TÜRKİYE CUMHURİYETİ
ANKARA ÜNİVERSİTESİ
SOSYAL BİLİMLER ENSTİTÜSÜ
AVRUPA BİRLİĞİ VE ULUSLARARASI EKONOMİK İLİŞKİLER ANABİLİM DALI
AVRUPA BİRLİĞİ HUKUKU BİLİM DALI

KİŞİSEL VERİLERİN KORUNMASI ALANINDA GENEL VERİ KORUMA TÜZÜĞÜ'NDE VERİ İHLALİ BİLDİRİMLERİ

Yüksek Lisans Tezi

Narin AMBARKÜTÜK

Ankara, 2025

TÜRKİYE CUMHURİYETİ
ANKARA ÜNİVERSİTESİ
SOSYAL BİLİMLER ENSTİTÜSÜ
AVRUPA BİRLİĞİ VE ULUSLARARASI EKONOMİK İLİŞKİLER ANABİLİM DALI
AVRUPA BİRLİĞİ HUKUKU BİLİM DALI

KİŞİSEL VERİLERİN KORUNMASI ALANINDA GENEL VERİ KORUMA TÜZÜĞÜ'NDE VERİ İHLALİ BİLDİRİMLERİ

Yüksek Lisans Tezi

Narin AMBARKÜTÜK

Tez Danışmanı
Dr. Öğr. Üyesi Emriye Özlem ŞEKER

Ankara, 2025

TÜRKİYE CUMHURİYETİ
ANKARA ÜNİVERSİTESİ
SOSYAL BİLİMLER ENSTİTÜSÜ
AVRUPA BİRLİĞİ VE ULUSLARARASI EKONOMİK İLİŞKİLER ANABİLİM DALI
AVRUPA BİRLİĞİ HUKUKU BİLİM DALI

KİŞİSEL VERİLERİN KORUNMASI ALANINDA GENEL VERİ KORUMA TÜZÜĞÜ'NDE VERİ İHLALİ BİLDİRİMLERİ

Yüksek Lisans Tezi

Tez Danışmanı
Dr. Öğr. Üyesi Emriye Özlem ŞEKER

TEZ JÜRİSİ ÜYELERİ

Adı Soyadı

1-Prof. Dr. Sanem Suphiye BAYKAL

2- Prof. Dr. İlke GÖÇMEN

3- Dr. Öğr. Üyesi Emriye Özlem ŞEKER

Tez Savunma Tarihi

30.05.2025

TÜRKİYE CUMHURİYETİ
ANKARA ÜNİVERSİTESİ
Sosyal Bilimler Enstitüsü Müdürlüğü'ne,

Dr. Öğr. Üyesi Emriye Özlem ŞEKER danışmanlığında hazırladığım **KİŞİSEL VERİLERİN KORUNMASI ALANINDA GENEL VERİ KORUMA TÜZÜĞÜ'NDE VERİ İHLALİ BİLDİRİMLERİ (Ankara, 2025)"** adlı yüksek lisans tezimdeki bütün bilgilerin akademik kurallara ve etik davranış etik ilkelerine uygun olarak toplanıp sunulduğunu, başka kaynaklardan aldığım bilgileri metinde ve kaynakçada eksiksiz olarak gösterdiğimi, çalışma süresince bilimsel araştırma ve etik kurallarına uygun olarak davrandığımı ve aksinin ortaya çıkması durumunda her türlü yasal sonucu kabul edeceğimi beyan ederim.

11.06.2025
Narin AMBARKÜTÜK

İÇİNDEKİLER

KISALTMA LİSTESİ

AB : Avrupa Birliği

ABAD : Avrupa Birliği Adalet Divanı

ABİHA : Avrupa Birliği'nin İşleyişi Hakkında Antlaşma

AEPD : Agencia Española de Protección de Datos

AT : Avrupa Topluluğu

BT : Bilişim Teknolojileri

C- : Case

CIA : Central Intellince Agency

CNPD : Commission nationale pour la protection des données

DPO : Data Protection Officer

EDPS : European Data Protection Supervisor

GDPR : General Data Protection Regulation

GVKT : Genel Veri Koruma Tüzüğü

KVKK : Kişisel Verilerin Korunması Kanunu

OECD : Organisation for Economic Co-operation and Development

s. : Sayfa

T.C. : Türkiye Cumhuriyeti

v. : Versus

VKI : Verein für Konsumenteninformation

€ : Euro

GİRİŞ

Bu çalışmada Kişisel Verilerin Korunması alanında önemli mevzuattan birisi olan ve Avrupa Birliği (AB) tarafından çıkarılan Genel Veri Koruma Tüzüğü (GDPR) üzerinde durulacaktır.[1] Çalışmanın odak noktası ise "veri ihlali bildirimleri"dir. Veri ihlali bildirimlerine, GDPR hakkında temel bilgiler verildikten sonra değinilecektir. Çalışmanın araştırma sorusu "Veri ihlal Bildirimi Nedir?", "Kişisel Verilerin Korunması Alanında Genel Veri Koruma Tüzüğü'nde Veri İhlali Bildirimleri"dir. Bu çalışmada veri ihlali bildirimlerine odaklanılmasının temel nedeni, hem kurumlar açısından ciddi yasal sorumluluklar doğurması hem de bireylerin güvenliğini doğrudan etkilemesidir. Ayrıca uygulamada yaşanan gecikmeler, eksik bildirimler veya yanlış risk değerlendirmeleri, hem para cezalarına hem de itibar kaybına yol açabilmektedir. Bu nedenle bu tez çalışması, GDPR çerçevesinde kişisel veri ihlali bildirimlerinin nasıl işlediğini, uygulamada karşılaşılan sorunları ve önerileri analiz etmeyi amaçlamaktadır. Çalışma iki bölümden oluşmaktadır. Birinci bölümde GDPR'ın kavramları, ilkeleri ve güncel tartışmalar incelenmiştir. İkinci bölümde ise kişisel veri ihlali bildirimi, bildirim sonrası, etkili bildirim, yargı kararları, bildirimin iyileştirilmesi ve GDPR'ın etkileri ile Türk hukukunda veri ihlali bildirimi incelenerek ilerlenmiştir.

