ve hızlı bir şekilde kaydedildiği ve neredeyse süresiz bir şekilde saklanabildiğine, hızlı paylaşım yapılabildiğine dikkat çekilmektedir.

Bu hak Yargıtay kararları kapsamında: "*bireyin geçmişte hukuka uygun olarak yayılmış ve doğru nitelikteki bilgilerinin zamanın geçmesine bağlı olarak erişimden kaldırılmasını ya da gündeme getirilmemesini talep edebilmesi*" olarak tanımlamaktadır.[161]

Uluslararası düzlemde bakıldığında, unutulma hakkına ilk karşılaşıldığı dava ABAD'ın 13.05.2014 tarihli kararıdır. Bu kararın tarafları İspanyol Veri Koruma Otoritesi ile Mario Costeja Gonzalez'in; L Vanguardia Ediciones SL, Google ve Google İspanya'dır. Söz konusu karar unutulma hakkına ilişkin önemli yargı kararı olarak değerlendirilmektedir.[162]

Bu davada, Costeja Gonzales, Google arama motorunda kendi adını yazdığında La Vanguardia gazetesinin iki farklı tarihli yayınında yer alan bu kişinin sosyal güvenlik borçlarını ödeyemediği için mülkünü satmak zorunda kaldığını belirten bilgilerin artık ilgisiz olduğunu belirterek gazete arşivlerinden ve Google arama sonuçlarından kaldırılmasını ve gizlenmesini istemiştir.

İspanyol Veri Koruma Otoritesi, ulusal mevzuat çerçevesinde kamuoyunun

---

[159] İlgili karar için bkz https://www.kvkk.gov.tr/Icerik/6776/2020-481 (E.T.: 16.09.2024).
[160] Usta, s.99.
[161] Yargıtay Hukuk Genel Kurulu'nun 17.06.2015 tarihli E:2014/4-56, K:2015/1679 sayılı Kararı.
[162] Judgement of the Court (Grand Chamber), Case C-131/12, EU:C:2014:317, 13.05.2014. gencia Española de Protección de Datos (AEPD) and Mario Costeja González v. Google Spain SL, Google Inc., (https://curia.europa.eu/juris/liste.jsf?td=ALL&language=en&jur=C,T&num=c-131/12) (E.T.: 16.09.2024).

bu bilgiye erişiminde menfaatinin bulunduğunu belirterek Gonzalez'in talebini reddetmiş, ancak Google'ın da ilgili linkleri kaldırmasına karar vermiştir. İspanya'da karara karşı temyiz yoluna başvuran Google, İspanya Yüksek Mahkemesi tarafından verilen bir kararla temyiz yoluyla kararı ABAD'a taşımıştır. ABAD, arama motorlarında çıkan sonuçların "*geçersiz, eksik, tamamen ilgisiz veya sonradan ilgisiz hale gelmiş*" olması durumunda, bu sonuçlarında ilgili arama motorları tarafından silinmesi gerektiğine karar vermiştir.

### a) Kurul Kararları Işığında Unutulma Hakkı

Kurul'un 23/06/2020 tarihli ve 2020/481 sayılı Karar Özeti'ne[163] konu olan olayda ilgili kişilerin medya kuruluşlarına ait internet sitelerindeki haberlerde yer alan isim ve soy isimlerinin veya haberlerin silinmesi talep edilmiştir. Ayrıca, bu gazete arşivlerinin arama motorları hakkında indekslenmemesi hususunda da talepler bulunmaktadır. Bu talepler, "*unutulma hakkı*" kapsamında değerlendirilmiştir.

Karar kapsamında unutulma hakkı bireyin geçmişte hukuka uygun olarak yayımlanmış bilgilerinin zamanın geçmesiyle erişimden kaldırılmasını veya gündeme getirilmemesini talep etme hakkı olarak tanımlanabileceği belirtilmiştir. Anayasa'nın 20. maddesi kapsamındaki kişisel verilerin korunmasını isteme hakkının düzenlendiği ve kişilere verilerin silinmesini talep etme hakkının tanındığı vurgulanmaktadır. Anayasa Mahkemesi ve Yargıtay kararları ışığında unutulma hakkı, "*dijital hafızada yer alan geçmiş olumsuz olayların unutulmasını ve kişisel verilerin silinmesini isteme hakkı"* olarak tanımlanmıştır. İlgili kararda ayrıca ABAD'ın Google İspanya davasına da atıf yapılmış ve kişinin özel hayatının gizliliği hakkının arama motorunun ekonomik çıkarı ve kamunun bilgiye erişim hakkının üzerinde olduğu vurgulanmıştır.

Sonuç olarak, arama motorlarının, internet üzerinde elde ettikleri verilerin

[163] Kişilerin Ad ve Soyadı ile Arama Motorları Üzerinden Yapılan Aramalarda Çıkan Sonuçların İndeksten Çıkarılmasına Yönelik Talepler ile ilgili olarak Kişisel Verileri Koruma Kurulunun 23/06/2020 Tarihli ve 2020/481 Sayılı Kararı (https://www.kvkk.gov.tr/Icerik/6776/2020-481) (E.T.: 16.09.2024).

işlenmesi sırasında bu işleme faaliyetinin amaç ve vasıtalarını belirledikleri ve veri sorumlusu olarak kabul edilmeleri gerektikleri belirtilmiştir. Bu doğrultuda ilgili kişilerin arama sonuçlarının indeksten çıkarılmasına yönelik taleplerini öncelikle ilgili arama motorlarına yönlendirmeleri gerekmektedir. Arama motorlarının bu talepleri reddetmeleri veya bu taleplere hiç cevap vermemeleri halinde ilgili kişiler şikâyet etme hakkına sahip olacaktır. Arama motorları tarafından bu taleplerin değerlendirilmesinde ilgili kişinin temel hak ve özgürlükleri ile kamuoyunun bu bilgiye erişmesindeki menfaatleri arasında bir denge olmalıdır, dolayısıyla bu noktada bir denge testi yapılmalıdır. İlgili kişiler, arama motorlarına başvurularının reddedilmesi veya cevap alınamaması halinde doğrudan yargı yoluna da başvurabilmektedirler.

Unutulma hakkı kapsamında arama motorunda yer alan kişiye ait ad ve soyadı ile bağlantılı sonuçların kaldırılması talebinin incelendiği bir karara[164] konu olayda üniversitede öğretim üyesi olan bir kişinin sosyal medyada yapılan ve bir yakını ile ilgili atamada kendisine yönelik usulsüzlük iddialarına ilişkin haberlerin arama sonuçlarından kaldırılmasını talep etmiştir. Başvuru sahibi, haberlerin hayatını ve kamu görevini olumsuz etkilediğini belirtmiştir. Kurul yaptığı değerlendirmede arama motorunun veri sorumlusu olarak kabul edildiklerini belirtmiştir. Bu talep kapsamında ilgili kişinin temel hak ve özgürlükleri ile kamuoyunun bilgiye erişim hakkı arasında denge testi yapılması gerektiği değerlendirilmiştir. Kriterler arasında ilgili kişinin kamusal yaşamda rol oynaması, bilginin doğruluğu ve güncelliği, bilginin ilgili kişi açısından herhangi bir risk teşkil edip etmediği ve bilginin gazetecilik faaliyeti kapsamında işlenip işlenmediği yer almaktadır. Sonuç olarak, ilgili kişinin adı soyadı ile bağlantılı sonuçların kaldırılmasına yönelik talebin yapılan haberlerin güncel ve çalışma yaşamına ilişkin olduğu, bilgilerin özel nitelikli kişisel veri niteliği taşımadığı ve içeriklerin gazetecilik faaliyeti kapsamında değerlendirilebileceği göz önüne

[164] Unutulma hakkı kapsamında ilgili kişinin arama motorunda adı ve soyadı ile bağlantılı sonuçların kaldırılması talebi"ne ilişkin Kişisel Verileri Koruma Kurulunun 08/12/2020 tarihli ve 2020/927 sayılı Karar Özeti: https://kvkk.gov.tr/Icerik/6871/2020-92 (E.T.: 16.09.2024).

alınarak reddedilmiştir.

Bir gazetedeki köşe yazısında bir kişinin adının geçtiği ve bu köşe yazısının silinmesi talebine ilişkin Kurul kararı[165] kapsamında ise başvuruda bulunan kişi, adının bir gazetedeki köşe yazısında geçtiği gerekçesiyle bu yazının silinmesini talep etmiştir. Kurul bu talebi değerlendirirken ilgili kişinin hala kamuyu ilgilendiren bir statüye sahip olduğu, ifade özgürlüğünün yansıması olan basın özgürlüğü kapsamında değerlendirilen bir köşe yazısı olduğunu dikkate almıştır. Bu kapsamda, Kurul, KVKK'nın 28. maddesinin birinci fıkrasının (c) bendi uyarınca, ifade özgürlüğünün ve basın özgürlüğünün korunması gerektiği gerekçesiyle ilgili kişinin köşe yazısını silinmesi talebine ilişkin herhangi bir işlem yapılmasına gerek olmadığına karar verilmiştir.

Diğer bir karar[166] kapsamında Kurul, ilgili kişinin kişisel verilerinin silinmesi talebini yerine getirilmediği bir durumu incelemiştir. Başvuruda bulunan kişi, aktif olmayan bir müşteri olarak kişisel verilerinin silinmesini talep etmiştir. Ancak veri sorumlusu, hukuki yükümlülükleri çerçevesinde işlediği kişisel verileri 10 yıl boyunca muhafaza etmek zorunda olduğunu belirtmiştir. Kurul, veri sorumlusunun, kişisel verileri saklama yükümlülüğünü kabul etmekle birlikte, bu verilerin saklama amacı dışında işlenmemesi gerektiği yönünde veri sorumlusuna talimat vermiştir. Bu kapsamda aktif olmayan müşterilerin kişisel verilerinin sadece saklama amacı doğrultusunda muhafaza edilmesi ve başka amaçlar ile işlenmemesi gerektiğine karar verilmiştir.

İlgili kişinin hüküm giydiği suça ilişkin haberin bir gazetenin internet sitesinden kaldırılmasını talep ettiği kararda[167] da ilgili kişinin vekili, müvekkilinin

---

[165] Bir Gerçek Kişinin Adının Geçtiği Köşe Yazısının Silinmesi Talebi https://kvkk.gov.tr/Icerik/5407/-Bir-Gercek-Kisinin-Adinin-Gectigi-Kose-Yazisinin-Silinmesi-Talebi (E.T.: 16.09.2024).

[166] İlgili Kişinin Kişisel Verilerinin Silinmesi Talebinin Yerine Getirilmemesi https://kvkk.gov.tr/Icerik/5415/Ilgili-Kisinin-Kisisel-Verilerinin-Silinmesi-Talebinin-Yerine-Getirilmemesi (E.T.: 16.09.2024).

[167] Hakkında hüküm verildiği suçtan dolayı cezası infaz edilen ilgili kişiye ait haberin yayımlandığı gazetenin internet sitesinden kaldırılması talebi" hakkında Kişisel Verileri Koruma Kurulunun 22/05/2020 tarihli ve 2020/414 sayılı Karar Özeti: https://kvkk.gov.tr/Icerik/6915/2020-414 (E.T.: 16.09.2024).

yurt dışında yaşadığı bir olay nedeniyle internet yayınlarında adı ve soyadının geçtiğini ve bu haberlerin Google arama motoru sonuçlarında göründüğünü belirtmiştir. Haberin 2009 yılına ait olduğunu ve cezanın infaz edildiğini ifade ederek, haberin müvekkilinin özel hayatına zarar verdiğini belirterek haberlerin kaldırılması için başvuru yapmıştır. Kurul'un yaptığı değerlendirmeye göre basın özgürlüğü ve kişilik hakları karşı karşıya geldiğinde, haberin kamu ilgi ve yararı taşıması, gerçek ve güncel olması, öz ile biçim arasındaki dengenin korunması kriterlerine göre değerlendirilmesi gerekmektedir. Haber, insan kaçakçılığı suçunu işleyen failler hakkında olduğundan toplumun bu haberi alma ve bilgilendirilme hakkı bulunmaktadır. Haberin gerçek ve güncel olması kriteri ise haberin verildiği tarihte kamu yararının bulunması ve haberde geçen olayın doğruluğunun kanıtlanmış olması anlamına gelir. Biçim ve öz arasındaki denge ise haberin veriliş biçiminin gerekli ve ilgili olmayan beyan ve değerlendirmelerin bulunmaması gerektiğini ifade etmektedir. Sonuç olarak, Kurul ilgili kişinin verilerinin haberde yayımlanmasının hala kamu yararı taşıdığını değerlendirmiş ve bu kapsamda ifade özgürlüğünün kişilik haklarına üstün geldiğine hükmetmiştir.

### b) Dijital Platformlarda Unutulma Hakkının Kullanımı

Unutulma hakkının dijital platformlarda uygulanması yukarıda anılan Kurul kararları, Unutulma Hakkı Rehberi başta olmak üzere belirli sınırlamalara tabidir. İlgili kişinin kamusal yaşamdaki statüsü, bilginin mahiyeti, kaynağı ve yayımlanmasından sonra aradan geçen zaman bu hakkın uygulanmasında önemli kriterlerdir.[168]

Kurul'un 23/06/2020 tarihli ve 2020/481 sayılı Karar Özeti'nin ekinde arama motorları üzerinden kişilerin ad ve soyadı ile yapılan aramalarda çıkan sonuçların indeksten çıkarılması sırasında dikkate alınacak ve her somut olay özelinde değerlendirilecek kriterler belirlenmiştir.[169]

[168] Yavuz, s. 173.
[169] İlgili kriterler için bkz. https://kvkk.gov.tr/SharedFolderServer/CMSFiles/68f1fb19-5803-4ef8-8696-f938fb49a9d5.pdf (E.T.: 16.09.2024).

Bu kriterler somut olay özelinde arama motorlarına yönelik belirtilmiş olsa da diğer dijital platformlarında uygulamalarında benimsemesi önemlidir. Değerlendirilmesi gereken kriterler şöyledir;

- **Kamusal Yaşamdaki Sosyal Statü Önemlidir:** Dijital platformlar, kamusal yaşamda önemli rol oynayan kişilerin bilgilerine erişimde daha fazla kamu yararı olduğunu göz önünde bulundurmalıdır.[170] Örneğin eski bir cumhurbaşkanının, milletvekilinin, futbolcunun kamusal hayatta önemli rol oynadıkları kabul edilmektedir.[171]

Burada kamusal yaşamda önemli rol oynayan kişiler "kamuya mal olmuş kişi" kriterinden daha geniş bir şekilde yorumlanmalıdır. [172]

Mesela bir dijital platformda ünlü bir siyasetçi hakkında yıllar önce yapılan yolsuzluk iddialarına dair haberler bulunuyorsa, bu kişinin kamuoyu tarafından tanınan ve kamusal yaşamda önemli rol oynayan bir kişi olması sebebiyle bu haberlerin kaldırılması talebi reddedilebilir. Ancak, siyasetçinin kişisel aile yaşamına dair bilgiler arama sonuçlarından kaldırılabilir.

- **Arama Sonuçlarının Çocuğa İlişkin Olması:** Kendisine ait verisi yayınlanan ilgili kişi o sırada reşit değilse[173], bu arama sonuçlarına ilişkin bağlantının kaldırılması talebinin kabul görmesi daha yüksek bir ihtimaldir.[174]

Bir dijital platformda reşit olmayan bir çocuğun adı geçiyor ve çocuk hakkında bir haber buluyorsa çocuğun üstün yararı gözetilerek bu haberlerin arama sonuçlarından kaldırılması talebi kabul edilebilir.

---

[170] Yavuz, s.173.
[171] Unutulma Hakkı Rehberi, s.28.
[172] Madde 29 Çalışma Grubu, Guidelines on The Implementation Of The Court Of Justice Of The European Union Judgment On "Google Spain And Inc V. Agencia Española De Protección De Datos (Aepd) And Mario Costeja González, s. 13-14. https://ec.europa.eu/newsroom/article29/items/667236/en (E.T.: 16.09.2024).
[173] 4721 sayılı Türk Medeni Kanunu madde 11 uyarınca "*Erginlik onsekiz yaşın doldurulmasıyla başlar. Evlenme kişiyi ergin kılar".* Madde 12: "*Onbeş yaşını dolduran küçük, kendi isteği ve velisinin rızasıyla mahkemece ergin kılınabilir."*
[174] Unutulma Hakkı Rehberi, s.29 ve ayrıca Yavuz, s.178.

- **Bilginin İçeriğinin Doğruluğu**: Bilginin yanlış veya yanıltıcı olması halinde yapılan başvuruların kuvvetle muhtemel kabul edilecektir.[175] Kendisi hakkında yanlış veya yanıltıcı bilgi yayınlandığını iddia eden ilgili kişi, iddiasını ispatla yükümlüdür. [176]

Bir dijital platformda yer alan haberin gerçek olmadığı ve kişinin itibarı hakkında yanlış izlenim oluşturduğu iddia ediliyorsa, haberin yanlış olduğunun ispat edilmesi halinde arama sonuçlarından kaldırılması talebi kabul edilebilir.

- **Bilginin Özel Hayata mı Yoksa İş Hayatına mı Yönelik Olduğu:** Bir kişiye ait her türlü veri kişisel veri olarak kabul edilirken bu veriler kişinin özel hayatına ilişkin olmayabilir.[177] Bilgilinin ilgili kişinin özel hayatına değil iş hayatına ilişkin olması halinde bu bilgiye ilişkin arama motorlarındaki bağlantısının kaldırılması talebinin kabul edilme ihtimali yükselmektedir.[178]

Örneğin bir dijital platformda bir doktor hakkında mesleki hatalarıyla ilgili bir haber bulunuyorsa, bu haber doktorun iş yaşamıyla ilgili olduğundan ve kamunun bilgi edinme hakkı bulunduğundan kaldırılmasının talebi reddedilme ihtimali daha yüksektir.

- **Bilginin Niteliği:** Eğer arama motorlarına yapılan içerik suç niteliği taşıyorsa, örneğin hakaret veya onur kırıcı ifadeler içeriyorsa, bu bağlantıların kaldırılması için yapılan başvuru reddedilirse mahkemeler vasıtasıyla çözümü kavuşturulması daha doğrudur.[179]

- **Bilginin Özel Nitelikli Kişisel Veri Olup Olmadığı**: Özel nitelikli kişisel veri doğası gereği daha fazla koruma gerektirmektedir. Bu doğrultuda eğer kamuya mal olmuş kişilerin özel nitelikli kişisel verilerine erişilmesi halinde bilgilere erişimdeki toplumun menfaati daha dikkatli bir şekilde

[175] Yavuz, s.176.
[176] Unutulma Hakkı Rehberi, s.29.
[177] Yavuz, s.175,176.
[178] Unutulma Hakkı Rehberi, s.30.
[179] Unutulma Hakkı Rehberi s.31, ayrıca Yavuz, s.177.

değerlendirilmelidir. Bu bilgilerde KVKK kapsamında yapılan özel nitelikli kişisel verilerin yanı sıra öğrenilmesinde ilgili kişinin zarara uğraması yüksek olan adres, telefon numarası, banka bilgileri gibi kişisel veriler için de önem arz etmektedir. [180]

- **Bilginin Güncel Olup Olmadığı:** İçeriğin konu ile ilgisinin hala mevcut olması önemlidir. Eğer artık ilişki kalmadı ve tüm bağ sona erdiyse indeksten çıkarma talebinin kabul edilme ihtimali artacaktır. [181]

- **Bilginin Önyargı Oluşturacak Nitelikte Olması:** Eğer bir bilgi kişi hakkında önyargıya sebep oluyor ve bunu iddia eden kişi kanıtlayabiliyorsa, bağlantının kaldırılması daha muhtemeldir.[182]

- **Bilginin Oluşturduğu Risk:** Toplumun erişebildiği bilgiler kimlik hırsızlığı gibi kişi aleyhine risk oluşturuyorsa kaldırılması ihtimali daha yüksektir. [183]

- **Bilgisi Yayınlayan Taraf Kişinin Kendisi ise:** Bilgi eğer ilgili kişinin kendisi tarafından veya açık rızası ile yayınlanmışsa ve kendileri kaldırabilecek durumdaysa yapacakları bu talebin kabul görme ihtimali düşüktür.[184]

- **Gazetecilik Faaliyetleri Kapsamında İşlenen Veri İçermesi:** Kamuoyunun arama sonuçlarına erişiminin sağlamak önemlidir. Ancak bu, bireylerin özel ve aile hayatlarını korumak için belirlenen sınırların ihlal edilmemesini de gerektirir. Bu tür durumlarda, gazetecilik içerikleriyle ilgili arama sonuçlarının kaldırılması da mümkün olabilir. Bu nedenle, her başvuruda arama sonuçlarına toplumun erişmesinde menfaati ile ifade özgürlüğü kapsamında basın özgürlüğü arasında bir denge kurulması gerekecektir. [185]

[180] Unutulma Hakkı Rehberi, s.31-32.
[181] Yavuz, s.183-186.
[182] Unutulma Hakkı Rehberi s.32.
[183] Unutulma Hakkı Rehberi s. 33.
[184] Unutulma Hakkı Rehberi s.33.
[185] Unutulma Hakkı Rehberi s.34-35.

- **Yasal Bir Zorunluluk Gereği Bilgilerin Yayınlanmasının:** Eğer bir kamu kurumu veya yasal yetkili bir kuruluş tarafından kişisel verilerin yayımlanması zorunlu kılınıyorsa ve bu zorunluluk hala geçerli ise, bu durum ilgili kişilerin ad ve soyadları ile arama motorları üzerinden yapacakları arama sonuçlarının kaldırılması taleplerinin olumsuz değerlendirilmesine yol açacaktır.[186]

- **Bilginin Bir Suça İlişkin Olması:** Arama sonuçlarında ilgili kişinin daha önce işlediği bir suç yer alıyorsa ve suç tarihi çok eski tarihliyse, daha yakın bir zamanda işlenen suçlara göre kaldırılma ihtimali daha yüksektir. Ayrıca, nispeten daha ağır bir suç yerine daha hafif nitelikteki bir suç ile ilgili arama sonuçlarının kaldırılması da daha muhtemeldir. [187]

### 2.5.3.4. Veri İşleme Faaliyetini Kısıtlama Hakkı

Kısıtlama hakkı, KVKK'da açıkça düzenlenmeyen ancak GDPR madde 18 uyarınca düzenlenen haklardan birisidir. Bu hak ile veriler üzerinde gerçekleştirilebilecek tehlikeli durumların önlenmesi amaçlanır. [188]

GDPR madde 18 kapsamında bu hak, ilgili kişinin aşağıdaki hallerden birinin varlığı halinde, veri sorumlusundan işleme faaliyetinin kısıtlanmasını talep edebileceğini düzenlemektedir. Bu haller şu şekildedir:

i. Kişisel verilerin doğruluğu ilgili kişi tarafından sorgulandığında ve veri sorumlusunun kişisel verileri doğrulamak için süreye ihtiyacının olması halinde;

ii. Veri işleme faaliyetinin yasadışı olması ve ilgili kişi kişisel verilerin silinmesine karşı çıkıyor ve kullanımlarının kısıtlanmasını talep etmesi halinde;

[186] Unutulma Hakkı Rehberi s.36.
[187] Unutulma Hakkı Rehber, s.36.
[188] Dülger, s.378.

iii. Veri sorumlusunun kişisel verileri işleme amacının sona ermesi halinde, ancak ilgili kişinin hukuki iddialarının oluşturulması, kullanılması veya savunulması için gerekmesi halinde;

iv. İlgili kişinin, bir veri işleme faaliyetine itiraz etmiş olması halinde veri sorumlusunun meşru nedenlerinin ilgili kişinin nedenlerine ağır basıp basmadığını tespit edene kadar bir süre gerekmesi halinde.

Dijital platformlar bakımından ise GDPR'da yer alan bu hak her ne kadar KVKK uyarınca ayrıca belirtilmemişse de uygulanması KVKK düzenlemelerinin doğal bir sonucu olduğundan önem arz etmektedir.

#### 2.5.3.5. Üçüncü Taraflara Bildirim Yükümlülüğü

Bildirim yükümlülüğü, düzeltme ve silinme hakları ile bağlantılıdır. İlgili kişinin kişisel verilerin işlenmesi sırasında yapılan hata veya eksikliklerin düzeltilmesini talep ettiğinde veya silinmesini talep hakkını kullandığında bu taleplerin aynı zamanda verilerin aktarıldığı diğer taraflara bildirilmesini talep etme hakkıdır.

KVKK lafzına göre bildirimi isteme hakkı ilgili kişiye tanınan bir menfaat olarak düzenlenmiştir. Dolayısıyla bu hakkın ilgili kişi tarafından kullanılması halinde veri sorumlusu tarafından yerine getirilmesi gereken bir yükümlülük olacaktır.[189]

Bazı durumlarda bu talebin karşılanması imkânsız veya beklenenden çok daha fazla aşırı bir çaba gerektirebilir. Bu takdirde GDPR'ın 19. maddesinde düzeltme işlemlerinin ancak işlemin imkânsız olmaması veya ölçüsüz bir çaba gerektirmemesi halinde yapılabileceği düzenlenmiştir.[190]

Dijital platformlar da öncelikle ilgili kişinin düzeltme ve silinme haklarının

[189] Krş. Dülger, s.360.
[190] Dülger, s. 360.

yerine getirilmesinin uygun olması halinde ve üçüncü taraf alıcılara bildirilmesinin talep edilmesi halinde bildirim yükümlülüğünü yerine getirmelidir. Bunu yerine getirirken de işlemin imkânsız olup olmadığı veya ölçüsüz bir çaba gerekip gerekmediğini değerlendirmesi gerekmektedir.

#### 2.5.3.6. KVKK Kapsamında Dijital Platformlarda Veri Taşınabilirliği

Veri taşınabilirliği hakkı, GDPR'da düzenlenmiş, ancak KVKK kapsamında yer almayan bir haktır. GDPR'a göre bu hak, ilgili kişinin veri sorumlusuna sağladığı kişisel verileri belirli koşullar altında alabilmesini ve bu verileri, mevcut bir sözleşmeye dayalı olarak veya kişinin açık rızasıyla gerçekleştirilen işlemlerde otomatik araçlarla işlendiği durumlarda başka bir veri sorumlusuna aktarmayı içermektedir. Bu hak kullanılırken, ilgili kişi kişisel verilerin teknik olarak mümkün olduğunda doğrudan bir veri sorumlusundan diğerine aktarılmasını talep etme hakkına sahiptir.

Türkiye'de veri taşınabilirliği hakkı hukukun farklı alanlarında değerlendirilmektedir. Rekabet hukuku bakımından iktisadi amaçlar kapsamında değerlendirilmekte ve teşebbüsler tarafından kişisel veri olup olmadığı fark etmeksizin verilerin paylaşma yükümlülüğü birçok karara konu olmuştur.[191] E-pazaryeri Platformları Sektör Raporu kapsamında rekabet hukuku sorunu olarak değerlendirilen üç temel başlıktan birisi veri taşıma ve veriye erişim hakkı olarak belirtilmiştir. Önemle belirtmek gerekir ki rekabet hukuku konusuna da giren veri, dijital pazar yerlerinde satış yapan satıcıların her türlü verisidir bu bilgiler; tüketiciden gelen talepten, talepteki değişime, tüketici tercihlerine oldukça kapsamlı verileri içermektedir.

Elektronik Ticaret Hizmet Sağlayıcılar Hakkında Yönetmelik[192] ek madde 2/2 (b) kapsamında da veri taşınabilirliği hakkı düzenlenmektedir. Bu düzenleme elektronik ticaret hizmet sağlayıcıları ile elektronik ticaret aracı hizmet

[191] Rekabet Hukuku Çerçevesinde Veri Taşınabilirliği ve Dijital Platformların Veri Paylaşma Yükümlülüğü: https://www.youtube.com/watch?v=Eld7dTJfCQI (E.T.: 16.09.2024).
[192] RG: 12.09.2022, 32058.

sağlayıcıları arasındaki ilişkiye odaklanmaktadır. Buna göre, elektronik ticaret hizmet sağlayıcıları, elektronik ticaret aracı hizmet sağlayıcılarına veri taşınabilirliği ve erişim taleplerine 15 gün içinde yanıt vermek zorundadır. Veri taşınabilirliği kapsamında sunulan bilgiler şunlardır; *satışa sunulan ürünlerin satış ve iade verileri, özellikleri, açıklamaları ve görselleri, bu ürünlere ilişkin soru, cevap ve değerlendirmeler, elektronik ticaret aracı hizmet sağlayıcı tarafından elde edilen dönemsel, özel gün, kategori ve ürün bazlı en çok tercih edilen ürün verileri, alıcıların cinsiyet, yaş grubu, il ve ilçe dağılımı ile satın alma gün ve saatleri, elektronik ticaret hizmet sağlayıcının performansına ilişkin değerlendirme puanı, elektronik ticaret aracı hizmet sağlayıcı tarafından elektronik ticaret hizmet sağlayıcının ürünü için verilerin ve elektronik ticaret pazar yerinde yer alan ürünleri ayırt etmeye yarayan tekilleştirilmiş numara.*

Türk hukukunda kişisel verilere ilişkin çalışmalar, Avrupa'daki düzenlemelere kıyasla gecikmiş durumdadır. Ancak bu gecikme, AB'deki mevcut sistemlerin incelenmesi ve bu deneyimlerden faydalanma şansı da sunmuştur. KVKK'nın hazırlık sürecinde, o dönemde yürürlükte olan 95/46/EC Kişisel Verilerin İşlenmesi ve Bu Tür Verilerin Serbest Dolaşımına Dair Bireylerin Korunması Direktifi ("**95/46/AT sayılı Direktif**") esas alınmıştır.[193] Ancak, 95/46/AT sayılı Direktif'te veri taşınabilirliği hakkı düzenlenmemiş olduğundan KVKK'da da neden yer almadığı anlaşılmaktadır.[194]

Zamanlama olarak GDPR'ın da hazırlık dönemine denk geldiğinden Kurul'un GDPR düzenlemelerinden ve veri taşınabilirliği hakkından haberdar olmadığı söylenemeyecektir. Kurul'un 19.11.2018 tarihli 2018/131 sayılı Karar Özeti[195] kapsamında da doğrudan veri taşınabilirliği hakkını yok saymadığını görüyoruz. Karar kapsamında bir tüzel kişiliğe ait elektronik ortamda bulunan

[193] Dülger, s.73.
[194] **YILMAZ Beste Ekin**, Kişisel Verilerin Korunması ve Rekabet Hukuku Bağlamında Veri Taşınabilirliği Hakkı, Baskı, 1 Ocak 2023, İstanbul, On İki Levha Yayıncılık s.12.
[195] "Tüzel kişiliğe ait elektronik ortamda yer alan verilerin başka bir tüzel kişilik tarafından talep edilmesi" hakkında Kişisel Verileri Koruma Kurulunun 19/11/2018 tarihli ve 2018/131 sayılı Kararı Özeti: https://www.kvkk.gov.tr/Icerik/5423/2018-131 (E.T.: 16.09.2024).

verilerin, başka bir tüzel kişi tarafından talep edilmesi durumu incelenmektedir. Kurul tarafından tüzel kişiliğe ait verilerin kişisel veri niteliğinde olmadığından KVKK kapsamında bulunmadığı belirtilmekle birlikte KVKK madde 11'de düzenlenen hak olan her gerçek kişinin veri sorumlusuna başvurarak herhangi bir kişisel verisinin işlenip işlenmediğini öğrenme, eğer işlenmişse buna ilişkin bilgi talep etme hakkına sahip olduğunun altı çizilmiştir.

Ek olarak şirketin ortağı ve yetkilisinin gerçek kişilere ilişkin kişisel verilere erişim sağlanması talebinin reddedilme sebebi ise bu erişimi talep edecek tarafın kişisel veri sahibinin kendisi olan ilgili kişi olabileceğinde KVKK madde 11 kapsamında değerlendirilemeyeceği belirtilmiştir. Bu karardaki yaklaşımdan veri taşınabilirliği hakkının KVKK'nın 11. maddesinde düzenlenen erişim hakkı kapsamında değerlendirildiğini anlıyoruz.

Dijital platformlar bakımından ise bu hakkın Türk hukukunda uygulama alanı olmadığının değerlendirilmesi kişisel verilerin üzerinde ilgili kişilerin kontrol yetkisini kısıtlayıcı nitelikte olacaktır. Bu sebeple dijital platformların, kullanıcıların kendi verilerine erişim sağlamalarını kolaylaştırmaları, buna imkân tanıyacak mekanizmaları kurmaları önemlidir. Bu mekanizmaları sağlarken kullanıcıların kişisel verilerini başka bir platforma taşımalarını kolaylaştıracak araçlar sunabilirler. Böylece, kullanıcıların verilerini yapılandırılmış ve yaygın kullanılan formatlarda indirmelerini ve başka bir platforma aktarmalarını sağlayabilirler.[196] Ayrıca aydınlatma yükümlülüğü kapsamında dijital platformlar, kullanıcıların sahip olduğu bu hakka ve nasıl kullanabileceklerine ilişkin bilgi sunabileceklerdir.

#### 2.5.3.7. İtiraz Hakkı

İtiraz hakkı, GDPR kapsamında öngörülmüşse de KVKK uyarınca düzenlenmemiştir. Özü itibariyle bu hak KVKK'nın genel düzenlemelerinin doğal bir sonucudur.[197] Bu sebeple her ne kadar KVKK kapsamında ayrı bir hak olarak

[196] Teknik açıdan uygulanmasına ilişkin daha fazla bilgi için bkz. Yılmaz, s.25.
[197] Dülger, s.361.

düzenlenmemişse de bu konuda başvuru alındığında dijital platformların diğer hakları da göz önünde bulundurarak değerlendirmesi önemlidir.

İtiraz hakkı, ilgili kişiye ait özel bir durumun olması sebebiyle kişisel verilerinin işlenmesine herhangi bir zaman sınırı olmaksızın itiraz edebilmesidir. Bu haller GDPR madde 21'in devamında belirtilmektedir.

İlk hal doğrudan pazarlama yürütülmesi amacıyla işlenmesi halinde ilgili kişinin herhangi bir zamanda profilleme de yapan bu pazarlama faaliyetine itiraz edebilmesidir. Bu şekilde bir itirazın yapılması halinde kişisel verilerin doğrudan pazarlama amacıyla işlenmemesi gerekir. Türkiye'de doğrudan veya dolaylı pazarlama faaliyeti ayrımı yapılmaksızın pazarlama faaliyetleri prensip olarak açık rızanın varlığını gerektirmektedir. GDPR madde 21 kapsamında pazarlama amacıyla veri işleme faaliyetine yapılacak itiraz KVKK uyarınca açık rızanın geri alınması olarak değerlendirilebilecektir.

Pazarlama amacının yanı sıra kişisel veriler, bilimsel veya tarihsel araştırma amaçları veya istatistiksel amaçlar çerçevesinde işleniyorsa, ilgili kişi, kendine ait özel durumuna dayanarak, kişisel verilerinin işlenmesine itiraz etme hakkına sahiptir. Ancak bu işleme faaliyeti, kamu yararı için gerçekleştirilen bir görevin yerine getirilmesi için gerekliyse itiraz edilemeyecektir.

#### 2.5.3.8. Otomatik Veri İşleme Faaliyetine Yönelik Haklar

Otomatik veri işleme faaliyeti, herhangi bir insan müdahalesi olmaksızın otomatik yollarla kişisel verilerin işlenmesidir. Örnek olarak kredi vermeye yönelik otomatik yollarla verilen bir karar veya önceden programlanmış algoritmalar ve kriterler kullanılarak yürütülen bir işe alım yetenek testi verilebilir.[198]

Hem GDPR kapsamında hem de KVKK uyarınca benzer şekilde düzenlense de GDPR'da daha kapsamlı bir şekilde ele alınan bir haktır. Bu doğrultuda ilgili kişilerin sadece otomatik işleme dayalı bir karara tabi tutulmama hakkı

[198] Guide to the General Data Protection Regulation, s.102.

düzenlemiştir. Bu otomatik işleme kavramı profil oluşturmayı (*profiling)*[199] kapsamaktadır.

Aşağıdaki durumlardan birisinin varlığı durumunda otomatik işleme faaliyetine yönelik bu itiraz hakkı kullanılamayacaktır;

a) veri işleme faaliyeti sonucu elde edilen karar ilgili kişi ile veri sorumlusu arasında bir sözleşmenin kurulması veya ifası için gerekli ise;

b) veri işleme faaliyeti sonucu elde edilen kararın, ilgili kişinin hak ve özgürlüğü ile meşru menfaatini korumak için gereken tedbirlerin sağlanması kapsamında bir yasaya dayanması halinde;

c) veri işleme faaliyeti sonucu elde edilen karar ilgili kişinin açık rızasını dayanıyor ise.