Veri ihlali bildirimleri önemlidir çünkü bireylerin temel hak ve özgürlüklerinin korunmasını sağlamaktadır. Ayrıca veri işleme faaliyetlerine karşı güven duyulabilmesini mümkün hale getirmektedir ve veri sorumlularının yükümlülüklerine dikkat etmelerini sağlamaktadır. Veri ihlali bildirimleri, ileride detaylı bir şekilde ele alınacağı üzere, GDPR'ın temel ilkelerinin uygulanabilmesinde önemli bir rol

[1] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), OJ L 119, 4.5.2016, s. 1–88.

oynamaktadır. Kişisel veri güvenliği alanında risklerin azaltılmasını sağlamaktadır. Dijital sistemde güven ve birbirine uyum değerlerini öne çıkarmaktadır. Küresel bağlamda da oldukça gündemde olan "kişisel verilerin korunması" konusu tüm ülkeleri birbiri ile bağlantılı olarak ilgilendirecek bir hal almıştır. Teknolojinin çok hızlı gelişmesi ile birlikte bu durum yeni ihtiyaçlar ortaya çıkarmıştır. Tarihsel açıdan, teknoloji alanında son elli yılda yaşanılan ilerleme önceki dönemlerden çok daha fazladır. Ayrıca hız açısından bakıldığında da teknoloji eski dönemlere göre daha hızlı gelişmiştir ve daha da hızlı bir şekilde her geçen gün gelişmeye devam etmektedir.

Tüm bu yaşanan gelişmeler hayatın her alanını etkilediği gibi, günlük olarak kullandığımız telefon, bilgisayar gibi cihazların kullanımını da etkilemiştir. Günümüzde bir kişinin telefonunda (özellikle akıllı telefonların kullanılmaya başlanması ile) o kişi ile ilgili bilinebilecek birçok bilgi depolanır hale gelmiştir. Bir kişinin adı, soyadı, adresi, yaşı, konum bilgisi gibi bilgiler buz dağının sadece görünen kısmıdır. Kişinin fotoğrafları ve videoları, yaptığı bir seyahatin rotası, cinsel yaşamı, sağlık verileri (kalp atış sayısı, günlük atılan adım sayısı gibi çok ayrıntılı ve belirgin bilgiler dahi), alışveriş yapma alışkanlıkları (ve bunlara uygun hazırlanan kişinin ilgi alanlarına özel reklamlar) gibi bilgiler depolanan bilgiler içinde ilk akla gelenlerdir.

Bu noktada depolanan bu bilgiler, şirketler veya kurumlar tarafından işlenip kendi stratejilerini belirlemede kullanılabilmektedir. Bu kişisel verilerin işlenip kullanılmasında kötü niyetli yaklaşımda bulunulma ihtimali ortaya çıkmıştır. Şöyle ki, tüm bu bilgileri kullanan şirketler veya kurumların, bilgilerin sızdırılmasına, satılmasına veya o kişisel verinin sahibini olumsuz etkilemesine engel olacak şekilde çalışmaları gerektiği üzerinde uzlaşılmaktadır. İşte bu noktada da devreye GDPR girmektedir. Günlük problemlerden doğan ihtiyaçlar, hukuk alanında da kendine yer bulmuştur ve AB tarafından bu şekilde bir tüzük hazırlanmıştır. GDPR'dan önce 1995 tarihli 95/46/EC sayılı "Kişisel Verilerin İşlenmesi ve Serbest Dolaşımı Bakımından Bireylerin

Korunmasına İlişkin Avrupa Parlamentosu ve Konsey Direktifi" bulunmaktaydı. Bu direktiften GDPR'a geçiş ihtiyacının nedenleri ise şöyle açıklanabilir: 95/46/EC sayılı direktif teknolojinin güncel dönemdeki kadar gelişmemiş olduğu bir dönemde kabul edildiğinden AB genelinde kişisel verilerle ilgili kuralların çağa uyması amacıyla 2016'da GDPR kabul edilmiştir.[2] GDPR'ın dibacesinde 95/46 sayılı Direktif ile alakalı durum açıklanmıştır. Dibacenin 9. paragrafına göre, 95/46 sayılı Direktif, gayesini ve prensiplerini sürdürse de AB genelinde kişisel verilerin dolaşımında üye devletler arası hukuki belirsizliğin önüne geçememiştir.[3] 95/46 sayılı direktif zamanına göre değerli bir direktif olsa da güncel durumda artık yenilenmesi gerektiği belirtilmekteydi.[4] 95/46 direktifinin her üye devletin kendi kurallarını koymasına imkân vermesi sebebiyle ortaya çıkan karışıklığı GDPR'ın ortadan kaldırması öngörülmüştür. AB'deki her işletmenin uyması gereken tek bir kılavuz olmuştur.[5] Bu kılavuz da GDPR'dır.