Otomatik veri işleme sonucu elde edilen karara itiraz edebilmek için, kararın sadece otomatik veri işleme sonucu elde edilmiş olması yeterli değildir; aynı zamanda, kararın ilgili kişi üzerinde önemli etkilere sahip olması da gereklidir. KVKK otomatik kararlardan bahsedilirken, kararın ilgili kişiye olumsuz sonuçlar doğurabileceği vurgulanmıştır. Ancak, bu hüküm, GDPR ile uyumlu olarak, olumsuz sonuçlar doğurabilecek önemli etkilere yol açabilecek şekilde yorumlanmalıdır.[200]

Dijital platformlarında hak kapsamında, gerektiğinde münhasıran otomatik müdahaleyi sona erdirerek insan müdahalesinde bulunabilecek şekilde ve otomatik veri işleme faaliyeti sonucu elde edilen karara itiraz etme hakkını içeren gerekli mekanizmaları kurması gerekmektedir.

[199] GDPR madde 4 uyarınca profil oluşturma kavramı *(profiling)* kişisel verilerin otomatik olarak işlenmesinin bir türüdür ve bu işlem, gerçek bir kişiyle ilgili belirli kişisel yönleri değerlendirmek amacıyla kişisel verilerin kullanılmasını içerir. Özellikle, bu işlem, bir kişinin iş performansı, ekonomik durumu, sağlık durumu, kişisel tercihleri, ilgi alanları, güvenilirliği, davranışları, konumu veya hareketleri hakkında analiz yapmak veya tahminde bulunmak için kullanılabilir.
[200] Dülger, s.381.

#### 2.5.3.9. Zararın Giderilmesini İsteme Hakkı

GDPR kapsamında düzenlenmemiş olan bu hak, kişisel verilerin hukuka aykırı bir şekilde işlenmesi halinde ilgili kişi nezdinde bir zarar doğdu ise bu zararın telafi edilmesini talep edebileceğini içermektedir. Bu hak, zaten genel tazminat hükümlerine dayanarak var olan bir haktır. Ancak, KVKK veri koruma sistemini kurarken, tazminat talebini denetim ve yaptırım sisteminin bir parçası olarak düzenlemiştir. Bu, ilgili kişinin zaten sahip olduğu genel sorumluluk hukuku çerçevesindeki bu hakkı, ayrı bir hak olarak güçlendirmeyi amaçlamaktadır.[201]

[201] Dülger, s.382.

# ÜÇÜNCÜ BÖLÜM
# DİJİTAL PLATFORMLARDA KİŞİSEL VERİ GÜVENLİĞİ

## 3.1. DİJİTAL PLATFORMLARDAKİ KİŞİSEL VERİLERİN GÜVENLİĞİ

Dijital platformlar, modern toplumun olmazsa olmaz bir parçası haline gelmiş durumdadır. Günlük aktivitelerimizin birçoğunu kolaylaştıran bu platformlar, iletişimden alışverişe, eğlenceden hizmet satın alımına kadar geniş bir yelpazede hizmet sunmaktadır. Kişilerin hayatlarına dokunduğu alanların hacmi arttıkça, elde ettiği kişisel veriler de artmıştır.

Bu bölümde, dijital platformlardaki kişisel veri güvenliği konusu ele alınacaktır. Özellikle, platformlardaki kişisel verilerin güvenliği için alınabilecek teknik ve idari tedbirler, Kurul kararları doğrultusunda mahremiyet endişeleri ve kişisel veri ihlal bildirimleri incelenecektir.

### 3.1.1. Alabileceği Teknik ve İdari Tedbirler

Bir dijital platformun kişisel veri güvenliğini sağlaması, günümüzün en önemli konularından biridir. Bu gerekli teknik ve idari tedbirlerin alınması ve politikaların uygulanması kullanıcıların kişisel veri mahremiyetinin korunması açısından büyük önem taşımaktadır.

KVKK'da kişisel verilerin güvenliği oldukça geniş bir ifade ile 12. madde altında düzenlenmiştir. Maddenin lafzından anlaşıldığı üzere her veri sorumlusunun kendi denetimini yaparak kendi ihtiyaçları doğrultusunda gerekli olan teknik ve idari tedbiri belirlemesi gerekmektedir. Bu kapsamda veri sorumlularının öncelikle kendi ihtiyaçlarını diğer bir deyişle potansiyel risk yaratabilecek noktalarını belirlemelidir. Daha sonrasında bu riskleri bertaraf etmek üzere gereken aksiyonu alması gerekmektedir.

Küresel düzlemde veri güvenliğine ilişkin standartlar sağlamaya yönelik olarak Uluslararası Standardizasyon Kurumu (*International Organization for*

*Standardization, "**ISO**")* ve Uluslararası Elektronik Komisyonu'nun ("**IEC**") iş birliği ile "Bilgi Teknolojileri – Güvenlik Teknikleri – Gizlilik Çerçevesi" ISO/IEC 29100 Standardı ("**ISO 29100**")[202] hazırlanmıştır. Bu standart ile veri güvenliğine ilişkin olarak ortak bir kriter geliştirilmesi ve iyileştirilmesi amaçlanmıştır. Temel amaçlar; sistemlerin tasarı, uygulamaya geçiş ve kullanım aşamalarındaki güvenliğin sağlanması, veri güvenliğine yönelik yenilikçi çözümlerin geliştirilmesi ve örnek uygulamalar ile kuruluşların veri güvenliği standartlarını geliştirmektedir. ISO ve IEC tarafından hazırlanan diğer standart ise ISO/IEC 27001 ve ISO/IEC 27002'ye ek – Gereklilikler ve rehber standardıdır (ISO 27701). Bu standart da benzer şekilde veri güvenliği için uyulması gereken bazı standartları düzenlemekte ve bunu yaparken de GDPR'a atıf yapmaktadır. Bu standartlar yerel mevzuat ile düzenlenen teknik ve idari tedbirlere tamamlayıcı niteliktedir.[203]

Türk veri hukukunda ise kanun koyucunun burada geniş bir ifade ile düzenleme yapmış olması oldukça yerindedir. Zira gelişen teknolojilerde, aynı hızda siber saldırganlar ve siber olaylar da kendini geliştirmektedir. Sabit yükümlülüklerle sınırlı olmaksızın veri sorumlusuna kendi kendini düzenli denetim yükümlülüğü getirmesi, veri güvenliğine ilişkin alınacak tedbirlerin beklentisini de artırmaktadır.

Her ne kadar kanun koyucu veri güvenliği için alınacak tedbirleri belirli standartlar ile sınırlamasa da uygulamada yol göstermek adına Kurul tarafından Kişisel Veri Güvenliği Rehberi[204] hazırlanmıştır. Dijital platformların kendi denetimini ve ihtiyaçlarına göre gerekli tedbiri belirlerken bu rehber yol gösterici nitelikte olacaktır. Bu rehberin yanı sıra Kurul kararları da hangi kişisel veri güvenliği tedbirlerin alınması gerektiğinde önemli bir kaynaktır.

---

[202] https://www.iso.org/standards.html (E.T.: 16.09.2024).
[203] Leyla Keser Berber, Ali Cem Bilgili, Güncel Gelişmeler Işığında Kişisel Verilerin Korunması Hukuku, 2020, On İki Levha Yayıncılık, 1. Baskı, İstanbul, s.1,2.
[204] Kişisel Verileri Koruma Kurumu, Kişisel Veri Güvenliği Rehberi (2018), KVKK Yayınları, Ankara https://www.kvkk.gov.tr/SharedFolderServer/CMSFiles/7512d0d4-f345-41cb-bc5b-8d5cf125e3a1.pdf (E.T.: 16.09.2024).

Teknik ve idari tedbirlerin uygulanmasının yanı sıra bu uygulamanın takip edileceği ve bu süreci yürütecek şekilde dijital platformlar bünyesinde veri güvenliğinden sorumlu olacak belirli bir kişi veya kişilerin seçilmesi faydalı olacaktır. Böylece veri güvenliği düzenli olarak denetlenerek herhangi bir ihlalin gerçekleşme riskinin önüne geçilebilecektir.[205]

#### 3.1.1.1. İdari Tedbirler

Kişisel veri güvenliğinin temin edilmesi adına gerekli her türlü teknik ve idari tedbir alınmalıdır. İdari tedbirler, kurum içerisinde genelde hukuk, kurumsal ilişkiler, insan kaynakları departmanı gibi birimlerin dahil olması ile uygulanmaktadır. Hangi tedbirin gerektiğine ilişkin öncelikle dijital platformun denetim yapması gerekse de Kişisel Veri Güvenliği Rehberi kapsamında alınması gereken, neredeyse her veri sorumlusu için gerekli olan tedbirler düzenlenmiştir.

**a) Kişisel Veri İşleme Envanteri**

Kişisel veri güvenliğinin sağlanabilmesi için öncelikle veri sorumlularının mevcut risk ve tehditleri belirlemesi gerekmektedir. Bunun için de öncelikle veri sorumlusunun işlediği bütün kişisel verilerin eksiksiz bir şekilde belirlenmesi gerekmektedir.[206] Bu kişisel verilerin neler olduğu, genel veya özel nitelikli olduğu, hangi derecede gizlilik seviyesi gerektirdiğini sistematik bir şekilde belirlemek için kişisel veri işleme envanterinin hazırlanmasına ilişkin tedbir uygulanabilecektir.

Kişisel veri işleme envanterinin hazırlanmasına ilişkin tedbirler, aslında Veri Sorumluları Sicili Hakkında Yönetmelik madde 5 uyarınca VERBİS'e kayıt yükümlülüğü altında olan veri sorumluları bakımından düzenlenmiştir. Aynı Yönetmeliğin 2. maddesini birinci fıkrasının (h) bendinde kişisel veri işleme envanteri şu şekilde tanımlanmıştır; "*veri sorumlularının iş süreçlerine bağlı olarak gerçekleştirmekte oldukları kişisel veri işleme faaliyetlerini; kişisel veri*

[205] Dülger, s.407.
[206] Kişisel Veri Güvenliği Rehberi s.8.

*işleme amaçları ve hukuki sebebi, veri kategorisi, aktarılan alıcı grubu ve veri konusu kişi grubuyla ilişkilendirerek oluşturdukları ve kişisel verilerin işlendikleri amaçlar için gerekli olan azami muhafaza edilme süresini, yabancı ülkelere aktarımı öngörülen kişisel verileri ve veri güvenliğine ilişkin alınan tedbirleri açıklayarak detaylandırdıkları envanter".*

Bu doğrultuda bir kişisel veri işleme envanterinde tüm süreçlerin takip edilmesini ve anlaşılmasını sağlayacak tüm bilgiler bulunmaktadır. Kişisel veri işleme envanteri, bir veri sorumlusunun kişisel veri işleme sürecinin haritası niteliğinde olup bütün veri güvenliğine yönelik düzen bu envanter üzerine kurularak takip edilebilecektir. Dolayısıyla, sadece VERBİS'e kaydolma yükümlülüğü altında olan veri sorumlularına yüklenen bir yükümlülük olsa da veri güvenliğinin sağlanması için veri sorumlusunun faaliyeti fark etmeksizin tüm veri sorumluları bakımından temel bir idari tedbirdir. Bu doğrultuda bir dijital platformun mutlaka süreçlerini açıkça tanımlayabilecek ve en az yukarıdaki tanımda yer alan unsurları barındıran bir kişisel veri işleme envanterini hazırlaması ve güncel tutması gerekecektir.

**b) Kurumsal Politika ve Prosedürlerin Belirlenmesi**

Kişisel veri güvenliğinin temin edilmesine amacıyla hazırlanacak kapsamlı bir politika ile risklerin meydana gelmeden önce tespit edilmesi sağlanabilecektir. Böylece, kişisel veri güvenliğini sağlamaya yönelik hazırlanan veri sorumlusuna uygun bir politika veya prosedürün veri sorumlusunun faaliyetlerine uygun bir şekilde dahil edilmesi oldukça önemlidir.[207]

Her veri sorumlusunun ihtiyaçları doğrultusunda hangi politika veya prosedürlerin incelenmesi gerektiği belirlense de her dijital platformun bir saklama ve imha politikasına, özel nitelikli veri işliyorsa bu konuda bir politika veya prosedür belirlemesi ve veri ihlali olması halinde nasıl müdahale edileceğine ilişkin veri ihlali müdahale planına sahip olması gerekir.

[207] Kişisel Veri Güvenliği Rehberi s. 11.

KVKK'nın 7. maddesi uyarınca ve Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi Hakkında Yönetmelik madde 5 uyarınca VERBİS'e kaydolmakla yükümlü olan veri sorumlularının, kişisel veri envanterine uygun olarak kişisel veri saklama ve imha politikası hazırlama yükümlülüğü bulunmaktadır. Bu politika yine aynı yönetmelik kapsamında işlenen kişisel verilerin saklanması için gerekli olan azami sürenin belirlenmesi ve imha işleminin yürütülmesine dayanak niteliktedir. İmha işlemi, veri sorumlusu tarafından belirlenecek en az altı aylık periyodik imha dönemlerinde gerçekleştirilmelidir.

İlgili yönetmelik madde 5 uyarınca VERBİS'e kayıt yükümlülüğü olmadığı için ayrıca anılan politikayı hazırlamaktan da muaf tutulan veri sorumlularının saklama süresinin sonunda kişisel verileri imha etme yükümlülüğü devam etmektedir.

Bir dijital platformun işleyeceği kişisel veri hacmini de göz önünde bulundurarak VERBİS kayıt yükümlülüğü altında olmasa dahi kişisel verileri imha etme yükümlülüğünü eksiksiz bir şekilde ifa edebilmek adına ilgili politikayı hazırlaması önemli bir tedbir olacaktır.

Kurul'un Özel Nitelikli Kişisel Verilerin İşlenmesinde Veri Sorumlularınca Alınması Gereken Yeterli Önlemler ile ilgili Kişisel Verileri Koruma Kurulu'nun 31.01.2018 tarihli ve 2018/10 sayılı kararı[208] kapsamında özel nitelikli veri işleyen veri sorumlularının özel nitelikli kişisel verilerin güvenliğine yönelik sistemli, kuralları net bir şekilde belli, yönetilebilir ve sürdürülebilir ayrı bir politika ve prosedürün belirlenmesi gerektiği belirtilmiştir. Bu sebeple özel nitelikli kişisel veri işleyen dijital platformların mutlaka aldığı diğer tedbirleri de içeren ayrı bir politika ve prosedürünün bulunması gerekmektedir.

Veri ihlali müdahale planı, Kişisel Veri İhlali Bildirim Usul ve Esaslarına İlişkin Kişisel Verileri Koruma Kurulunun 24.01.2019 tarih ve 2019/10 sayılı

[208] "Özel Nitelikli Kişisel Verilerin İşlenmesinde Veri Sorumlularınca Alınması Gereken Yeterli Önlemler" ile ilgili Kişisel Verileri Koruma Kurulunun 31/01/2018 Tarihli ve 2018/10 Sayılı Kararı: https://www.kvkk.gov.tr/Icerik/4110/2018-10 (E.T.: 16.09.2024).

Kararı[209] kapsamında herhangi bir veri ihlali meydana gelmesi durumunda veri sorumlusu bünyesindeki hangi birimlere ve kişilere raporlama yapılacağı, KVKK kapsamında Kurum'a ve ihlalden etkilenen ilgili kişilere yapılacak bildirimleri ve bu ihlalin olası sonuçlarının değerlendirilmesini, sorumluluk belirlemelerinin yapılmasını içerecek şekilde bir planın hazırlanması ve düzenli olarak takip edilmesini gerektirmektedir.[210]

**c) Sözleşmeler (Veri Sorumlusu – Veri Sorumlusu, Veri Sorumlusu – Veri İşleyen Arasında)**

Dijital platformlar, kişisel veri işleme faaliyetlerinde gerek veri sorumlusu gerek veri işleyen pozisyonundaki üçüncü taraflarla iş birliği yaparken veri güvenliğini sağlamak için sözleşme yapması önemli bir tedbir olarak değerlendirilmektedir. Bu sözleşmeler için kritik unsurlar ve uygulanması gereken tedbirler Kişisel Veri Güvenliği Rehberi kapsamında incelenmiştir.

Sözleşmelerdeki karşı tarafın veri işleyen olması halinde yalnızca veri sorumlusundan aldığı talimatlar doğrultusunda hareket etmeli ve işlediği kişisel verilerin gizliliğini sağlamak için uygun teknik ve idari tedbirleri almalıdır. Ayrıca, veri işleme faaliyetinin sona ermesi ile tüm kişisel verileri veri sorumlusuna iade etmeli veya silmelidir.[211]

Sözleşme içeriğinde veri işleme faaliyetine ilişkin konular, süre, amaç ve verilerin türü gibi detayları açıkça belirtmelidir. Örneğin bir e-ticaret pazar yerinin üçüncü taraf analiz şirketlerine kullanıcı verilerini gönderirken veri işleme amacını, süresini mutlaka sözleşmeye eklemelidir. Veri işleyenin, veri ihlali durumunda veri sorumlusuna yardımcı olmakla yükümlü olduğu belirtilmelidir.[212]

---

[209] Kişisel Veri İhlali Bildirim Usul ve Esaslarına İlişkin Kişisel Verileri Koruma Kurulunun 24.01.2019 tarih ve 2019/10 sayılı Kararına İlişkin Duyuru: https://www.kvkk.gov.tr/Icerik/5362/Veri-Ihlali-Bildirimi (E.T.: 16.09.2024).

[210] Veri ihlaline ilişkin veri sorumlusu olarak dijital platformların diğer yükümlülükleri Bölüm 3.3'e bakınız.

[211] Kişisel Veri Güvenliği Rehberi, s.9.

[212] Kişisel Veri Güvenliği Rehberi, s.10-11.

GDPR kapsamında ise veri işleyenler ile yapılan sözleşmelerde belirli yükümlülükler öngörülmektedir.[213] Bu yükümlülükler, veri güvenliği ve şeffaflık ilkelerini sağlamaya yönelik olarak belirlenmiştir. Kişisel Veri Güvenliği Rehberi'ne benzer şekilde işleme faaliyetinin konusunun, süresinin, amacının, türünün ve ilgili veri kategorilerinin açıkça belirtilmesi gerekmektedir.[214] Veri işleyen ver sorumlusunun yazılı talimatlarına göre hareket etmelidir. Ayrıca, veri ihlali durumunda veri işleyen veri sorumlusuna yardımcı olmak ve veri koruma erki değerlendirmelerinde destek sağlamak ile yükümlüdür.[215]

Bu doğrultuda kişisel veri aktarımı halinde üçüncü kişiler ile yapılan sözleşmeler tarafların yükümlülük ve sorumluluklarını belirlemek için önemlidir. Dijital platformların bu kapsamda sözleşme ile veri güvenliğini sağlamaya yönelik tedbirlerin alması gerekmektedir.

**d) Gizlilik Taahhütnameleri**

Dijital platformlar, veri işleme süreçlerinde yer alan çalışanlar, yükleniciler ve diğer ilgili taraflar arasında gizliliği sağlamak amacıyla yapacağı gizlilik taahhütnamelerinin uygulanması diğer bir idari tedbirdir. Bu taahhütnameler kişisel verilerin yetkisiz erişim, ifşa, değişiklik veya imha edilmesini önlemek için alınması gereken idari tedbirler arasından önemli bir yer tutmaktadır.

**e) Kurum İçi Periyodik ve/veya Rastgele Denetimler**

Kişisel Veri Güvenliği Rehberi'nde veri sorumlularının kişisel veri güvenliğini sağlamak için alması gereken her türlü teknik ve idari tedbirlere örnek olarak kurum içi periyodik ve/veya rastgele denetimler verilmiştir. Bu doğrultuda, dijital platformların veri güvenliğini sağlamak ve KVKK uyumluluğunu kontrol etmek amacıyla denetimler gerçekleştirmesi ve aldığı tedbirlerin etkin olup olmadığını değerlendirmesi, olası güvenlik açıklarını tespit etmesi için önemlidir. Bu doğrultuda periyodik ve/veya rastgele olacak şekilde çeşitli stratejiler

[213] GDPR, Madde 28.
[214] GDPR Recital 81.
[215] Bkz. https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/accountability-and-governance/contracts-and-liabilities-between-controllers-and-processors-multi/ (E.T.: 16.09.2024).

uygulanabilecektir.

**f) İnsan Kaynaklarına İlişkin Belgelere Ek Hükümler**

Bir kurum içerisindeki çalışanlar ilgili kişi ve veri sorumlusu bünyesinde veri işleme faaliyetini yürüten kişi olarak iki farklı statüye sahiptir. İlgili kişi olduğu hallerde veri sorumlusu kurum, diğer ilgili kişiler gibi kişisel veri işleme faaliyetlerine yönelik başta aydınlatma yükümlülüğü olmak üzere tüm yükümlülüklerini ifa etmesi gerekmektedir.

Öte yandan, veri sorumlusu bünyesindeki kişisel verilerin güvenliğini sağlayabilmek adına yürütülen veri işleme faaliyetlerindeki insan unsuruna ilişkin gerekli yükümlülük ve sorumlulukları belirleyerek olabilecektir. Bu doğrultuda iş sözleşmesi ve disiplin yönetmeliklerinde çalışanların kişisel verilerin korunması konusunda uymaları gereken kurallar ve bu kurallara uyulmaması durumunda uygulanacak yaptırımlar açık ve net bir şekilde belirtilmelidir.

**g) Kurumsal İletişim**

Kurumsal iletişim, dijital platformların kişisel verilerin korunmasına yönelik aldıkları idari tedbirler arasında kritik bir öneme sahiptir. Bu süreç, kriz yönetimi, Kurul ve ilgili kişiyi bilgilendirme süreçleri ve itibar yönetimi gibi unsurları kapsamaktadır.

Kriz yönetimi, sürecin etkin bir şekilde çözüme kavuşturulması olarak değerlendirilebilecektir. Veri ihlalinin tespit edilmesi, etkilerinin minimize edilmesi ve benzer olayların önlenmesi için alınacak önlemleri içerir. Kriz yönetimi, kişisel verilerin korunmasına ilişkin hızlı aksiyonlar alınması ve aynı zamanda şirketin itibarını koruması için önemlidir. Önemli bir kriz yönetim materyali olarak veri ihlali müdahale planı örnek verilebilir.

Veri ihlali veya benzeri durumlarda Kurum ve ihlalden etkilenen ilgili

kişilerin bilgilendirilmesi gerekmektedir. Kurul'un 2019/10 sayılı Kararı[216] kapsamında bu bilgilendirmenin 72 saat içerisinde Kurum'a ve makul süre içerisinde ilgili kişiye yapılması gerekmektedir. GDPR kapsamında da bu süreler aynı şekilde düzenlenmiştir.[217]

Veri ihlalleri ve sonuçları, dijital platformların itibarını ciddi bir şekilde zedeleyebilmektedir. İtibar yönetimi, bu tür olayların ardından şirket güvenilirliğini yeniden tesis etmeyi amaçlar. Şeffaf iletişim ve proaktif önlemler, müşteri güveninin yeniden kazanılmasında önemli rol oynamaktadır. Örneğin, 2017 yılın Equifax bünyesinde yaşanan veri ihlalinin[218] ardından kapsamlı bir itibar yönetimi stratejisi geliştirilmiş ve müşterilerine sağladığı güvenlik önlemlerini artırmıştır. Bu doğrultuda şirket, veri ihlalinin etkilerini minimize etmek için kullanıcılarına ücretsiz kredi izleme hizmetleri sunmuştur.

Sonuç olarak, kurumsal iletişim stratejileri, dijital platformların veri ihlallerine karşı hazırlıklı olmalarını ve bu tür olaylar karşısında etkin yanıt vermelerini sağlamaktadır.

**h) Eğitim ve Farkındalık Faaliyetleri**

Dijital platformların, kişisel verilerin korunması ve bilgi güvenliğinin sağlanması amacıyla düzenledikleri eğitimleri çalışanların bilinçlenmesini sağalama noktasında kritik öneme sahiptir. Kurul kararlarına baktığımızda, Kurul tarafından veri sorumlularının çalışanlarına her yıl düzenli olarak farkındalık eğitimi vermesi beklenmektedir.[219]

---

[216] Kişisel Veri İhlali Bildirim Usul ve Esaslarına İlişkin Kişisel Verileri Koruma Kurulunun 24.01.2019 Tarih ve 2019/10 Sayılı Kararına İlişkin Duyuru: https://www.kvkk.gov.tr/Icerik/5362/Veri-Ihlali-Bildirimi (E.T.: 16.09.2024).

[217] GDPR madde 33.

[218] Bkz. https://en.wikipedia.org/wiki/2017_Equifax_data_breach (E.T.: 16.09.2024).

[219] Örneğin Kurulun 2020/359 sayılı kararında (https://www.kvkk.gov.tr/Icerik/7028/2020-359) şikayet üzerine veri sorumlusunun kişisel verilerin korunmasına yönelik yeterli tedbirleri almadığı ve bu nedenle veri ihlali yaşandığı iddialarını değerlendirmiştir. İnceleme sonucunda aşağıdaki değerlendirmeler yapılmıştır;"

- *Veri sorumlusu, çalışanlarına kişisel verilerin korunması konusunda düzenli eğitimler vermemiştir.*

İlgili eğitimlerin içeriği, veri sorumlusunun ihtiyaçları doğrultusunda değişebilecektir. Temel olarak veri sorumlusunun kişisel veri koruma politikalarını, dikkat edilmesi gereken tedbirleri, ilgili kişinin haklarını, veri ihlallerini ve ihlallerin sonuçlarını kapsamalıdır. Bu kapsamda yeni işe başlayan çalışanlara başlangıç eğitimi ile yıllık kişisel veri koruma güncelleme eğitimlerinin sunulması önemlidir.

**i) VERBİS'e Bildirim**

VERBİS, koşulları sağlanması halinde belirli veri sorumluları tarafından kaydolunması gereken bir sistem olsa da Kurul rehberinde ayrıca tedbir olarak yer vermiştir. Şeffaflığı sağlamanın önemli bir aracı olarak değerlendirilen VERBİS kaydının güncel ve doğru olması gerekmektedir. Bu tedbir ve yükümlülüğün[220] tam ve eksiksiz uygulanabilmesi için Kurul tarafından "Sorularla VERBİS" rehberi yayımlanmıştır. Veri Sorumluları Sicili Yönetmeliği madde 13 uyarınca VERBİS'e bildirilen bilgilerde herhangi bir değişiklik olması halinde meydana gelen değişiklikler yedi gün içerisinden Kurum'a bildirilmelidir.

### 3.1.1.2. Teknik Tedbirler

Dijital platformlarda kişisel verilerin korunması, günümüzün hızla gelişen teknoloji dünyasında büyük bir önem taşımaktadır. Kişisel verilerin korunması, yalnızca KVKK'da bir yükümlülük değil, aynı zamanda bireylerin mahremiyetini korumanın ve bilgi güvenliğini sağlamanın temel bir unsurudur. Teknik tedbirler,

---

- *Veri güvenliği farkındalığını artıracak etkinlik ve bilgilendirme çalışmaları yetersiz kalmıştır.*
- *Kişisel verilerin işlenmesi ve korunması ile ilgili yazılı politika ve prosedürler oluşturulmamıştır.*
- *Veri sorumlusunun, veri güvenliği ile ilgili iç denetim ve control mekanizmaları yeterince uygulanmamıştır.*
- *Veri ihlallerini önlemek amacıyla iç denetim ve izleme faaliyetleri etkin bir şekilde yürütülmemiştir*."

Sonuç olarak Kurul veri sorumlusunun veri güvenliğine ilişkin yükümlülüklerine aykırı hareket ettiğini ve gerekli teknik ve idari tedbirleri almadığı kanaatine varmış, ihlal bildirimini de 72 saat içinde yapılmamasını göz önünde bulundurarak toplam 450.000 TL tutarında idari para cezası uygulamıştır.

[220] Sorularla Veri Sorumluları Sicil Bilgi Sistemi (VERBİS): https://verbis.kvkk.gov.tr/UploadedFiles/SORULARLA_VERB%C4%B0S.pdf (E.T.: 16.09.2024).

bu bağlamda kişisel verilerin bütünlüğünü, gizliliğini ve erişilebilirliğini sağlamak için alınan önlemler olarak karşımıza çıkmaktadır. Siber güvenlik, şifreleme, erişim kontrolü ve sızma testleri gibi teknik tedbirler, veri ihlallerini önlemek ve olası güvenlik açıklarını kapatmak için kritiktir.

Teknik tedbirler, kişisel verilerin korunması hukukunun bir gerekliliği olsa da bilgi teknolojileri (BT) ekipleri ile dirsek dirseğe çalışılmasını gerektirmektedir. BT ekipler, sistemlerin güvenliğini sağlamak ve sürekli olarak güncel tehditlere karşı savunma mekanizmaları geliştirmek konusunda uzmanlaşmışlardır. BT ekipleri ile yakın iş birliği, veri güvenliği politikalarının uygulanmasına tutarlılık ve bütünlük sağlamaktadır.

Sonuç olarak, dijital platformlarda kişisel verilerin korunması için Kurul kararlarında ve Kişisel Veri Güvenliği Rehberi'nde belirtilenlerle sınırlı olmaksızın veri sorumlusunun veri güvenliğini sağlamak üzere gerekli olduğunu tespit ettiği tüm teknik tedbirlerin alınması ve BT ekipleri ile yakın iş birliği içinde çalışması hem KVKK'ya uyum sağlanması hem de kullanıcıların veri mahremiyetinin temin edilmesi için önemlidir. Bu bölümde Kişisel Veri Güvenliği Rehberi kapsamında uygulanması gereken tedbirler Kurul kararları ışığında değerlendirilecektir.

**a) Siber Güvenliğin Sağlanması**

Siber güvenlik, dijital platformların güvenliği ve kullanıcı bilgilerinin korunması için kritik öneme sahiptir. Bu kapsamda aşağıdaki teknik tedbirler ve bunlara ilişkin örnek kararlar detaylandırılmıştır:

- Ağ Güvenliği: Güvenlik duvarları, saldırı tespit ve önleme sistemleri gibi araçlar kullanılarak iç ve dış tehditlere karşı koruma sağlanmalıdır. Örneğin, Kurul'un 24.11.2020 tarih ve 2020/905 sayılı Karar Özeti[221] kapsamında Kurul, bir sigorta şirketine ait test sunucusuna yapılan saldırı sonucu gerçekleşen veri

[221] "Bir sigorta şirketinin kişisel veri ihlal bildirimi hakkında" Kişisel Verileri Koruma Kurulunun 24.11.2020 tarih ve 2020/905 sayılı Karar Özeti: https://www.kvkk.gov.tr/Icerik/6862/2020-905 (E.T.: 16.09.2024).

ihlalini incelemiş ve sızma testlerinin önemini vurgulamıştır. En nihayetinde şirketin ağ güvenliği önlemlerinin yetersiz olduğu ve sızma testlerinin düzenli olarak yapılmadığı tespit edilmiştir.

- Sızma Testi: Sistemlerin güvenlik açıklarını tespit etmek ve bu açıkları kapatmak için düzenli olarak sızma testleri yapılmalıdır. Kurul'un 23.12.2021 tarih ve 2021/1324 sayılı Karar Özeti[222] kapsamında bir bankanın veri ihlali sonrası yapılan incelemelerde sızma testlerinin yetersiz kişiler tarafından ele geçirilmesine neden olmuştur. Bu karar kapsamında da sızma testlerinin düzenli yapılmasının önemi vurgulanmaktadır.

- Güncel anti-virüs Sistemleri: Sistemlerin güncel antivirüs yazılımları ile korunması, kötü amaçlı yazılımlara karşı etkin bir savunma sağlar. Kurul'un 23.03.2023 tarih ve 2023/1645 sayılı Karar Özeti[223], geniş katılımlı çevrim içi bir oyunun dağıtıcısının ihmalini ele almaktadır. Olaydaki açık, çevrim içi oyunun dolandırıcılık önleyici yazılımının kişisel verileri izinsiz taramasından kaynaklanmaktadır. Veri sorumlusu, bu yazılımın işleyişini tam anlamıyla kontrol edemediği için güvenlik açıklarına yol açmış ve bu durum, kişisel verilerin korunmasıyla ilgili yükümlülüklerin ihlaline neden olmuştur.

Güncel antivirüs yazılımları, veri ihlallerine ve kötü niyetli yazılımlara karşı koruma sağlamaktadır. Veri sorumlularının, sistemlerini düzenli olarak güncelleyerek ve güvenlik açıklarını kapatarak veri koruma yükümlülüklerini yerine getirmeleri gerektiği belirtilmiştir.

### b) Kişisel Veri Güvenliğinin Takibi

Kişisel verilerin güvenliğinin sağlanması için sürekli izleme ve kontrol gereklidir. Bu konuda uygulanabilecek metotlar aşağıdaki şekilde

[222] "Yemek Sepeti Elektronik İletişim Perakende Gıda Lojistik AŞ veri ihlal bildirimi hakkında" Kişisel Verileri Koruma Kurulunun 23/12/2021 tarih ve 2021/1324 sayılı Karar Özeti: https://www.kvkk.gov.tr/Icerik/7168/2021-1324 (E.T.: 16.09.2024).
[223] "Geniş katılımlı çevrim içi bir oyunun Türkiye'deki dağıtıcısı ve tek yetkilisi konumundaki veri sorumlusu tarafından kişisel verilerin hukuka aykırı işlenmesi" hakkında Kişisel Verileri Koruma Kurulunun 28/09/2023 Tarihli ve 2023/1645 Sayılı Karar Özeti: https://www.kvkk.gov.tr/Icerik/7765/2023-1645 (E.T.: 16.09.2024).

örneklendirilebilir:

- Erişim Logları: Kişisel verilere kimlerin eriştiğinin kaydedilmesi ve düzenli olarak denetlenmesini gerektirir. Özellikle dijital platformlarda, kullanıcı aktivitelerinin izlenmesi ve olası ihlallerin tespit edilmesi için erişim logları kritik öneme sahiptir. Örnek karar olarak Kurul'un 06.08.2021 tarihli ve 2022/413 sayılı Karar Özeti[224] verilebilir, bir sağlık kuruluşunun hasta bilgilerine yapılan yetkisiz erişimler sonucunda alınan kararları içermektedir. Sağlık kuruluşu, erişim loglarını düzenli olarak tutmadığı ve denetlemediği için kişisel verilerin güvenliğini sağlayamadığı sonucuna varılmıştır. Bu karar da erişim loglarının önemini ortaya koymaktadır.

- Yetki kontrolü: Kişisel verilere sadece yetkili kişilerin erişebilmesi sağlanmalıdır. Dijital platformlarda kullanıcıların erişim yetkileri net bir şekilde belirlenmeli ve düzenli olarak güncellenmelidir. Örnek karar olarak Kurul'un 05.05.2020 tarihli 2020/344 sayılı Karar Özeti[225] verilebilir. Bir bankanın iç kontrol faaliyetleri sırasında, 3 personelin yetkilerini kötüye kullanarak banka müşterisi olmayan kişilere ait kredi bilgilerine eriştiğini ortaya koymaktadır. Personel, Kredi Kayıt Bürosu (KKB) sorgulama ekranını amacı dışında kullanmış ve bu eylem bankanın bilgi güvenliği politikalarına aykırı bulunmuştur.

### c) Kişisel Veri İçeren Ortamların Güvenliğinin Sağlanması

Veri depolama alanlarının güvenliği, verilerin yetkisiz erişimlerden korunması açısından kritik öneme sahiptir. Bu konuda uygulanabilecek teknik tedbirler aşağıdaki şekilde örneklendirilebilir:

- Veri maskeleme: Kişisel verilerin muhafaza edildiği ortamda maskelenerek tutulması, yetkisiz kullanıcıların bu verilere erişimini engeller. 25.03.2021 tarih

[224] "Kişisel sağlık verilerinin hastanedeki yetkisiz çalışanlar tarafından velayete sahip olmayan ebeveyn ile paylaşılması" hakkında Kişisel Verileri Koruma Kurulunun 06/08/2021 tarihli ve 2021/761 sayılı Karar Özeti: https://www.kvkk.gov.tr/Icerik/7137/2021-761 (E.T.: 16.09.2024).
[225] "Bir bankanın veri ihlal bildirimi hakkında" Kişisel Verileri Koruma Kurulunun 05.05.2020 tarih ve 2020/344 sayılı Karar Özeti: https://www.kvkk.gov.tr/Icerik/6764/2020-344 (E.T.: 16.09.2024).

ve 2021/311 sayılı Karar Özeti[226] kapsamında veri maskelemenin önemi vurgulanmıştır. Karar konu olayda, kozmetik şirketinin veri maskeleme ve şifreleme gibi önlemleri ihlalden sonra almayı planladığı belirtilmiştir. Kişisel Veri Güvenliği Rehberi'nde yer verilen "şifreleme ve veri maskeleme" önlemlerine uygun hareket edilmesi gerektiğini vurgulanmıştır.