Her üye devletin ayrı kurallar koyması yerine GDPR ile kurallarda bütünlük sağlanmıştır ve AB dijital tek pazar alanında veri güvenliği açısından işletmelerin nelere dikkat etmeleri gerektiğinin yol haritası çizilmiştir.[6] AB'nin kişisel verilerin korunmasına ilişkin yetkisinin dayanağı olarak Avrupa Birliği'nin İşleyişi Hakkında Antlaşma (ABİHA)'nın 16. maddesi gösterilmektedir. Antlaşmanın 16. maddesi uyarınca "Herkes, kendisiyle ilgili kişisel verilerin korunması hakkına sahiptir. Avrupa Parlamentosu ve Konsey, Birlik hukuku kapsamına giren faaliyetlerin yürütülmesinde, Birlik kurum, organ, ofis veya ajansları ile üye devletler tarafından kişisel verilerin

[2] Dülger, M. V**., Avrupa Birliği Genel Veri Koruma Tüzüğü Bağlamında Kişisel Verilerin Korunması**, Yaşar Hukuk Dergisi, Cilt 1, Sayı 2, 2019, s. 71-174.
[3] GDPR Dibace 9.paragraf.
[4] Göçmen Uyarer, S**., Kişisel Verilerin Korunması Kanunu Ve Türk Ceza Kanunu Kapsamında Kişisel Verilerin Korunması**, Seçkin, 2020, s.65.
[5] Inspired eLearning https://inspiredelearning.com/blog/a-brief-history-of-the-gdpr/#:~:text=GDPR%20was%20created%20to%20replace,data%20is%20the%20common%20currency. Erişim Tarihi 29.12.2023.
[6] Daha ayrıntılı bilgi için bakınız. Övündür, F., **Dijital Tek Pazar Stratejisinin Hukuki Bağlamında Kişisel Veri Güvenliğinin Sağlanması**, İstanbul Ticaret Üniversitesi Sosyal Bilimler Dergisi, Sayı 38, 2020, s.118-131.
https://dergipark.org.tr/en/pub/iticusbe/issue/57051/780007 Erişim Tarihi 04.04.2025.

işlenmesi sırasında bireylerin korunmasına ve bu bilgilerin serbest dolaşımına ilişkin kuralları olağan yasama usulü uyarınca belirler. Bu kurallara uyulması, bağımsız otoritelerin denetimine tabidir."[7] 2016 yılında kabul edilen GDPR, 1995 direktifinin yerini almıştır ve üye devletlerin Mayıs 2018'e kadar kendi ülkelerinde GDPR'ı uygulamaya hazır hale getirmeleri için zaman verilmiştir.[8] AB Resmi Gazetesi'nde GDPR yayımlanmıştır. GDPR'ın 94. maddesinde yürürlüğe dair tarih belirtilmiştir. GDPR'ın 94. maddesi uyarınca 95/46 sayılı direktif 25 Mayıs 2018'den itibaren yürürlükten kaldırılmıştır ve eski direktife yapılan atıflar GDPR'a yapılmış gibi görülecektir. Eski direktifteki bireylerin korunması hakkında Çalışma Grubuna yapılan atıflar ise Avrupa Veri Koruma Kurulu'na (EDPB) yapılmış gibi görülecektir.[9] Mayıs 2018'de yürürlüğe dair süre dolmuş bulunmaktadır.

Bu noktada AB Hukuku'nda GDPR ile direktifin farkına değinmek doğru olacaktır. Tüzükler her üye devlette bağlayıcı yasal güce sahiptir ve tüm üye devletlerde belirli bir tarihte yürürlüğe girer. Direktifler, ulaşılması gereken belirli sonuçları ortaya koyar ancak her üye devlet, direktiflerin ulusal yasalara nasıl aktarılacağına karar vermekte özgürdür.[10] GDPR'ın oluşum sürecindeki etkenlerde güncel olayların da etkisi bulunmuştur. 2013 tarihli Snowden olayı ile yeni veri koruma kuralları ihtiyacına olan dikkat artmıştır ve AB kurumlarında veri güvenliği kaygısı büyümüştür. 24 Mayıs 2016'da GDPR metni son halini almıştır ve 25 Mayıs 2018'de yürürlüğe girmiştir.[11] GDPR, kuruluşların ve şirketlerin kişisel verileri dürüstlük dostu bir şekilde nasıl

[7] Avrupa Birliği'nin İşleyişi Hakkında Antlaşma (T.C. Dışişleri Bakanlığı Avrupa Birliği Başkanlığı Çevirisi) 16. madde. https://www.ab.gov.tr/files/pub/antlasmalar.pdf Erişim Tarihi 29.12.2023.

[8] Avrupa Veri Koruma Denetçisi https://edps.europa.eu/data-protection/data-protection/legislation/history-general-data-protection regulation_en#:~:text=In%202016%2C%20the%20EU%20adopted,as%20law%20across%20the%20EU. Erişim Tarihi 14.11.2023.

[9] GDPR 94. madde.

[10] Avrupa Birliği'nin İşleyişi Hakkında Antlaşma (T.C. Dışişleri Bakanlığı Avrupa Birliği Başkanlığı Çevirisi) 288. madde.

[11] Dal, U., **Avrupa Birliği Genel Veri Koruma Tüzüğü'nün ülke dışı uygulama yetkisi ve bu yetkinin uluslararası hukukta meşruiyeti**, Kişisel Verileri Koruma Dergisi, Cilt 1, Sayı 1, 2019, s. 21-33. https://dergipark.org.tr/en/pub/kvkd/issue/45759/553880 Erişim Tarihi 12.12.23

kullanmaları gerektiğine ilişkin zorunlu kuralları içeren bir AB tüzüğüdür.[12] Kişisel verilerin çalınması, yetkisiz kullanılması, satılması, değiştirilmesi gibi olumsuz olaylara karşı GDPR düzenlemeleri yapılmıştır. Zarar gerçekleşmeden önlenebilmesine ve veri güvenliğinin sağlanmasına önem verilerek yeterli önlemlerin alınmasına dikkat çekilmiştir.[13] Zarar gerçekleşmeden zararın önlenebilmesi, tamamen önlenemiyorsa azaltılması gayesi ile hareket edilmiştir.

Bu çalışmada GDPR merkezli ilerlenerek kişisel veri ihlali bildirimi incelenecektir. Kişisel veri ihlali bildirimi düzenlemesi, GDPR ile ilgili bilinmesi gereken noktalar açıklandıktan sonra irdelenecektir. GDPR'ın anlaşılabilmesi için temel kavramları ve ilkeleri, Avrupa Veri Koruma Kurulu, GDPR'ın uygulama alanı gibi değinilmesi gereken konuların ele alındığı bir arka planda ilerlenecektir. Bu arka planda kişisel veri ihlali bildirimleri, kişisel verilerin güvenliği alanının altına girmektedir. Veri ihlali bildiriminin GDPR'daki yeri, onun uygulanma araçlarından birisi olmasıdır. GDPR'ın temel ilkelerini destekleyen bir mekanizmadır. Kişisel veri ihlali bildirimi, bir veri ihlali yaşandığında denetim makamına veya veri öznesine ihlalin bildirilmesi anlamına gelmektedir. Veri ihlal bildirimi, veri sorumlusunun yükümlülük almasını sağlayıp hesap verebilirliği sağlamaktadır. Bildirim önemlidir çünkü bireylerin haklarını ve özgürlüklerini korumaktadır, ihlallerde zamanında ve yeterli cevap verilmesini sağlamaktadır. Kişisel veri ihlali bildirimi ise ileride denetim makamına bildirilmesi, veri öznesine (veri sahibine) bildirilmesi, bildirimde bulunması gereken unsurlar ve bildirim sonrası karşılaşılabilecek yaptırımlar doğrultusunda ele alınacaktır. Bir sonraki başlıkta GDPR ile ilgili bilgilendirmelerde bulunulacaktır.

[12] GDPR Summary https://www.gdprsummary.com/gdpr-summary/ Erişim Tarihi 14.11.2023.
[13] Çimen Bulut, İ., **Avrupa Birliği Genel Veri Koruma Tüzüğü Kapsamında Getirilen Yeni Teknik ve Yaptırım Mekanizmaları**, Anadolu Üniversitesi Sosyal Bilimler Dergisi, Cilt 20, Sayı 2, 2020, s. 127-142. https://dergipark.org.tr/en/pub/ausbd/article/758041 , Erişim Tarihi 09.12.23.

BİRİNCİ BÖLÜM

1. AVRUPA BİRLİĞİ GENEL VERİ KORUMA TÜZÜĞÜ

Bu çalışmanın konusu olan veri ihlali bildirimi GDPR'da düzenlenmektedir, bu nedenle bu başlıkta ilk olarak GDPR'ın genel yapısı ve veri ihlali bildiriminin GDPR'daki yeri ele alınacaktır. Daha sonra alt başlıklarda veri ihlali bildirimi ile bağlantılı GDPR kavramları, Avrupa Veri Koruma Kurulu ve GDPR'ın uygulanma alanı ele alınacaktır. Böylelikle veri ihlalinin nasıl bir hukuki çerçeve içinde yer aldığı belirlenmiş olacaktır. Bu terimde AB tarafından hazırlanan 2016/679 sayılı GDPR kastedilmektedir. Tüzüğün orijinal adı ise "*General Data Protection Regulation*" olarak geçmektedir ve "GDPR" şeklinde kısaltılmaktadır. GDPR, 95/46 sayılı direktifi kaldırıp AB genelinde veri güvenliği kurallarının tekelinin oluşmasını sağlamıştır.[14] Bu sebeple hem AB'de hem de dünya genelinde oldukça önemli bir konuma sahiptir.

1.1. Avrupa Birliği Genel Veri Koruma Tüzüğü'ne İlişkin Genel Bilgiler

Bu alt başlıkta GDPR'ın daha açık ve bütüncül şekilde anlaşılabilmesini sağlamak amacıyla temel nitelikte bilgilendirmelere yer verilecektir. GDPR, bireylerin kişisel verilerinin işlenmesinde yüksek düzeyde koruma sağlamayı amaçlamaktadır. GDPR'ın 1. maddesinin 1. fıkrası uyarınca, GDPR gerçek kişilerin veri işleme faaliyetinde korunmasına dair normları belirlemektedir.[15] Yine 1. maddenin 2. fıkrası uyarınca ise GDPR'ın kişilerin temel hak ve özgürlüklerini koruduğunu belirterek GDPR'ın konu ve amaçlarına değinilmiştir.[16] Kişisel verileri işlenen kişilerin haklarını, veri işleme faaliyetinde bulunanların yükümlülüklerini, kurallara uyum sağlama yöntemlerini ve kurallara uymayanlar hakkında uygulanacak yaptırımları

[14] Korkmaz, İ., **Kişisel Verilerin Ceza Hukuku Kapsamında Korunması**, Seçkin, 2019. s. 239-240.
[15] GDPR 1. madde 1. fıkra.
[16] GDPR 1. madde 2. fıkra.