- Veri Kaybı Önleme Yazılımları: Veri kaybını önlemek için kullanılan yazılımlar kişisel veri güvenliğini sağlamak için önemli rol oynamaktadır. Kurul'un 08.12.2020 tarihli ve 2020/935 sayılı Karar Özeti[227] kapsamında bir sigorta şirketinin veri kaybı önleme sisteminin düzenli kontrolleri sırasında, sistemi kontrol eden görevli tarafından veri ihlalinin tespit edildiği ve ilgili birimlere aksiyon alınması için iletildiği belirtilmiştir. Veri ihlal risklerinin en aza indirgenebilmesi için oldukça önemli bir tedbirdir.

- Log Kayıtları: Verilerin kimler tarafından ve nasıl kullanıldığının kaydedilmesi, izleme ve denetim açısından önemlidir. Dijital platformlar, kullanıcı aktivitelerini izlemek ve olası ihlalleri tespit etmek için log kayıtlarını düzenli olarak tutmalıdır. Örneğin Kurul'un 06.08.2021 tarihli 2021/761 sayılı Karar Özeti[228] kapsamında bir hastanenin otomasyon sisteminin log kayıtları ile ilgili eksiklikler tespit edilmiş ve bu eksikliklerin veri güvenliği için ciddi riskler oluşturduğu belirtilmiştir. Özellikle, kimin hangi veriye eriştiğinin loglanmadığı ve bu durumun kontrolsüz erişimlere neden olduğu ifade edilmiştir.

### d) Kişisel Verilerin Bulutta Depolanması

Bulut hizmetleri, verilerin esnek ve güvenli bir şekilde depolanmasını sağlar, ancak belirli tedbirler alınması gerekmektedir. Bu tedbirler aşağıdaki

[226] "Bir kozmetik şirketinin veri ihlal bildirimi hakkında" Kişisel Verileri Koruma Kurulunun 25.03.2021 tarih ve 2021/311 sayılı Karar Özeti: https://www.kvkk.gov.tr/Icerik/7001/2021-311 (E.T.: 16.09.2024).
[227] "Bir sigorta şirketinin veri ihlal bildirimi hakkında" Kişisel Verileri Koruma Kurulunun 08/12/2020 tarih ve 2020/935 sayılı Karar Özeti: https://www.kvkk.gov.tr/Icerik/7019/2020-935 (E.T.: 16.09.2024).
[228] "Kişisel sağlık verilerinin hastanedeki yetkisiz çalışanlar tarafından velayete sahip olmayan ebeveyn ile paylaşılması" hakkında Kişisel Verileri Koruma Kurulunun 06/08/2021 tarihli ve 2021/761 sayılı Karar Özeti: https://www.kvkk.gov.tr/Icerik/7137/2021-761 (E.T.: 16.09.2024).

şekilde örneklendirilebilir.

- Şifreleme: Kişisel verilerin buluta aktarılmadan önce şifrelenmesi, kişisel veri güvenliği risklerini azaltır. Bu doğrultuda dijital platformların bulutta depolanan kişisel verilerini şifreleme ile koruması tavsiye edilir. Kurul'un 06.05.2021 tarihli ve 2021/470 sayılı Karar Özeti[229] kapsamında, bir yemek kartı şirketinin, kullanıcısının hesap hareketleriyle ilgili talep ettiği bilgileri güvenli bir şekilde paylaşmak için şifreleme yöntemini kullandığı belirtilmiştir. İlgili kişi, kendisine ait hesap hareketlerini görmek istemiş ve bu talep doğrultusunda veri sorumlusu şirket, bilgileri şifreli bir dosya olarak göndermiştir. Kurul, şifreleme yönteminin kişisel verilerin korunmasında kritik bir güvenlik tedbiri olduğunu vurgulamıştır.

- Güvenlik Duvarları (*Firewalls)*: Bulut hizmetlerine erişimlerin güvenlik duvarları ile korunması gerekmektedir. Dijital platformlar da bulut hizmetlerini kullanırken güvenlik duvarları ile koruyarak yetkisiz erişimleri engellemelidir. Kurul'un 23.12.2021 tarihli ve 2021/1324 sayılı Karar Özeti[230] kapsamında Kararda, Yemeksepeti'ne ait bir web uygulama sunucusunun saldırıya uğradığı ve kişisel verilerin sızdırıldığı tespit edilmiştir. Güvenlik duvarlarının (*firewall*) üzerinde saldırıya dair izler bulunmasına rağmen, büyük miktarda verinin dışarıya sızdırılması fark edilemediği belirtilmektedir. Bu durum, güvenlik duvarlarının izleme ve uyarı mekanizmalarının etkili bir şekilde yönetilmediğini ve bu nedenle güvenlik kontrollerinin yetersiz olduğunu göstermiştir.

- Yedekleme: Bulut sistemlerinde düzenli olarak yedekleme yapılması, veri kaybı durumlarında kurtarma işlemlerini kolaylaştırmaktadır.

---

[229] "İlgili kişinin yemek kartı hesap hareketlerine ilişkin kişisel verilerine erişim talebinin veri sorumlusu tarafından yerine getirilmediği iddiası" hakkında Kişisel Verileri Koruma Kurulunun 06/05/2021 tarihli ve 2021/470 sayılı Karar Özeti: https://www.kvkk.gov.tr/Icerik/6982/2021-470 (E.T.: 16.09.2024).

[230] "Yemek Sepeti Elektronik İletişim Perakende Gıda Lojistik AŞ veri ihlal bildirimi hakkında" Kişisel Verileri Koruma Kurulunun 23/12/2021 tarih ve 2021/1324 sayılı Karar Özeti: https://www.kvkk.gov.tr/Icerik/7168/2021-1324 (E.T.: 16.09.2024).

**e) Bilgi Teknolojileri Sistemleri Tedariği, Geliştirme ve Bakımı**

Dijital platformlarda bilgi teknoloji sistemlerinin güvenli bir şekilde tedarik edilmesi, geliştirilmesi ve bakımı, kişisel verilerin güvenliğinin sağlanması açısından kritik öneme sahiptir. Bu kapsamında alınması gereken teknik tedbirlere ilişkin örnekler aşağıda sunulmaktadır:

- Güvenli Yazılım Geliştirme: Yazılım geliştirme süreçlerinde güvenlik öncelik olmalıdır. Bu, kod incelemeleri, güvenlik testleri ve güvenlik açıklarını düzenli olarak gözden geçirilmesi gibi uygulamaları içerir. Örneğin Kurul'un 16.06.02020 tarihli ve 2020/465 sayılı Karar Özeti[231] kapsamında bir yazılım firmasının güvenlik açıkları nedeniyle aldığı cezayı ele almaktadır. Kararda, yazılım firmasının sistemlerinde "parola püskürtme" saldırıları sonucu kimlik doğrulama anahtarlarının kaydedilmesi ve önemli miktarda verinin sızdırılması gibi güvenlik zafiyetleri tespit edilmiştir. Bu karar, yazılım geliştirme süreçlerinde güvenlik açıklarının kapatılmasının ve düzenli güvenlik testlerinin yapılmasının önemini vurgulamaktadır.

- Güvenlik Gereksinimlerini Belirleme: Bilgi teknolojisi sistemlerinin tedarik aşamasında, güvenlik gereksinimlerinin net bir şekilde belirlenmesi ve bu gereksinimlerin karşılandığının doğrulanması gerekmektedir. Kurul'un 16/06/2020 tarih ve 2021/464 sayılı Karar Özeti[232], bir otoyol işletmesinin veri ihlal bildirimiyle ilgilidir ve güvenlik gereksinimlerinin belirlenmesi konusundaki eksiklikleri vurgulamaktadır. Kararda, veri sorumlusunun bordro sisteminde yaşanan teknik hatalar sonucunda çalışanların kişisel e-posta adreslerine yanlışlıkla başkalarına ait bordroların gönderildiği tespit edilmiştir. Bu durumun, güvenlik gereksinimlerinin net bir şekilde belirlenmemesinin ve idari eksikliklerin bir sonucu olduğu anlaşılmaktadır. Kurul, Kişisel Veri Güvenliği

[231] "Kurumsal yazılım hizmeti sunan bir veri sorumlusunun veri ihlali bildirimi hakkında" Kişisel Verileri Koruma Kurulunun 16/06/2020 tarih ve 2020/465 sayılı Karar Özeti: https://www.kvkk.gov.tr/Icerik/7031/2020-465 (E.T.: 16.09.2024).
[232] "Bir otoyol işletmesinin veri ihlal bildirimi hakkında" Kişisel Verileri Koruma Kurulunun 16.06.2020 tarih ve 2021/464 sayılı Karar Özeti: https://www.kvkk.gov.tr/Icerik/6994/2021-464 (E.T.: 16.09.2024)

Rehberi'ne atıfta bulunarak, veri güvenliğinin sağlanması için tüm kişisel verilerin neler olduğunun ve bu verilerin korunmasına yönelik risklerin belirlenmesi gerektiğini belirtmiştir. Ayrıca, güvenlik zafiyetlerinin ve tehditlerin raporlanması için resmi prosedürlerin oluşturulması gerektiği vurgulanmıştır

- Bakım ve Güncelleme: Bilgi teknoloji sistemlerinin düzenli olarak bakımı ve güncellemelerinin yapılması, yeni ortaya çıkan güvenlik tehditlerine karşı korunması için gereklidir. Özellikle güvenlik yamalarının zamanında uygulanması önemlidir.

- Saldırı Tespit ve Önleme Sistemleri: Bilgi teknoloji sistemlerine yönelik olası saldırıları tespit etmek ve önlemek amacıyla saldırı tespit ve önleme sistemleri kurulmalıdır. Kurul'un 09/10/2020 tarihli ve 2020/787 sayılı Karar Özetinde[233], sağlık sektöründe faaliyet gösteren bir veri sorumlusunun, saldırı tespit ve önleme sistemlerini kullanarak veri ihlaline yönelik güvenlik tedbiri aldığı belirtilmiştir. Kararda, sunuculardaki açıkların giderilmesi, saldırı tespit ve önleme sistemlerinin kullanılması, güvenlik duvarlarının aktif olarak yönetilmesi gibi önlemler sayesinde olası güvenlik tehditlerinin azaltılmasının sağlandığı vurgulanmıştır.

**f) Kişisel Verilerin Yedeklenmesi**

Kişisel verilerin yedeklenmesi, veri kaybı durumlarında verilerin geri kazanılmasını sağlamak için elzemdir. Dijital platformlarda veri yedekleme stratejilerinin etkili bir şekilde uygulanması gerekmektedir. Bu kapsamda alınması gereken tedbirler aşağıdaki şekilde örneklendirilebilir:

- Düzenli Yedekleme: Kişisel verilerin düzenli olarak yedeklenmesi, veri kaybı durumlarında verilerin geri kazanılmasını sağlar. Bunun için bir program kullanılarak otomatik bir şekilde yedekleme gerçekleştirilebilir.

[233] Bir özel sağlık kuruluşu tarafından sunulan sağlık hizmetinin açık rıza şartına bağlanması hakkında Kişisel Verileri Koruma Kurulunun 02/05/2023 tarihli ve 2023/692 sayılı Karar Özeti: https://www.kvkk.gov.tr/Icerik/7691/2023-692 (E.T.: 16.09.2024)

- Yedeklerin Güvenliği: Yedeklenen verilerin güvenliği sağlanmalı ve yetkisiz erişimlerden korunmalıdır.

- Yedeklerin Test Edilmesi: Yedekleme süreçlerinin etkinliğini sağlamak amacıyla yedeklerin düzenli olarak test edilmesi gerekmektedir. Bu testler, veri geri yükleme işlemlerinin sorunsuz çalıştığını doğrulamak için yapılmalıdır.

#### 3.1.1.3. Özel Nitelikli Kişisel Veriler

Özel nitelikli kişisel veriler, yukarıda belirtildiği üzere öğrenildiğinde kişilerin ayrımcılığa uğrama riski olan özel koruma gerektiren kişisel verilerdir. Bu sebeple, Kurul Özel Nitelikli Kişisel Verilerin İşlenmesinde Veri Sorumlularınca Alınması Gereken Yeterli Önlemler" ile ilgili 31.01.2018 tarihli ve 2018/10 sayılı Kararı[234] kapsamında özel nitelikli kişisel verilerin korunması için ayrıca teknik ve idari tedbirler öngörmüştür. Bu doğrultuda;

- Veri sorumlularının özel nitelikli kişisel verilerin güvenliğini sağlamak için özel bir politikaya sahip olması gerekmektedir.

- Özel nitelikli kişisel verilerin işlenmesine dahil olan çalışanların KVKK ve ilgili düzenlemelere ilişkin olarak eğitim almaları gerekmektedir. Ayrıca çalışanlar ile gizlilik sözleşmeleri yapılmalı, yetki kapsamları ve süreleri net bir şekilde belirlenmelidir.

- Özel nitelikli kişisel verilerin elektronik veya fiziksel ortamda işlenmesi ya da aktarılması halinde buna ilişkin gerekli tedbirleri alması gerekmektedir.

Bir dijital platformun ayrıca biyometrik veri işlemesi halinde, Kurul'un Biyometrik Verilerin İşlenmesinde Dikkat Edilmesi Gereken Hususlara İlişkin

[234]"Özel Nitelikli Kişisel Verilerin İşlenmesinde Veri Sorumlularınca Alınması Gereken Yeterli Önlemler" ile ilgili Kişisel Verileri Koruma Kurulunun 31/01/2018 Tarihli ve 2018/10 Sayılı Kararı https://www.kvkk.gov.tr/Icerik/4110/2018-10 (E.T.: 16.09.2024).

Rehber'e[235] de dikkat etmesi gerekmektedir. Temel olarak veri güvenliğinin sağlaması kritiktir, bu sebeple güçlü şifreleme yöntemleri kullanılmalıdır. Biyometrik verilere erişim, yetkilendirilmiş personelle sınırlandırılmalı ve erişim kayıt altına alınmalıdır. En önemlisi de eğer daha az müdahaleci alternatif bir veri işleme faaliyeti ile hedeflenen sonuca ulaşılabiliyorsa biyometrik veri işleme faaliyetinden kaçınılması gerekmektedir.

Dijital platformun biyometrik veri işlemesine örnek olarak Kurul'un 30.08.2023 tarihli ve 2023/1310 sayılı Kararı[236] verilebilir. Bu karar kapsamında biyometrik veri işlemek yerine yürütülebilecek alternatiflerin değerlendirilmesinin ve bu konuda bilgilendirmenin yapılmasının önemi vurgulanmıştır. Karara konu olayda bir banka mobil bankacılık hizmeti sunduğu platformda müşterinin kurumsal hesabına giriş yapmak istediğinde yüz verilerinin işlenmesi için onay verilmesinin şart koşulması ve bu onayın verilmemesi durumunda hizmetten faydalandırılmaması iddiasıyla şikâyet konusu olmuştur. Veri sorumlusu banka, müşterilerin yüzlerine ait verilerin işlenmesine yönelik müşterilerden açık rıza talep ettiği, açık rıza verilmediği takdirde alternatif olarak şube veya telefon bankacılığı kanallarının kullanılabildiğini belirtmiştir. Kurul yaptığı incelemesinde Bankaların Bilgi Sistemleri ve Elektronik Bankacılık Hizmetleri Hakkında Yönetmelik'in[237] 34. maddesi gereğince, elektronik bankacılık hizmetleri için bankaların en az iki bileşenli bir kimlik doğrulama sistemini uygulaması gerektiğini belirtmiştir. Bu kapsamda, bankanın, müşterilerinin güvenliği için biyometrik verileri kullanmasının iki bileşenli kimlik doğrulama mekanizmasına uygun olduğu, ancak alternatif seçeneklerin yeterince açık şekilde sunulmadığı tespit edilmiştir. Bankanın, yüz verilerinin işlenmesi için açık rıza vermeyen müşterilere alternatif hizmet kanalları sunduğu, ancak bu bilgilerin daha anlaşılır

[235] Biyometrik Verilerin İşlenmesinde Dikkat Edilmesi Gereken Hususlara İlişkin Rehber: https://www.kvkk.gov.tr/SharedFolderServer/CMSFiles/bd06f5f4-e8cc-487e-abe1-d32dc18e2d7e.pdf (E.T.: 16.09.2024).
[236] "Banka mobil uygulamasında dijital parola belirlerken yüz verisinin işlenmesi suretiyle kişisel verilerin işlenmesi" hakkında Kişisel Verileri Koruma Kurulunun 03/08/2023 Tarihli ve 2023/1310 Sayılı Karar Özeti: https://kvkk.gov.tr/Icerik/7775/2023-1310 (E.T.: 16.09.2024).
[237] RG: 15.03.2020, 31069.

ve ulaşılabilir şekilde sağlanması gerektiğini vurgulamıştır.

Dijital platformun genetik veri işlemesi halinde ise Kurul'un Genetik Verilerin İşlenmesinde Dikkat Edilmesi Gereken Hususlara İlişkin Rehber'ini[238] göz önünde bulundurması gerekecektir. Burada da özetle veri güvenliği ve erişime dikkat edilmesi gerekmektedir. Mümkün olan her durumda genetik verilerin anonimleştirilmek suretiyle işlenmesi gerekmektedir.

## 3.2. KURUL KARARLARI IŞIĞINDA DİJİTAL PLATFORMLARIN MAHREMİYET ENDİŞELERİ

### 3.2.1. Dijital Platformlarda Kişisel Verilerin Doğru ve Güncel Olmasını Sağlama Yükümlülüğü

Dijital platformlarda kişisel verilerin korunması ve bu kapsamda kişisel verilerin doğruluğunu ve güncelliğini sağlaması için veri güvenliğinin temin edilmesi açısından kritiktir. KVKK'nın 4. maddesinin ikinci fıkrası, kişisel verilerin işlenmesinde uyulması gereken temel ilkeleri belirlemektedir. Bu ilkelerden biri de kişisel verilerin doğru ve gerektiğinde güncel olma ilkesidir. Bu ilkeye göre, veri sorumluları, topladıkları kişisel verilerin doğruluğunu sağlamak ve gerektiğinde güncellemelerini yapmakla yükümlüdürler.

Kurul'un 22.12.2020 tarihi ve 2020/966 sayılı İlke Kararı[239], veri sorumlularının kişisel verilerin doğruluğunu ve güncelliğini sağlamaları konusunda önemli bir karardır. Özellikle e-ticaret, telekomünikasyon, ulaşım ve turizm gibi sektörlerde faaliyet gösteren veri sorumlularının, kişisel veri içeren dokümanları sms veya e-posta yoluyla gönderirken bu verilerin doğruluğunu ve

[238] Kişisel Verileri Koruma Kurumu, Genetik Verilerin İşlenmesinde Dikkat Edilmesi Gereken Hususlara İlişkin Rehber, Ankara:. https://www.kvkk.gov.tr/SharedFolderServer/CMSFiles/703442e0-690c-4618-91c3-83e7583170ca.pdf (E.T.: 16.09.2024).

[239] Veri sorumluları tarafından kişilerin telefon numarası, e-posta adresi gibi iletişim kanallarına Kanuna aykırı şekilde gönderilen üçüncü kişilere ait kişisel veriler hakkında Kişisel Verileri Koruma Kurulunun 22/12/2020 Tarihli ve 2020/966 sayılı İlke Kararı.: https://www.kvkk.gov.tr/Icerik/6858/2020-966 (E.T.: 16.09.2024).

güncelliğini nasıl sağlamaları gerektiği konusunu ele almaktadır.

Söz konusu İlke Kararı çerçevesinde veri sorumlularının kişisel verilerin doğru ve güncel tutulmasını sağlamak amacıyla aşağıdaki önlemleri almaları gerekir:

- Kişisel verilerin elde edildiği kaynakların belirlenmesi: Kişisel verilerin hangi kaynaklardan elde edildiğinin belirlenmesi ve bu kaynakların doğruluğunun tespit edilmesi gerekmektedir.

- Doğrulama mekanizmalarının oluşturulması: Kişisel verilerin doğruluğunu ve güncelliğini sağlamak amacıyla, veri sorumlularının, ilgili kişilerin beyan ettiği telefon numarası ve e-posta adresi gibi iletişim bilgilerinin doğrulanmasına yönelik mekanizmalar oluşturması gerekmektedir. Bu, doğrulama kodu veya doğrulama linki gönderilmesi gibi yöntemlerle sağlanabilir.

- Güncel olmayan verilerin riskleri: Güncel olmayan veya yanlış tutulan kişisel verilerin, ilgili kişilere maddi ve manevi zararlar verebileceği göz önünde bulundurulmalıdır. Bu nedenle, veri sorumlularının, kişisel verilerin doğru ve güncel olmasını temin edecek kanalları her zaman açık tutmaları önem arz etmektedir.

Dijital platformlarda kişisel verilerin doğru ve güncel tutulması, veri güvenliğinin sağlanması ve ilgili kişilerin haklarının korunması açısından büyük önem taşımaktadır. Anılan İlke Kararı, veri sorumlularının yükümlülüklerini yerine getirmeleri için gerekli önlemleri almalarını vurgulamaktadır.[240]

### 3.2.2. Dijital Platformlarda Kampanya ve Pazarlama Faaliyetleri

Dijital platformun konusunun ne olduğu fark etmeksizin en çok karşılaşılan faaliyetlerden birisi platformun kampanya ve pazarlama faaliyeti yürütmesidir. Bu kapsamda, Kurul'un çeşitli kararlarında bu faaliyetlerin hukuka uygun yürütülmesi

[240] Benzer başka bir karar için bkz: https://kvkk.gov.tr/Icerik/7576/2022-853 (E.T: 16.09.2024).

açısında yol gösterici nitelikte kararlar vermiştir.

Kurul'un 04.06.2021 tarihli ve 2021/548 sayılı Karar Özeti[241] kapsamında ilgili kişi bir dijital platformu şikâyet ederek, kendisi ile ilişkisi olmamasına rağmen çağrı merkezinden sürekli arandığı ve söz konusu platforma üye olmasına dair pazarlama faaliyeti yürütüldüğü belirtilmiştir. Kurul yaptığı incelemede söz konusu faaliyet kapsamında ilgili kişinin açık rızasının gerektiği, söz konusu olayda dijital platformun bayisinin veri sorumlusu gibi hareket ettiği ve herhangi bir veri işleme şartına dayanmadığı belirlenmiştir. Kurul, ilgili kişinin kişisel verisi olan telefon numarasının hukuka aykırı olarak elde edilmesi ve işlenmesi sebebiyle veri sorumlusu haline gelen bayi hakkında idari para cezası uygulamıştır.

Dijital platformlarda en sık karşılaşılan uygulamalarından birisi sadakat programlarıdır. Kurul'un 05.07.2019 tarihli ve 2019/198 sayılı Karar Özeti[242] kapsamında ihbar üzerine bir mağazanın sadakat programı incelenmiştir. İhbarda belirtildiği üzere mağazanın sadakat programı kapsamında belirli ürünlere özel indirimler uygulamakta ve bu programdan faydalanmak isteyen müşterilerin kişisel verilerini işleyebilmek için açık rızalarını vermesi koşul olarak dayatılmıştır. Kurul, yaptığı incelemesinde açık rızanın temel unsurlarını vurgulamış ve sadakat programı kapsamında yapılan indirimlerin ve ek menfaatlerin temel ürünün veya hizmetin sunulmasına ilişkin olmadığını, ek menfaat niteliğinde olduğu ve bu durumun açık rızanın özgür irade ile verilmesi koşulunu ortadan kaldırmadığını değerlendirmiştir. Sadakat programına dahil olmak istemeyen veya açık rıza vermek istemeyen müşterilere de alışveriş yapma imkânı sunulduğu ve ürünlerin indirimsiz fiyatlarla satışa devam edildiği sürece

[241] "İlgili kişinin cep telefonu numarasının kampanya adı altında bir dijital platform bayisi tarafından edinilmesi, işlenmesi ve rızası olmaksızın arama yapılması" hakkında Kişisel Verileri Koruma Kurulunun 04/06/2021 tarih ve 2021/548 sayılı Karar Özeti: https://kvkk.gov.tr/Icerik/7123/2021-548 (E.T.: 16.09.2024).

[242] "İlgili kişinin, bir sadakat programı kapsamında veri sorumlusunca hukuka aykırı kişisel veri işlendiği yolundaki ihbarı" hakkında Kişisel Verileri Koruma Kurulunun 05/07/2019 tarihli ve 2019/198 sayılı Karar Özeti: https://kvkk.gov.tr/Icerik/7348/2019-198 (E.T.: 16.09.2024)

veri sorumlusunun herhangi bir hukuka aykırılık taşımadığı sonucuna varılmıştır.

### 3.2.3. Dijital Platformlarda Kullanıcı Güvenliği

Kullanıcı güvenliği, dijital platformların sürdürülebilirliği ve güvenilirliği açısından kritik bir öneme sahiptir. KVKK'nın 12. maddesinin birinci fıkrasında belirtildiği üzere veri sorumluları kişisel verilerin hukuka aykırı olarak işlenmesini ve erişilmesini önlemek kişisel verilerin muhafazasını sağlamak amacıyla gerekli her türlü teknik ve idari tedbirleri almak zorundadır. Bu teknik ve idari tedbirler Bölüm 4.1 kapsamında anılan Kişisel Veri Güvenliği Rehberi ve Kurul kararları ışığında belirlenmektedir.

Kullanıcı güvenliğine ilişkin Kurul'un "Kullanıcı Güvenliğine İlişkin Veri Sorumluları Tarafından Alınması Tavsiye Edilen Teknik ve İdari Tedbirlere İlişkin Kamuoyu Duyurusu"[243] kapsamında önerilere yer verilmiştir. Kamuoyu duyurusu özellikle finans, e-ticaret, sosyal medya ve oyun gibi çeşitli sektörlerde faaliyet gösteren veri sorumlularının internet sitelerine ait kullanıcı hesap bilgilerinin (kullanıcı adı ve parolalar) bazı internet sitelerinde herkese açık şekilde ifşa edildiğinin tespit edildiğini belirtmektedir. Üçüncü kişiler bu hesap bilgilerini kullanarak ilgili internet sitelerine kullanıcıların haberi olmadan giriş yapabilmekte ve kullanıcı verilerini görüntüleyebilmektedir. Ayrıca, veri sorumlularının sistemlerinden veya son kullanıcı bilgisayarlarındaki güvenlik açıklarından faydalanılarak elde edilen kişisel veriler hukuka aykırı bir şekilde paylaşılmakta ve ekonomik bir değer karşılığında satışa sunulabilmektedir.

Veri sorumlularının yukarıda belirtilen tedbirler kapsamında kendi risk değerlendirmemelerini yaparak uygun olanlarını uygulamaları, kullanıcı güvenliğini artırmak ve veri ihlallerini önlemek açısında büyük önem taşımaktadır. Bu tedbirleri uygulanması, dijital platformlarda kullanıcı güvenliği için kritiktir.

[243] Kullanıcı Güvenliğine İlişkin Veri Sorumluları Tarafından Alınması Tavsiye Edilen Teknik ve İdari Tedbirlere İlişkin Kamuoyu Duyurusu: https://www.kvkk.gov.tr/Icerik/7177/Kullanici-Guvenligine-Iliskin-Veri-Sorumlulari-Tarafindan-Alinmasi-Tavsiye-Edilen-Teknik-ve-Idari-Tedbirlere-Iliskin-Kamuoyu-Duyurusu (E.T.: 16.09.2024)

### 3.2.4. Dijital Platformların Profilleme Faaliyetleri

Dijital platformlarda profilleme faaliyetleri, kişisel verilerin belirli amaçlar doğrultusunda işlenmesi sürecinde önemli bir yer tutmaktadır. Bu bağlamda, araç kiralama firmaları tarafından gerçekleştirilen profilleme faaliyetleri Kurul'un 23.12.2021 tarihli ve 2021/1303 sayılı Karar Özeti[244] ile değerlendirilen "kara liste" uygulamaları üzerinden incelenebilecektir.

Profilleme, genellikle bireylerin davranışlarını analiz ederek bunlar hakkında tahminlerde bulunmayı amaçlayan bir süreçtir. İlgili karar; araç kiralama programları yazılımcıları ve satıcıları tarafından oluşturulan kara liste programları, müşterilere ait işlenen kişisel verilerin diğer araç kiralama firmalarıyla paylaşılmasına ilişkindir. İnceleme ihbar üzerine başlamıştır. İhbara göre; araç kiralama yazılımı üreten firmalar, müşterilerin verilerini kaydederek bu verileri diğer firmalarla paylaşmaktadır. Bu paylaşım, müşterilerin açık rızası olmaksızın gerçekleştirilmektedir.

Yukarıda açıklandığı üzere ilgili kişiler otomatik sistemler vasıtasıyla analiz edilmesi sonucunda ortaya çıkan olumsuz sonuçlara itiraz etme hakkına sahiplerdir. Araç kiralama firmalarının da müşterileri hakkında profilleme yaparak onları kara listeye alması ve bu bilgileri diğer firmalarla paylaşması, ilgili kişilerin temel hak ve özgürlüklerini ihlal edebilecek bir uygulama olduğu belirtilmektedir. Bu doğrultuda kara liste uygulaması kapsamında işlenen kişisel verilerin imha edilmesine hükmedilmiştir.

Bu karar, dijital platformlarda yürütülecek profilleme faaliyetlerinin yönetilmesinde dikkat edilmesi gereken önemli noktaları ortaya koymaktadır. Kişisel verilerin işlenmesi ve paylaşılması süreçlerinde veri sorumlularının hukuka uygun hareket etmesi ve ilgili kişilerin temel hak ve özgürlüklerine saygı

[244] "Araç kiralama programları yazılımcısı ve satıcısı firmalar tarafından, ilgili kişilerin verilerinin işlenmesi ve bu verilerin araç kiralama firmaları arasında paylaşılmasını sağlayan bir kara liste programı oluşturulması" hakkında Kişisel Verileri Koruma Kurulunun 23/12/2021 tarihli ve 2021/1303 sayılı Karar Özeti: https://www.kvkk.gov.tr/Icerik/7288/2021-1303 (E.T.: 16.09.2024)

göstermesi gerekmektedir.

## 3.3. KİŞİSEL VERİ İHLAL BİLDİRİMLERİ

Dijital platformların veri ihlal bildirim yükümlülüğü kişisel verilerin korunması konusundaki en önemli konulardan biridir. Kişisel verilerin kanuni olmayan yollarla başkaları tarafından elde edilmesi halinde; bu durumu bildirme yükümlülüğü hem bireylerin haklarının korunması hem de veri güvenliğinin sağlanması açısından büyük önem taşır.

KVKK'nın 12. maddesinin beşinci fıkrasında ise, kişisel verilerin kanuni olmayan yollarla elde edilmesi halinde yapılacak bildirimi düzenlemektedir. Böyle bir durumda veri sorumlusu bu durumu en kısa sürede ilgilisine ve Kurul'a bildirmekle yükümlüdür.

Kurul'un 24.01.2019 tarihli ve 2019/10 sayılı Kararı kapsamında[245] veri ihlal bildirim usul ve esasları detaylandırılmıştır. Bu karara göre KVKK'nın 12. Maddesinin beşinci fıkrasında belirtilen "en kısa sürede" ifadesi, 72 saat olarak kabul edilmektedir. Bu bağlamda, bir dijital platform bir veri ihlali olduğunu öğrendikten itibaren en geç 72 saat içinde Kurul'a bildirimde bulunmak zorundadır. Bildirimde gecikme olması durumda, bu gecikmenin nedenleri de Kurul'a açıklanmalıdır. [246]

Bu konuda kişisel veri ihlalinin geç bildirimine ilişkin Kurul'un bir kararında[247] veri sorumlusu gerçekleşen bir veri ihlalini ilgili kişilere on yedi ay, Kurul'a ise on aylık bir gecikmeyle bildirmiştir. Bu gecikmeler KVKK'nın 12. maddesinin beşinci fıkrasında belirtilen "en kısa süre"yi aşan bir süre olduğu için

[245] Kişisel Veri İhlali Bildirim Usul ve Esaslarına İlişkin Kişisel Verileri Koruma Kurulunun 24.01.2019 Tarih ve 2019/10 Sayılı Kararına İlişkin Duyuru: https://www.kvkk.gov.tr/Icerik/5362/Veri-Ihlali-Bildirimi (E.T.: 16.09.2024).

[246] Kişisel Veri İhlali Bildirimi Formu Kılavuzu: https://kvkk.gov.tr/SharedFolderServer/CMSFiles/369d954a-aaee-44ca-9ca6-105e8b4102f9.pdf (E.T.: 16.09.2024).

[247] Kişisel Veri Güvenliği İhlalinin Geç Bildirimi: https://kvkk.gov.tr/Icerik/5411/Kisisel-Veri-Guvenligi-Ihlalinin-Gec-Bildirimi (E.T.: 16.09.2024).

veri sorumlusu aleyhine idari para cezası uygulanmasına karar verilmiştir.

Bu doğrultuda bir dijital platform bünyesindeki kişisel verilerin kanuni olmayan yollarla elde edilmesi halinde takip edilecek bildirim süreci şu şekildedir:

- **İhlalin Tespiti ve Bildirimi:** Veri sorumlusu, kişisel verilerin kanuni olmayan yollarla elde edildiğini tespit eder etmez, bu durumu en geç 72 saat içinde Kurul'a bildirmelidir.

- **Etkilenen Kişilerin Bilgilendirilmesi:** İhlalden etkilenen kişilerin belirlenmesi müteakip, bu kişilere makul olan en kısa sürede bildirim yapılmalıdır. Bildirim, ilgili kişilerin iletişim adresine doğrudan yapılabileceği gibi ulaşılamıyorsa veri sorumlusunun internet sitesi üzerinden de yayımlanabilir.

- **Gerekçeli Bildirim:** Veri sorumlusunun, 72 saat içinde bildirim yapamaması durumunda, gecikmenin nedenlerini içeren gerekçeli bir bildirimde bulunması gerekmektedir.

- **Bildirim Formu:** Kurul'a yapılacak bildirimlerde Kurul tarafından belirlenen "Kişisel Veri İhlal Bildirim Formu" kullanılmalıdır.[248]

- **Kayıt Altına ve İncelemeye Hazır Bulundurma:** Veri sorumluları, veri ihlalleriyle ilgili bilgileri, etkilerini ve alınan önlemleri kayıt altına almalı ve Kurul'un incelemesine hazır halde bulundurmalıdır.[249]

Veri ihlalinin yurt dışında yerleşik veri sorumlusu nezdinde gerçekleşmesi halinde, bu ihlalin sonuçlarının Türkiye'de yerleşik ilgili kişileri etkilemesi ve ilgili kişilerin sunulan ürün ve hizmetlerden Türkiye'de faydalanması durumunda, yurt dışındaki veri sorumlusu da aynı esaslar çerçevesinde Kurul'a bildirimde

[248] Kişisel Veri İhlal Bildirim Formu: https://www.kvkk.gov.tr/SharedFolderServer/CMSFiles/8217d07e-5af7-43f0-ad02-a48cb1e23cd7.pdf (E.T.: 16.09.2024).
[249] Kişisel Veri İhlali Bildirimi Formu Kılavuzu

bulunmak zorundadır. [250]

Kurul'un kararı doğrultusunda, veri sorumluları bir veri ihlali müdahale planı hazırlamalıdır. Bu plan, veri ihlali durumunda kimlere raporlama yapılacağı, kanun kapsamında yapılacak bildirimler ve veri ihlalinin olası sonuçlarının değerlendirilmesi gibi konuları içermelidir. Bu planın belirli aralıklarla gözden geçirilmesi ve güncellenmesi gerekmektedir.[251]

Dijital platformlar, topladıkları kişisel verilerin hacmi göz önünde bulundurulduğunda kişisel verilerin korunması konusunda oldukça büyük bir sorumluluk taşımaktadır. Veri ihlallerinin zamanında ve doğru bir şekilde bildirilmesi hem ilgili kişilerin haklarının korunması hem de veri güvenliğinin sağlanması açısından kritiktir.

[250] Kişisel Veri İhlali Bildirimi Formu Kılavuzu
[251] Kişisel Veri İhlali Bildirimi Formu Kılavuzu

## SONUÇ

Bu tez, dijital platformlarda kişisel verilerin işlenmesi konusunu inceleyerek bu alandaki mevcut durum, yasal düzenlemeler ve karşılaşılan sorunlara ele almıştır. Dijitalleşmenin hızla ilerlediği günümüzde, kişisel verilerin korunması ve güvenliği hem ilgili kişiler açısından hem de veri sorumlularının yasal yükümlülükleri açısından kritik öneme sahiptir.

Bu çerçevede uygulamada dijital platformlarda kişisel verilerin işlenmesi faaliyetleri bakımından ortaya çıkan sorun ve çözüm önerileri aşağıdaki şekilde özetlenebilecektir:

- Küreselleşen dünyada Türkiye'de "dijital platform" kavramı tek bir mevzuat altında düzenlenmemektedir. Bu durum uyulması gereken hukuki düzenlemelerin ayrı ayrı değerlendirilmesi ve tam uyumun sağlanması için dijital platformların yükümlülüklerini belirlemesi bakımından zorluklar yaratmaktadır.