öngören GDPR, giderek daha fazla kişisel verinin işlendiği günümüzde, veri gizliliği ve güvenliği konusunda uluslararası aktörleri ve üçüncü ülkeleri de etkileyen bir düzenlemedir.[17] Kişisel verilerin korunmasına dair hak, geçmişten günümüze gelen ve günümüzde önemi daha çok ortaya çıkan bir haktır. Bazı hakların bir parçası olarak geçmişte de düzenlenmiştir.[18] Bazı haklara örnek olarak özel hayatın gizliliği veya özel hayata ve aile hayatına saygı hakları verilebilir. Bu hakların altında düzenlenen kişisel verilerin korunması hakkı sonradan kendi önemine layık yerini almıştır.[19] Neredeyse yarım asır önce düzenlenmiş belgeler ile düzenlenmeye çalışılmış olması ise kişisel veri konusunun önemini vurgular niteliktedir.

Bu belgelere örnek olarak; Ekonomik İş Birliği ve Kalkınma Teşkilatı'nın (OECD) 23.09.1980 tarihli Özel Yaşamın Gizliliğinin ve Sınır Ötesi Kişisel Veri Dolaşımının Korunmasına İlişkin Rehber İlkeler[20], 28 Ocak 1981 tarihli Avrupa Konseyi tarafından hazırlanan 108 No'lu Kişisel Verilerin Otomatik İşleme Tabii Tutulması Karşısında Bireylerin Korunması Sözleşmesi (108 No'lu Sözleşme)[21] verilebilir. Devamında; 24 Ekim 1995 tarihli 95/46 Sayılı Kişisel Verilerin İşlenmesi ve Serbest Dolaşımı Bakımından Bireylerin Korunmasına İlişkin Avrupa Parlamentosu ve Konsey Direktifi[22], 27 Nisan 2016 tarihli ve 2016/680 sayılı Yetkili Makamlar Tarafından Suçun Önlenmesi, Soruşturulması, Tespiti veya Kovuşturulması veya Cezai Süreçlerin Yürütülmesi Amacıyla İşlenen Kişisel Verilere İlişkin Gerçek Kişilerin

[17] T.C. Dışişleri Bakanlığı Avrupa Birliği Başkanlığı Haberler. https://www.ab.gov.tr/ab-genel-veri-koruma-tuzugu-gdpr-turkceye-cevrildi_53650.html Erişim Tarihi 14.11.2023.
[18] Dülger, s. 71-174.
[19] Dülger, s. 71-174.
[20] Organisation for Economic Co-operation and Development (OECD), Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data, 23.09.1980.
[21] Council of Europe. (1981). Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Convention 108). Strasbourg, 28.01.1981. European Treaty Series – No. 108.
[22] Directive 95/46/EC of the European Parliament and of the Council of 24.10.1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, OJ L 281, 23.11.1995, s. 31–50.

Korunmasına ve Bu Tür Verilerin Serbest Dolaşımına Dair Direktif[23] ve 2016/679 sayılı GDPR örnek verilebilir. 108 No'lu Sözleşme ise daha sonra 18 Mayıs 2018 tarihinde 108+[24] şeklinde yenilenmiştir. Bunların dışında Avrupa Birliği Temel Haklar Şartı'nın 8. maddesinde kişisel bilgilerin korunmasına değinilmiştir.

Temel Haklar Şartı'nın 8. maddesi uyarınca "Herkes, kendine ait kişisel bilgilerin korunması hakkına sahiptir. Söz konusu bilgiler, hukuka uygun bir şekilde, belli amaçlar için ve ilgili kişinin iznine veya yasaların koyduğu diğer haklı nedenlere dayanılarak işleme tabi tutulmalıdır. Herkes, kendisi ile ilgili olarak toplanmış verilere erişmek ve bunların düzeltilmesini sağlamak hakkına da sahiptir."[25]

GDPR'ın AB dışında sınır aşırı etkisi bulunmaktadır. Hâlihazırdaki en güncel ve önemli konulardan biri olan kişisel verilerin korunması ile çoğu birey karşılaşmaktadır. Konunun güncelliğine kısaca mevcut bir örnek ile değinilecek olursa, kişisel verilerin korunması önümüze "aydınlatma formu onayı" şeklinde çıkmaktadır. Bu durum standart bir uygulama haline gelmiştir. GDPR'ın kişisel veri kullanan işletmelere getirdiği bir yükümlülük türüdür. GDPR 13. maddede düzenlenen aydınlatma formu onayı, kişisel verileri veri sahibinden alan işletmelerin veri işleme faaliyetlerine yansımaktadır. Kısaca açıklamak gerekirse, kişisel verilerin veri sahiplerinden toplanırken belirtilmesi gereken bilgiler ilgili maddede sayılmıştır ve aydınlatma formu da bu bilgileri ihtiva eden bir formdur. Kişisel veriler bir ürüne dönüşmüştür. Örneğin önceden internette araştırılan bir ürün ile daha sonra reklam olarak tekrar

[23] Directive (EU) 2016/680 of the European Parliament and of the Council of 27.04.2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data,
OJ L 119, 4.5.2016, s. 89–131.