- "Kişisel veri" kavramı bakımından KVKK mevzuatında sınırlı bir tanım yapılmaması dijital platformlar ile elde edilen yeni türetilebilecek kişisel veri kategorileri için doğru bir yaklaşım olmuştur. Dijital platformlar, performans ve veri güvenliğini geliştirmek gibi çeşitli amaçlarla çok sayıda kişisel veri elde etmektedir. Bu kişisel verileri işlerken genelde veri sorumlusu sıfatını sahip ve küresel yapıdaki dijital platformların öncelikle KVKK nezdindeki yükümlülüklerini yerine getirmesi gerekmektedir.

- Küresel yapıdaki dijital platformların yurt dışında yerleşik veri sorumlusu niteliğinde olduğu hallerde Türkiye'de bir gerçek kişi veya tüzel kişi veri sorumlusu temsilcisi atayarak VERBİS'e kaydolması ve kişisel veri işleme faaliyetlerini VERBİS'e bildirmesi gerekmektedir. AB mevzuatında yer almayan bu yükümlülük yurt dışında yerleşik bir veri sorumlusu için alışık olmadığı bir düzenleme olsa da "hesap verilebilirlik" ilkesini sağlamak adına önemlidir.

- Aydınlatma yükümlülüğünün yerine getirilmesi sırasında dijital platformların veri işleme faaliyetlerini önceden belirlemesi gerekmektedir. Veri işleme faaliyetine başlamadan önce yerine getirilmesi gereken bu yükümlülük için şekilde şartı olmaması veri sorumluları bakımından serbest bir alan sağlasa da bu yükümlülüğünü yerine getirildiğinin ispat yükü veri sorumlusu dijital platforma aittir. Bu kapsamda dijital platformlar herhangi bir üyelik, satış veya kişisel veri işlemesi gereken işlemden önce okunasını zorunlu tutarak; "*okudum, anladım"* şeklinde bir ifade ile ispat yükümlülüğünü yerine getirebilirler.

- Dijital platformların elde ettiği kişisel verilerin doğru ve güncel olmasını sağlama yükümlülüğü elde ettiği kişisel verilerin hacmi arttıkça ağırlaşmaktadır. Bu noktada dijital platformlar elde ettiği özellik iletişim bilgileri için doğruluğunun teyit edilmesi amacıyla doğrulama kodu veya bağlantı gönderme gibi yöntemleri kullanabilirler. Ayrıca, kullanıcıların kendi kişisel verilerini kolayca güncelleyebileceği araçların elverişli bir şekilde sunulması da bu noktada uyumun sağlanmasında etkili olacaktır.

- Dijital platformlarda uygulamada *"opt-out"* rızanın uygulandığı haller ile karşılaşılmış ve Kurul tarafından bu şekilde bir rızanın geçersiz olduğu sonucuna varılmıştır. Dolayısıyla, sunulacak açık rıza metinlerinin "*opt-in"* şekilde kullanıcın özgür iradesini gösterecek şekilde sunulması gerekmektedir.

- Dijital platformların yurt dışına kişisel veri aktarması 12 Mart 2024 tarihinde mevzuat değişikliğine kadar uyum konusunda çıkmaza girmiş durumdadır. Bu değişiklik ile birlikte yurt dışına veri aktarım süreçlerini hukuka uygun bir şekilde yürütülmesi gerekmektedir. Veri işleme faaliyetinin niteliğine göre küresel yapıdaki dijital platformlar bakımından başta bağlayıcı şirket kurallarının hazırlanması, standart sözleşmelerin imzalanması değerlendirilmelidir.

- Dijital platformların çerezler aracılığıyla elde ettiği kişisel veriler

bakımından ise Kurul'un Çerez Rehberi ve kararları ışığında uyumu sağlamaları gerekmektedir. Bu kapsamda dijital platformların kullandığı çerezlerin amaçları belirleyici niteliktedir. Amaçların belirlenmesinden sonra veri işleme ilke ve şartları doğrultusunda dijital platformların aydınlatma yükümlülüğünü yerine getirmesi ve gerekmesi halinde ilgili kişilerin açık rızalarını talep etmesi gerekmektedir. Bu çerçevede dijital platformların elde ettiği kişisel verileri hangi amaçlarla, nasıl kullandığı, ilgili kişi haklarını kullanmasına ilişkin şeffaflığı sağlayacak çerez paneli gibi araçları geliştirmesi gerekmektedir.

- Kişisel verilerin korunmasında esas alınan temel nokta ilgili kişilerin haklarıdır. Dijital platformlar KVKK nezdindeki ilgili kişi haklarını aynı zamanda hizmet sunduğu diğer ülkelerdeki ilgili kişi haklarını gözeterek etkin bir şekilde kullanılmasını sağlamalıdır. Bunun için dijital platformların ilgili kişilerin kişisel verileri üzerinde daha fazla kontrol sahibi olmalarını sağlayabilecek şekilde ilgili kişi başvuruları için özel sistemler veya buna özgülenmiş e-posta adresleri oluşturması ve ilgili kişinin talebini kolaylıkla iletmesine imkân vermesi veri mahremiyetini sağlamak adına önemlidir.

- Kişisel veri güvenliğini sağlamak dijital platformların en geniş yükümlülüğüdür. Dijital platformun konusu ve yapısına göre öncelikle ihtiyacı olan veri güvenliği tedbirlerini analiz etmesi gerekmektedir. Bu analizler yürütülürken alınabilecek teknik ve idari tedbirler, Kurul kararları ve rehberleri ışığında değerlendirilmelidir.

- Dijital platformların profilleme faaliyetleri ve kullanıcı güvenliği konularına yönelik olarak KVKK'ya uygun hareket edilmesi ve olası risklerin bertaraf edilmesi için gerekli tedbirlerin alınması gerekmektedir. Bu çerçevede profilleme faaliyeti sonucu "kara liste" gibi uygulamaların geliştirilmesine önemli bir risk teşkil etmektedir. Bu riski bertaraf etmek adına ilgili kişi haklarından otomatik veri işleme faaliyetine itiraz hakkının

aktif bir şekilde kullanılmasına imkân tanınması gerekmektedir.

Dijital platformlarda kişisel veri işleme faaliyetleri KVKK nezdinde genel hükümler çerçevesinde değerlendirilmesinin yanı sıra işlenen verinin hacminin büyüklüğü, gelişen teknoloji neticesinde ortaya çıkan yeni kişisel veri kategorileri, veri sorumlusu dijital platformların veri mahremiyetini sağlamaya yönelik gerekli çalışmaları yürütmesi yerinde olacaktır. Böylece yeni gelişen teknolojilerde yürütülecek çalışmalar kişisel verilerin korunması odaklı yaklaşımlar getiren tasarımların oluşturulmasına imkân sağlanacaktır.

## KAYNAKÇA

- **Kitap ve Makaleler**

**AKGÜL, Aydın**; Danıştay ve Avrupa İnsan Hakları Mahkemesi Kararları Işığında Kişisel Verilerin Korunması, Beta Yayınları, İstanbul, 2016

**AŞIKOĞLU, Şehriban İpek**; Avrupa Birliği ve Türk Hukukunda Kişisel Verilerin Korunması ve Büyük Veri, On İki Levha Yayıncılık, İstanbul, 2018

**BAŞALP, Nilgün;** Avrupa Birliği Veri Koruması Genel Regülasyonu'nun Temel Yenilikleri, 2015, 21 Marmara Üniversitesi Hukuk Fakültesi Hukuk Araştırmaları Dergisi, 77 (Kısaltılmış: Başalp, Temel Yenilikler)

**BAŞALP, Nilgün;** Kişisel Verilerin Korunması ve Saklanması, Yetkin Yayınları, Ankara, 2004 (Kısaltılmış: Başalp, Kişisel Verilerin Korunması)

**BAYCIK, Gaye/ CİVAN, Orhan Ersun/ TOLU YILMAZ, Hazal/ BOSNA**, **Berrin**: "Platform Çalışanlarını Yasal Güvenceye Kavuşturmak: Sorunlar ve Çözüm Önerileri", Galatasaray Üniversitesi Hukuk Fakültesi Dergisi, S:1, 2021, 713-801, s. 716

**Cahn**, A., **Alfred**, S., **Barford**, P., & **Muthukrishnan**, S. An Empirical Study of Web Cookies. In *25th International Conference on World Wide Web (WWW'16).* Republic and Canton of Geneva, CHE: International World Wide Web Conferences Steering Committee. s. 891-901, 2016

**CASTELLUCCİA, C. ve NARAYANAN, A.;** 2012, Privacy considerations of online behavioural tracking, The European Network and Information Security Agency (ENISA)

**ÇEKİN, Mesut Serdar;** Avrupa Birliği Hukukuyla Mukayeseli Olarak 6698 sayılı Kişisel Verilerin Korunması Kanunu, On İki Levha, İstanbul, 2020

**ÇELİKEL**, **Serdar**; “Kişisel Verilerin Korunması Hukuku Kapsamında Veri Sorumlusu ve Veri Sorumlusunun Yükümlülükleri”, Doktora Tezi, Ankara Üniversitesi, 2021

**ÇOLAK, Betül / TEVETOĞLU, Mete**, "Dijital Reklamcılığın Yol Açtığı Hukuki Sorunlar ve Çözüm Önerileri", Maltepe Üniversitesi Hukuk Fakültesi Dergisi, 2021, S. 1, s. 43-86

**OLGUN Değirmenci,** “Yargısal İçtihatların Ortaya Çıkardığı Bir Hak: Unutulma Hakkı (Çerçevesi ve Hak Üzerine Düşünceler)”, THD, 2018, C.13, sf.144, 153-263.

**DEVELİOĞLU, Hüseyin Murat;** 6698 sayılı Kişisel Verilerin Korunması Kanunu ile Karşılaştırmalı Olarak Avrupa Birliği Genel Veri Koruma Tüzüğü Uyarınca Kişisel Verilerin Korunması Hukuku, On İki Levha Yayınları, İstanbul, 2017

**DOĞAN, Cihan;** Rekabet Hukuku ve İktisadi Bağlamında Dijital Platformlar, İstanbul, On İki Levha Yayıncılık, 2021

**DÜLGER, Murat Volkan;** Kişisel Verilerin Korunması Hukuku, Hukuk Akademisi Yayınları, İstanbul, 2020

**EKİN, Beste;** Kişisel Verilerin Korunması ve Rekabet Hukuku Boyutuyla Büyük Veri, On İki Levha Yayıncılık, İstanbul, 2021

**GELLERT, Raphael;** Personal data’s ever-expanding scope in smart environments and possible path(s) for regulating emerhing digital Technologies, International Data Privacy Law, 2021, Vol.11, No.2, Oxford University Press

**JULES, A. Jakobsson, M., & JAGATİC, T. N.** 2006, Cache cookies for browser authentication. 2006 IEEE Symposium on Security and Privacy (S&P’06). Doi: 10.1109/SP.2006.8, s.1

**TAŞTAN, Furkan Güven;** Türk Sözleşme Hukukunda Kişisel Verilerin Korunması, On İki Levha, İstanbul, 2017

**TIKKINEN-PIRI, Christina / ROHUNEN, Anna / MARKKULA, Jouni;** EU General Data Protection Regulation: Changes and Implications for Personal Data Collecting Companies, Computer Law&Security Reviews, Cilt:34, Sayı.1, Şubat 2018, s.134-153

**TOPARLAK, Rüya Tuna**; Veri Koruması Hukukunda Bağlayıcı Şirket Kuralları: 2016/679 Sayılı Genel Veri Koruma Tüzüğü ve 6698 Sayılı Kişisel Verilerin Korunması Kanunu Karşılaştırması, On İki Levha Yayıncılık, 2021.

**KAYA, Mehmet Bedii;** KVKK Reformu: 2024 Değişiklikler, (Dijital Baskı v.1.0), 2024

**KESER BERBER, Leyla; BİLGİLİ Ali Cem**, Güncel Gelişmeler Işığında Kişisel Verilerin Korunması Hukuku, 2020, On İki Levha Yayıncılık, 1. Baskı, İstanbul

**KÜZECİ, Elif**, Kişisel Verilerin Korunması, On İki Levha, Ankara, 2020

**KUENZLER, Adrian;** On (some aspects of) social privacy in the social media space, 2022, Vol.12, No:1, Oxford University Press

**OĞUZ, Sefer;** Kişisel Verilerin Korunması Hukukunun Genel İlkeleri, BEYDER. 2018, C. 13, S.2, s.121-138

**ÖNOK, Murat,** Kişisel Verilerin Korunması Bağlamında "Unutulma Hakkı" ve Türkiye Açısından Değerlendirmeler, İKÜHFD, 2017, C.16, S.1

**ÖZDEMİR, Hayrunnisa**, Elektronik Haberleşme Alanında Kişisel Verilerin Özel Hukuk Hükümlerine Göre Korunması, Seçkin Yayıncılık, 2009

**POLATER, Salih,** Kişisel Verilerin Reklam Amaçlı İşlenmesinde Hukuka Uygunluk Sebepleri, Kişisel Verileri Koruma Dergisi, Sayı: 1, Yıl: 2019,

**USTA, Oğuz**, Kişilik Hakkı Bağlamında Unutulma Hakkı,, Adalet Yayınevi, Ankara, 2023

**YAVUZ, Can;** İnternet'teki Arama Sonuçlarından Kişisel Verilerin Kaldırılması Unutulma Hakkı, 2. Baskı Seçkin Yayınları, Ankara, 2018

**YÜCEDAĞ, Nafiye;** Medeni Hukuk Açısından Kişisel Verilerin Korunması Kanunu'nun Uygulama Alanı ve Genel Hukuka Uygunluk Sebepler, İÜHFM, 2017, LXXV, S.2, s. 765-790

**YÜCEDAĞ, Nafiye;** Kişisel Verilerin Korunması Kanunu Kapsamında Genel İlkeler, KVKD, 2019, C.1, S.1, s.47-63 (Kısaltılmış: Yücedağ, Genel İlkeler)

**WHITE, Tiffany Barnett / ZAHAY, Debra / THORBJØRNSEN Helge / SHAVİTT Sharon**, 'Getting Too Personal: Reactance to Highly Personalized Email Solicitations', Marketing Letters, Sayı: 19(1), 2008

- **Ulusal ve Uluslararası Mevzuat**

95/46/EC sayılı Avrupa Direktifi, Erişim Linki: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A31995L0046 (Erişim Tarihi: 16.09.2024)

Avrupa Birliği Adalet Divanı, *Judgement of the Court (Grand Chamber), Case C-131/12, EU:C:2014:317, 13.05.2014, Agencia Española de Protección de Datos (AEPD) and Mario Costeja González v. Google Spain SL, Google Inc.* Erişim Linki: https://curia.europa.eu/juris/liste.jsf?td=ALL&language=en&jur=C,T&num=c-131/12 (Erişim Tarihi: 16.09.2024)

Avrupa Birliği Adalet Divanı, Verbraucherzentrale Bundesverband eV v. Planet49 GmbH (C 673/17). Erişim Linki: https://curia.europa.eu/juris/document/document.jsf;jsessionid=0A3A5F81BE1A7718127D2689B3033679?text=&docid=218462&pageIndex=0&doclang=en&mode=lst&dir=&occ=first&part=1&cid=590749 (Erişim Tarihi: 16.09.2024)

Avrupa Birliği, *Genel Veri Koruma Tüzüğü (GDPR)* Erişim Linki: https://eur-lex.europa.eu/eli/reg/2016/679/oj (Erişim Tarihi: 16.09.2024)

Avrupa Komisyonu, "Türkiye'nin veri koruma yeterliliğini reddetmesi ve Türkiye'nin veri koruma yasalarının AB'nin GDPR standartlarıyla uyumlu olmadığını belirtmesi." Erişim Linki: https://marpatas.com/en/european-commission-rejects-turkeys-data-protection-adequacy-impacts-and-future/ (Erişim Tarihi: 16.09.2024)

Avrupa Konseyi, 108 sayılı Kişisel Verilerin Otomatik İşlenmesi Karşısında Bireylerin Korunması Sözleşmesi Erişim Linki: https://rm.coe.int/1680078b37, (Erişim Tarihi: 16.09.2024)

CNIL, Closure of the injunction issued against GOOGLE. Erişim Linki: https://www.cnil.fr/en/closure-injunction-issued-against-google (Erişim Tarihi: 16.09.2024)

CNIL, Deliberation of the restricted committee No. SAN-2021-023 of 31 December 2021 concerning GOOGLE LLC and GOOGLE IRELAND LIMITED, Erişim Linki: https://www.cnil.fr/sites/cnil/files/atoms/files/deliberation_of_the_restricted_committee_no._san-2021-023_of_31_december_2021_concerning_google_llc_and_google_ireland_limited.pdf (Erişim Tarihi: 16.09.2024)

ILO, *World Employment and Social Outlook: The Role of Digital Labour Platforms in Transforming the World of Work*, Cenevre, 2021, Erişim Linki: https://www.ilo.org/publications/flagship-reports/role-digital-labour-platforms-transforming-world-work (Erişim Tarihi: 16.09.2024)

ISO, Standards Erişim Linki: https://www.iso.org/standards.html (Erişim Tarihi: 16.09.2024).

Kişisel Verileri Koruma Kurumu, 6698 sayılı Kanunda Yer Alan Temel Kavramlar, Erişim Linki: https://www.kvkk.gov.tr/SharedFolderServer/CMSFiles/8110dc3c-2856-4e54-9129-5e2e375469af.pdf (Erişim Tarihi: 16.09.2024)

Kişisel Verileri Koruma Kurumu, 6698 sayılı Kanunda Yer Alan Temel Kavramlar, Erişim Linki: https://www.kvkk.gov.tr/SharedFolderServer/CMSFiles/8110dc3c-2856-4e54-9129-5e2e375469af.pdf (Erişim Tarihi: 16.09.2024)

Kişisel Verileri Koruma Kurumu, Aydınlatma Yükümlülüğünün Yerine Getirilmesi Rehberi, Erişim Linki: https://www.kvkk.gov.tr/SharedFolderServer/CMSFiles/a569a068-c079-4189-b134-f57bc727af7d.pdf (Erişim Tarihi: 16.09.2024)

Kişisel Verileri Koruma Kurumu, Çerez Uygulamaları Hakkında Rehber, Erişim Linki: https://www.kvkk.gov.tr/SharedFolderServer/CMSFiles/fb193dbb-b159-4221-8a7b-3addc083d33f.pdf (Erişim Tarihi: 16.09.2024)

Kişisel Verileri Koruma Kurumu, Kişisel Veri Güvenliği Rehberi Erişim Linki https://www.kvkk.gov.tr/SharedFolderServer/CMSFiles/7512d0d4-f345-41cb-bc5b-8d5cf125e3a1.pdf (Erişim Tarihi: 16.09.2024)

Kişisel Verileri Koruma Kurumu, Kişisel Verilerin İşlenmesine İlişkin Temel İlkeler, Erişim Linki: https://www.kvkk.gov.tr/SharedFolderServer/CMSFiles/32ff74f6-9798-405a-b3d2-b42d28423fde.pdf (Erişim Tarihi: 16.09.2024)

Kişisel Verileri Koruma Kurumu, Madde ve Gerekçesi İle Kişisel Verilerin Korunması Kanunu (Bilgi Notu) ve Kişisel Verilerin Korunmasına İlişkin Terimler Sözlüğü, Erişim Linki: https://www.kvkk.gov.tr/Icerik/5388/Madde-ve-Gerekcesi-ile-Kisisel-Verilerin-Korunmasi-Kanunu-Bilgi-Notu-ve-Kisisel-Verilerin-Korunmasina-Iliskin-Terimler-Sozlugu (Erişim Tarihi: 16.09.2024)

Kişisel Verileri Koruma Kurumu, Veri Sorumlusu Veri İşleyen, Erişim Linki: https://www.kvkk.gov.tr/SharedFolderServer/CMSFiles/31d9c444-27a5-4a75-95b1-1ca9bdb81ea5.pdf (Erişim Tarihi: 16.09.2024)

Madde 29 Çalışma Grubu, *Guidelines on The Implementation Of The Court Of Justice Of The European Union Judgment On "Google Spain And Inc V. Agencia Española De Protección De Datos (Aepd) And Mario Costeja González*, Erişim Linki: https://ec.europa.eu/newsroom/article29/items/667236/en (Erişim Tarihi: 16.09.2024).

OECD Glossary of Statistical Terms, Erişim Linki: https://read.oecd-ilibrary.org/economics/oecd-glossary-of-statistical-terms_9789264055087-en#page39, (Erişim Tarihi: 16.09.2024)

OECD, *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*, 1980, Erişim Linki: https://www.oecd-ilibrary.org/docserver/9789264196391-

en.pdf?expires=1710964015&id=id&accname=guest&checksum=DBF322B08C808FC584FA61E85F578921, (Erişim Tarihi: 16.09.2024)

Rekabet Hukuku Çerçevesinde Veri Taşınabilirliği ve Dijital Platformların Veri Paylaşma Yükümlülüğü. Erişim Linki: https://www.youtube.com/watch?v=Eld7dTJfCQI (Erişim Tarihi: 16.09.2024).

**SEPİCİ GÜLEŞGEN**, Şive, Kişisel Verilerin Korunması Hukuku Açısından Meşru Menfaat Kavramının Değerlendirilmesi, İstanbul Bilgi Üniversitesi, Lisansüstü Programları Enstitüsü Bilişim ve Teknoloji Hukuku Yüksek Lisans Programı, İstanbul, 2021 (Yayınlanmayan Tez)

**ŞİMŞEK, Umman Tuğba**, "Veri madenciliği ve müşteri ilişkileri yönetiminde (CRM) bir uygulama," Doktora Tezi, İstanbul Üniversitesi, Sosyal Bilimler Enstitüsü, Sayısal Yöntemler Bilim Dalı, 2006. Tez bağlantısı: https://tez.yok.gov.tr/UlusalTezMerkezi/tezDetay.jsp?id=SHQeQrNLBdDS_RADHJThrg&no=PdfR5WEOenvfhwwSCkL6Vw (Erişim Tarihi: 16.09.2024)

- **Kurul Kararları**

Arabulucuların Veri Sorumluları Siciline Kayıt Zorunluluğundan İstisna Tutulması ile ilgili Kişisel Verileri Koruma Kurulunun 05/07/2018 Tarihli ve 2018/75 Sayılı Kararı (https://www.kvkk.gov.tr/Icerik/5270/2018-75) (Erişim Tarihi: 16.09.2024)

Gümrük Müşavirlerinin Sicile Kayıt İstisnası Hakkında Görüş Talebi" ile ilgili Kişisel Verileri Koruma Kurulunun 28/06/2018 Tarihli ve 2018/68 Sayılı Kararı (https://www.kvkk.gov.tr/Icerik/5269/2018-68) (Erişim Tarihi: 16.09.2024)

Araç kiralama programları yazılımcısı ve satıcısı firmalar tarafından, ilgili kişilerin verilerinin işlenmesi ve bu verilerin araç kiralama firmaları arasında paylaşılmasını sağlayan bir kara liste programı oluşturulması" hakkında Kişisel Verileri Koruma Kurulunun 23/12/2021 tarihli ve 2021/1303 sayılı Karar Özeti: https://www.kvkk.gov.tr/Icerik/7288/2021-1303 (Erişim Tarihi: 16.09.2024)

Veri sorumlusu Banka'nın, müşteri temsilcisi ile ilgili kişi arasında gerçekleştirilen görüşmeye ilişkin ses kaydı dökümünün ilgili kişiye sağlanması yönündeki talebi yerine getirmemesi" hakkında Kişisel Verileri Koruma Kurulunun 15/06/2023 Tarih ve 2023/1050 Sayılı Karar Özeti https://kvkk.gov.tr/Icerik/7769/2023-1050 (Erişim Tarihi: 16.09.2024)

Yeterli korumanın bulunduğu ülkelerin tayininde kullanılmak üzere oluşturulan form" hakkındaki Kişisel Verileri Koruma Kurulu'nun 02/05/2019 tarihli ve 2019/125 sayılı Karar Özet: (https://www.kvkk.gov.tr/Icerik/5469/-Yeterli-korumanin-bulundugu-ulkelerin-tayininde-kullanilmak-uzere-olusturulan-form-hakkindaki-02-05-2019-tarihli-ve-2019-125-sayili-Kurul-Karari) (Erişim Tarihi: 16.09.2024)

Amazon Turkey Perakende Hizmetleri Limited Şirketi hakkındaki başvuru ile ilgili Kişisel Verileri Koruma Kurulunun 27/02/2020 Tarihli ve 2020/173 Sayılı Karar Özeti: https://www.kvkk.gov.tr/Icerik/6739/2020-173 (Erişim Tarihi: 16.09.2024)

Banka mobil uygulamasında dijital parola belirlerken yüz verisinin işlenmesi suretiyle kişisel verilerin işlenmesi" hakkında Kişisel Verileri Koruma Kurulunun 03/08/2023 Tarihli ve 2023/1310 Sayılı Karar Özeti: https://kvkk.gov.tr/Icerik/7775/2023-1310 (Erişim Tarihi: 16.09.2024)

Bir Gerçek Kişinin Adının Geçtiği Köşe Yazısının Silinmesi Talebi: https://kvkk.gov.tr/Icerik/5407/-Bir-Gercek-Kisinin-Adinin-Gectigi-Kose-Yazisinin-Silinmesi-Talebi (Erişim Tarihi: 16.09.2024)

Bir internet sitesinde yer alan çerezlere ilişkin aydınlatma ve açık rıza metinlerinin sunulmaması" hakkında Kişisel Verileri Koruma Kurulunun 23/12/2022 tarihli ve 2022/1358 sayılı Karar Özeti: https://www.kvkk.gov.tr/Icerik/7595/2022-1358 (Erişim Tarihi: 16.09.2024)

Bir sigorta şirketinin ilgili kişiye vereceği hizmeti açık rıza şartına bağlaması sebebiyle Kuruma iletilen şikâyet hakkında Kişisel Verileri Koruma Kurulunun 03/09/2020 tarihli ve 2020/667 sayılı Karar Özeti, https://www.kvkk.gov.tr/Icerik/6878/2020-667 (Erişim Tarihi: 16.09.2024)

Hakkında hüküm verildiği suçtan dolayı cezası infaz edilen ilgili kişiye ait haberin yayımlandığı gazetenin internet sitesinden kaldırılması talebi" hakkında Kişisel Verileri Koruma Kurulunun 22/05/2020 tarihli ve 2020/414 sayılı Karar Özeti: https://kvkk.gov.tr/Icerik/6915/2020-414 (Erişim Tarihi: 16.09.2024)

İlgili kişi ile veri sorumlusu şirket arasında gerçekleştirilen telefon görüşmelerine ilişkin kayıtların ilgili kişiye verilmesi yönündeki talebin reddedilmesi hakkında" Kişisel Verileri Koruma Kurulunun 14/01/2020 Tarihli ve 2020/13 Sayılı Karar Özeti: https://www.kvkk.gov.tr/Icerik/6698/2020-13 (Erişim Tarihi: 16.09.2024)

İlgili kişinin cep telefonu numarasının kampanya adı altında bir dijital platform bayisi tarafından edinilmesi, işlenmesi ve rızası olmaksızın arama yapılması" hakkında Kişisel Verileri Koruma Kurulunun 04/06/2021 tarih ve 2021/548 sayılı Karar Özeti: https://kvkk.gov.tr/Icerik/7123/2021-548 (Erişim Tarihi: 16.09.2024)

İlgili kişinin, bir sadakat programı kapsamında veri sorumlusunca hukuka aykırı kişisel veri işlendiği yolundaki ihbarı" hakkında Kişisel Verileri Koruma Kurulunun 05/07/2019 tarihli ve 2019/198 sayılı Karar Özeti: https://kvkk.gov.tr/Icerik/7348/2019-198 (Erişim Tarihi: 16.09.2024)

Kişilerin Ad ve Soyadı ile Arama Motorları Üzerinden Yapılan Aramalarda Çıkan Sonuçların İndeksten Çıkarılmasına Yönelik Talepler ile ilgili olarak Kişisel Verileri Koruma Kurulunun 23/06/2020 Tarihli ve 2020/481 Sayılı Kararı: https://www.kvkk.gov.tr/Icerik/6776/2020-481 (Erişim Tarihi: 16.09.2024)

Kişilerin Ad ve Soyadı ile Arama Motorları Üzerinden Yapılan Aramalarda Çıkan Sonuçların İndeksten Çıkarılmasına İlişkin Değerlendirmede Dikkate Alınacak Kriterler: https://kvkk.gov.tr/SharedFolderServer/CMSFiles/68f1fb19-5803-4ef8-8696-f938fb49a9d5.pdf (Erişim Tarihi: 16.09.2024)

Kişisel Veri İhlali Bildirim Usul ve Esaslarına İlişkin Kişisel Verileri Koruma Kurulunun 24.01.2019 Tarih Ve 2019/10 Sayılı Kararına İlişkin Duyuru: https://www.kvkk.gov.tr/Icerik/5362/Veri-Ihlali-Bildirimi (Erişim Tarihi: 16.09.2024)

Kişisel Veri İhlali Bildirim Usul Ve Esaslarına İlişkin Kişisel Verileri Koruma Kurulunun 24.01.2019 Tarih Ve 2019/10 Sayılı Kararına İlişkin Duyuru: https://www.kvkk.gov.tr/Icerik/5362/Veri-Ihlali-Bildirimi (Erişim Tarihi: 16.09.2024)

Kişisel Verileri Koruma Kurulu, Yurtdışına Veri Aktarımında Veri Sorumlularınca Hazırlanacak Taahhütnamede Yer Alacak Asgari Unsurlar: (https://www.kvkk.gov.tr/Icerik/4236/Yurtdisina-Veri-Aktariminda-Veri-Sorumlularinca-Hazirlanacak-Taahhutnamede-Yer-Alacak-Asgari-Unsurlar) (Erişim Tarihi: 16.09.2024)

Kişisel Verileri Koruma Kurulu'nun Bağlayıcı Şirket Kuralları Hakkında Duyurusu: (https://www.kvkk.gov.tr/Icerik/6728/YURT-DISINA-KISISEL-VERI-

AKTARIMINDA-BAGLAYICI-SIRKET-KURALLARI-HAKKINDA-DUYURU) (Erişim Tarihi: 16.09.2024)

Kullanıcı Güvenliğine İlişkin Veri Sorumluları Tarafından Alınması Tavsiye Edilen Teknik ve İdari Tedbirlere İlişkin Kamuoyu Duyurusu https://www.kvkk.gov.tr/Icerik/7177/Kullanici-Guvenligine-Iliskin-Veri-Sorumlulari-Tarafindan-Alinmasi-Tavsiye-Edilen-Teknik-ve-Idari-Tedbirlere-Iliskin-Kamuoyu-Duyurusu (Erişim Tarihi: 16.09.2024)

Kurumsal e-posta hizmetinin, Google (gmail) üzerinden yine aynı uzantıya sahip olarak kullanılıp kullanılamayacağı ilişkin Kişisel Verileri Koruma Kurulu'nun 31/05/2019 Tarihli ve 2019/157 Sayılı Karar Özeti https://www.kvkk.gov.tr/Icerik/5493/2019-157 (Erişim Tarihi: 16.09.2024)

Özel Nitelikli Kişisel Verilerin İşlenmesinde Veri Sorumlularınca Alınması Gereken Yeterli Önlemler" ile ilgili Kişisel Verileri Koruma Kurulunun 31/01/2018 Tarihli ve 2018/10 Sayılı Kararı: https://www.kvkk.gov.tr/Icerik/4110/2018-10(Erişim Tarihi: 16.09.2024)

Özel Nitelikli Kişisel Verilerin İşlenmesinde Veri Sorumlularınca Alınması Gereken Yeterli Önlemler" ile ilgili Kişisel Verileri Koruma Kurulunun 31/01/2018 Tarihli ve 2018/10 Sayılı Kararı: https://www.kvkk.gov.tr/Icerik/4110/2018-10 (Erişim Tarihi: 16.09.2024)

Sorularla Veri Sorumluları Sicil Bilgi Sistemi (VERBİS): https://verbis.kvkk.gov.tr/UploadedFiles/SORULARLA_VERB%C4%B0S.pdf(Erişim Tarihi: 16.09.2024)

Tüzel kişiliğe ait elektronik ortamda yer alan verilerin başka bir tüzel kişilik tarafından talep edilmesi" hakkında Kişisel Verileri Koruma Kurulunun 19/11/2018 tarihli ve 2018/131 sayılı Kararı Özeti, https://www.kvkk.gov.tr/Icerik/5423/2018-131 (Erişim Tarihi: 16.09.2024)

Unutulma hakkı kapsamında ilgili kişinin arama motorunda adı ve soyadı ile bağlantılı sonuçların kaldırılması talebi"ne ilişkin Kişisel Verileri Koruma Kurulunun 08/12/2020 tarihli ve 2020/927 sayılı Karar Özeti: https://kvkk.gov.tr/Icerik/6871/2020-92 7(Erişim Tarihi: 16.09.2024)

Unutulma Hakkının Arama Motorları Özelinde Değerlendirilmesi: https://www.kvkk.gov.tr/SharedFolderServer/CMSFiles/11b6fd99-d42a-45b1-a009-21f2d36ded21.pdf (Erişim Tarihi: 16.09.2024)

Veri Sorumluları Siciline Kayıt Yükümlülüğünden İstisna Tutulacak Veri Sorumluları ile ilgili Kişisel Verileri Koruma Kurulunun 19/07/2018 Tarihli ve 2018/87 Sayılı Kararı (https://www.kvkk.gov.tr/Icerik/5271/2018-87) (Erişim Tarihi: 16.09.2024)

Veri Sorumluları Siciline Kayıt Yükümlülüğünden İstisna Tutulacak Veri Sorumluları ile ilgili Kişisel Verileri Koruma Kurulunun 02/04/2018 Tarihli ve 2018/32 Sayılı Kararı (https://www.kvkk.gov.tr/Icerik/4233/2018-32) (Erişim Tarihi: 16.09.2024)

Veri Sorumluları Siciline Kayıt Yükümlülüğüne İlişkin İstisna Kriterinde Değişiklik Yapılması Hakkında Kişisel Verileri Koruma Kurulunun 06/07/2023 Tarihli ve 2023/1154 Sayılı Kararı https://www.kvkk.gov.tr/Icerik/7647/2023-1154(Erişim Tarihi: 16.09.2024)

Veri sorumluları tarafından kişilerin telefon numarası, e-posta adresi gibi iletişim kanallarına Kanuna aykırı şekilde gönderilen üçüncü kişilere ait kişisel veriler hakkında Kişisel Verileri Koruma Kurulunun 22/12/2020 Tarihli ve 2020/966 sayılı İlke Kararı: https://www.kvkk.gov.tr/Icerik/6858/2020-966(Erişim Tarihi: 16.09.2024)

Veri sorumluları tarafından kişilerin telefon numarası, e-posta adresi gibi iletişim kanallarına Kanuna aykırı şekilde gönderilen üçün kişilere ait kişisel veriler hakkında Kişisel Verileri Koruma Kurulu'nun 22/12/2020 tarihli ve 2020/966 sayılı

İlke Kararı, (https://www.kvkk.gov.tr/Icerik/6858/2020-966) (Erişim Tarihi: 16.09.2024)

Veri sorumlusu bir havayolu şirketi tarafından ilgili kişiye ait çağrı merkezi görüşme kayıtlarının transkriptinin teslim edilmemesi" hakkında Kişisel Verileri Koruma Kurulunun 30/06/2020 tarihli ve 2020/504 sayılı Karar Özeti: (https://www.kvkk.gov.tr/Icerik/6932/2020-504) (Erişim Tarihi: 16.09.2024)

Veri sorumlusu tarafından ilgili kişiye yapılan veri ihlali bildiriminde yer alması gereken asgari unsurlara ilişkin, Kişisel Verileri Koruma Kurulunun 18.09.2019 tarih ve 2019/271 sayılı Kararı: https://www.kvkk.gov.tr/Icerik/5547/2019-271 (Erişim Tarihi: 16.09.2024)

Veri sorumlusu ve veri işleyenin tespitinde göz önünde bulundurulması gereken hususlar ile aydınlatma yükümlülüğünün kim tarafından yerine getirileceği"ne ilişkin Kişisel Verileri Koruma Kurulunun 30/01/2020 tarihli ve 2020/71 sayılı Karar Özeti: https://www.kvkk.gov.tr/Icerik/6874/2020-71(Erişim Tarihi: 16.09.2024)

Yurtdışında Yerleşik Tüzel Kişilerin Türkiye'deki Şubeleri ile İrtibat Bürolarının Sicile Kayıt Yükümlülüğü Hakkındaki Görüş Talebi ile ilgili Kişisel Verileri Koruma Kurulunun 23/07/2019 tarih ve 2019/225 sayılı Karar Özeti https://www.kvkk.gov.tr/Icerik/5545/2019-225 (Erişim Tarihi: 16.09.2024)