[24] Council Decision (EU) 2019/682 of 9 April 2019 authorising Member States to sign, in the interest of the European Union, the Protocol amending the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data.
Official Journal of the European Union, L 115, 02.05.2019, s. 7–9.

[25] Avrupa Birliği Temel Haklar Şartı 8. madde (Türkçe Çevirisi).
http://www.ceidizleme.org/ekutuphaneresim/dosya/687_1.pdf Erişim Tarihi 03.01.2024.

karşılaşılmaktadır.[26] Çoğu zaman tamamı okunmadan onay verilen bu açık rıza formları, aydınlatma formları aslında yeni yasal düzenlemeler olan 6698 sayılı Kişisel Verilerin Korunması Kanunu'nun (KVKK) ve AB tarafından hazırlanan GDPR'ın getirdiği yükümlülüklerin sonucudur. Bu iki mevzuat özellikle Türkiye için en önemli çalışmalardandır. Bunun sebebi ise 6698 sayılı KVKK'nın günümüzde Türkiye'de yürürlükte olmasıdır ve AB gerçek veya tüzel kişileriyle bağlantı durumuna göre de buradaki şirketlerin de GDPR ile uyumlu olmalarının gerekmesidir. Ancak GDPR'ın alanı daha da geniştir ve birden çok coğrafyada etkili olabilmektedir. Buna daha sonra GDPR Sınır Aşırı Etkisi başlığında değinilecektir.

GDPR'nin veri ihlali bildirimi konusundaki net ve bağlayıcı hükümleri, sistemik şeffaflık sağlamaktadır. Buna karşın KVKK'nın daha genel ifadelerle yetinmesi, ihlal durumlarının denetim ve yaptırım açısından yeterince öngörülebilir olmamasına neden olabilmektedir. Bu fark, birey haklarını koruma kapasitesini doğrudan etkilemektedir. Alan olarak ise GDPR'da olup da KVKK'da olmayan bazı konular bulunmaktadır. Bunlara örnek olarak; çocuklara ilişkin düzenlemeler, hassas verilerin işlenmesi açısından "zorunlu veri koruma görevlisi" belirlenmesi ve riskli veri işleme faaliyetleri açısından ise "zorunlu veri koruma etki değerlendirmesi" yapılması, veri sahibinin kişisel verisini yetkili veri sorumlusundan bir başka veri sorumlusuna taşıyabilmesi, unutulma hakkı verilebilir.[27]

Çocuklara ilişkin düzenlemelere sebep olarak ise, onların yetişkin bireylere kıyasla daha savunmasız olmaları gösterilebilir. Çocuklar veri güvenliği ile alakalı tehlikelerden veya haklardan haberdar olmayacağından GDPR tarafından korunmuşlardır.[28] GDPR'da kişisel veriyle ilgili her işlemi gerçekleştiren sorumlu iken

[26] Dal, s. 21-33.
[27] KVKK Asistan https://www.kvkkasistan.com/Haberler/turkiye%E2%80%99de-kurulu-sirketlerin-gdpr-uyum-sorumlulugu/79 Erişim Tarihi 03.01.2024.
[28] Voigt, P., von dem Bussche, A., **The EU General Data Protection Regulation (GDPR),** Springer, 2017, s. 21.

KVKK'da sorumluluk veri sorumlusundadır.[29] GDPR 9. maddede KVKK'ya göre daha açıklayıcı çocukların verilerinin işlenmesine dair bilgiler verilmiştir.[30]

Teknolojinin gelişmesi, kişisel veri güvenliği alanında etkilere sebep olmaktadır. Güncel durumda insanlar kendileri ile ilgili pek çok kişisel veriyi kendileri sosyal medyada paylaşmaya başlamıştır ve bu durum yeni bir toplum düzeni oluşmasına yol açmaktadır.[31] Bu konuda en çok karşılaşılan durumlardan birisi de veri ihlalleri veya veri ihlali tehlikesidir. Bu durum için GDPR içinde de ayrıca belirtildiği üzere veri sorumlusu, veri işleyen gibi görevli özneler bulunmaktadır.

Veri ihlalleri somut örnekleri de bulunmakla beraber, kişisel verilerin açığa çıkması, satılması, pazarlanması, kötü niyetle kâr elde edilmesi açısından oldukça zarar verici olabilmektedir. Örneğin, 2021 yılında Lüksemburg Ulusal Veri Koruma Komisyonu (CNPD), Amazon.com Inc.'e 746 milyon € idari para cezası vermiştir. Amazon'un veri işlemesine ilişkin yapılan incelemede uygun şekilde rıza alınmadan hedefli reklamcılık yapması sebebiyle ihlal gerçekleştiği ortaya çıkmıştır.[32] Bu ceza Lüksemburg Ulusal Veri Komisyonu tarafından verilmiştir.[33] Somut bir şekilde analiz etmek gerekirse, bu cezaya GDPR'a aykırı şekilde veri işlemesi ile davranışa bağlı reklamcılık yapılması sebep olmuştur. Ceza, şirketlerin reklam yöntemlerini gözden geçirmesine neden olmuştur ve alanında örnek teşkil etmektedir. Rızanın açıkça verilmesinin önemine dikkat çekilmiştir ve ihlal yaşanmamasının GDPR'a uygunluk için yeterli olmadığı anlaşılmıştır. Verilerin korunmasına sadece veri ihlalinde değil veri işlemesinde de dikkat edilmesi gerektiğini ortaya çıkarmıştır. Veri ihlallerinin ise

[29] KVKK Asistan https://www.kvkkasistan.com/Haberler/turkiye%E2%80%99de-kurulu-sirketlerin-gdpr-uyum-sorumlulugu/79 Erişim Tarihi 03.01.2024
[30] Taşçı Aydemir, E., Kişisel Verilerin Kaydedilmesi Suçu, Seçkin, 2022, s.34.
[31] Yılmaz, T., **Avrupa Birliğinde Kişisel Verilerin Korunması Hukuku**, Adalet, 2022. s. 42.
[32] La Justice https://justice.public.lu/fr/actualites/2025/03/tribunal-administratif-jugement-amazon-amende-cnpd.html Erişim Tarihi 07.04.2025.
[33] CNPD decision regarding Amazon Europe Core S.À R.L. https://cnpd.public.lu/en/actualites/national/2025/03/amazon-decision.html Erişim Tarihi 07.04.2025.

bildirimleri açısından belli bazı kurallar (örneğin 72 saat kuralı 33. maddede) GDPR'da bulunmaktadır. Kişisel verinin ihlalini bildirme sorumluluğu ihlalin tespitinden itibaren ortaya çıkmaktadır ve tespit edilemeyen ihlal bildirilemeyeceğinden fark edilmeme tehlikesi bulunmaktadır.[34] Bu nedenle veri ihlali bildirimlerinin oldukça etkili bir şekilde yapılması önem taşımaktadır. Veri güvenliği kişilerin gizliliğine dair bir hak olması sebebiyle kurallar ile korunmaktadır.[35] Veri ihlali sürecinde kaybedilen zaman ve ne kadar sızıntı yaşandığı da önemlidir. Veri ihlali yaşanana kadar nasıl önlemler alındığı ve ihlalden sonra neler yapıldığı da dikkat edilmesi gereken bir durumdur. Bu hususlar, bildirimin yapılmasının daha etkili ve hatta uygulamaya yönelik iyileştirilebilir yönlerinin olduğunu karşımıza çıkarmaktadır. Bu nedenle bu çalışmada bu noktalara önem verilecektir.

Son olarak, GDPR ile veri ihlali bildirimi bağlantısı şöyle açıklanabilir: GDPR, AB ve etki çevresinde kişisel verilerin korunmasına ilişkin temel yasal düzenlemedir ve bu kapsamda veri ihlal bildirimlerini de düzenlemektedir. Veri ihlal bildirimi ise GDPR'a aykırı durumlarda GDPR'ı hedeflerine uygunluğu tekrar sağlama yollarından biridir ve GDPR'ın parçasıdır. Hem GDPR hem de GDPR'ın veri ihlal bildirimi maddeleri bireylerin veri güvenliğini korumayı amaçlamaktadır ve şeffaflığı, hesap verebilirliği teşvik etmektedir. Bu ilkeler ileride ayrıca ele alınacaktır. GDPR, veri ihlali bildirimi için denetim makamlarına da ek roller vermektedir. Veri işleyenler ve veri sorumlularının GDPR'ın koyduğu ilkelere uyarak hareket etmesi, bir veri ihlali durumunda karşılaşılabilecek zararı azaltmayı hedeflemektedir. Dolayısıyla, bu iki kavram biri diğerini tamamlayan parça olarak değerlendirmektedir.

[34] Sevindi N. S., Ordu., M. E., **AB ve Türk Hukukunda Veri İhlalinin Tespiti ve Bildirim Süresinin Karşılaştırmalı Değerlendirmesi**, Kişisel Verileri Koruma Dergisi, Cilt 5, Sayı 1, 2023, s.12-22.
[35] Seçkin, A. Z., **Türk Kişisel Verileri Koruma Mevzuatının Avrupa Birliği Genel Veri Koruma Tüzüğü İle Uyumlaştırılması Sürecinde Doğabilecek Sorunlar Ve Bu Sorunlara Yönelik Çözüm Önerileri**, Yeditepe Üniversitesi Akademik Açık Arşiv. https://openaccess.yeditepe.edu.tr/yayinaea/Ayca%20Zanbaklar%20Se%C3%A7kin_Preprint_653903412ac2e.pdf Erişim Tarihi 12.12.23.

Bir sonraki alt başlıkta, kişisel veri ihlal bildirimine ilişkin GDPR hükümlerinin daha anlaşılır olabilmesi için bununla bağlantılı temel GDPR kavramları ele alınacaktır.

1.2. Veri İhlali Bildirimi İle Bağlantılı Genel Veri Koruma Tüzüğü Kavramları

GDPR ile ilgili genel bilgiler sunulduktan sonra bu alt başlıkta GDPR'da geçen ve veri koruma için yapılan tüm faaliyetlerin anlaşılabilmesi için bilinmesi gereken temel kavramlar ele alınacaktır. Bu inceleme kavramların GDPR'daki madde sıralamasına göre yapılacaktır. Böylelikle veri ihlali ele alınırken kullanılacak kavramların hukuki tanımı ve uygulamasını ortaya koymak suretiyle çalışmanın hukuki unsurları belirlenmiş olacaktır.

1.2.1. Kişisel Veri Kavramı

Veri ihlali tanımında geçen en önemli unsurlardan biri kişisel veridir. Kişisel veri bir kişiyi teşhis edebilecek bir veridir. Veri kullanılarak bir kişinin kim olduğuna ulaşılabiliyorsa bu veri, kişisel veri olmaktadır. Kişisel veri kavramı GDPR'da açıklanmıştır. GDPR'ın 4. maddesinin 1.fıkrası uyarınca kişisel veri kim olduğu belli olan veya belirlenebilir olan bir birey hakkında her çeşit bilgidir. Kim olduğu belirlenebilecek kişi, adı ve soyadı, fiziksel özellikleri, yer bilgisi, psikolojik bilgileri, finansal bilgileri gibi verilerine dayanarak bulunabilecek kişiyi ifade etmektedir.[36] Bu maddede kişisel veri tanımı yapılmakla yetinilmeyip bir de tanımın içinde geçen kimliği belirlenebilir bir gerçek kişi kavramı açıklanmıştır. Bu kişisel veri türlerinden kişinin tıbbi veya dini bilgileri diğerlerinden daha hassas kişisel veriler olarak görülmektedir. Bu özel kategorilerdeki kişisel verilerden GDPR 9. maddede bahsedilmiştir. Bu bilgiler,

[36] GDPR 4. madde 1. fıkra.

kişinin özel hayatına dair ve kritik bilgiler olması nedeniyle özel olarak nitelendirilmiştir.

Avrupa Birliği Adalet Divanı (ABAD), Peter Nowak v Data Protection Commissioner davasında (Case C-434/16) kişisel veri kavramının kapsamını genişletmiştir. ABAD, bir sınavda adayın verdiği yazılı cevapların ve sınav değerlendiricisinin bu cevaplara ilişkin yorumlarının, adayın kimliğini belirlemeye olanak tanıyan bilgiler içerdiğini ve bu nedenle kişisel veri olarak değerlendirilmesi gerektiğini belirtmiştir.[37] Bu karar, kişisel verinin sadece açık kimlik bilgileriyle sınırlı olmadığını, bireyin tanınmasını sağlayan her türlü bilginin bu kapsama girebileceğini ortaya koyar niteliktedir. Neyin kişisel veri kapsamına girdiği ABAD sayesinde net olarak anlaşılmıştır.

Kişisel verinin, çalışmanın temel kavramlarından olması sebebiyle bu kavramın Türk hukukundaki tanımına kısaca değinilecektir. 6698 sayılı Kişisel Verileri Koruma Kanunu'nun gerekçesi uyarınca "Bu bağlamda sadece bireyin adı, soyadı, doğum tarihi ve doğum yeri gibi onun kesin teşhisini sağlayan bilgiler değil, aynı zamanda kişinin fiziki, ailevi, ekonomik, sosyal ve sair özelliklerine ilişkin bilgiler de kişisel veridir. Bir kişinin belirli veya belirlenebilir olması, mevcut verilerin herhangi bir şekilde bir gerçek kişiyle ilişkilendirilmesi suretiyle, o kişinin tanımlanabilir hale getirilmesini ifade eder."[38]

Kişisel veri kişi ile ilgili her tür bilgidir. Tüzel kişilerin ve vefat edenlerin verileri KVKK kapsamı dışındayken GDPR dibacesinin 27.paragrafında vefat edenlere ilişkin veriler üye devletin kurallarına bırakılmıştır.[39] GDPR'ın dibace kısmının 27.

[37] Case C-434/16 (Court of Justice), Peter Nowak v Data Protection Commissioner [2017], ECLI:EU:C:2017:994, 34.paragraf.
[38] KVKK Gerekçesi 3. madde.
[39] Oğuz, S., **Kişisel Verilerin Korunması Hukukunun Genel İlkeleri**, Bilgi Ekonomisi Ve Yönetimi Dergisi, Cilt 13, Sayı 2, 2018, s.121-138. https://dergipark.org.tr/en/pub/beyder/issue/41709/425303 Erişim Tarihi 12.12.23

paragrafına göre GDPR vefat eden bireylerin bilgileri için geçerli olmamaktadır. Ancak üye devletler kendileri hukuki kurallar koyabilmektedirler.[40] Kişisel veriler nerede bulunursa bulunsun veri öznelerinin haklarına önem verilmelidir.[41] Bu konuda üye devletlere çalışabilecekleri bir alan tanınmıştır.

Veri ihlali bildirimi ile kişisel veri kavramı birbirine derinden bağlıdır. Kişisel veri olmadan bir veri ihlali bildirimi gerçekleşemez. Bildirim ancak kişisel veri dahil olduğunda yapılmaktadır. Kişisel veri olmadan bildirilebilecek bir veri ihlali de oluşmamaktadır. Örneğin bir şirketin sistemi hacklendiğinde hiçbir kişisel veri etkilenmediyse bu olay GDPR kapsamına girmeyebilmektedir. Veri ihlali bildiriminin amacı kişisel verileri ihlale uğrayan veri öznelerini korumaktır. Risk varlığında, veri ihlali bildirimi de kişisel veri de veri öznesini koruma amaçlı hareket etmektedir.

1.2.2. Veri Sorumlusu veya Veri Kontrolör Kavramı

Veri sorumlusu veya veri kontrolörü, toplanan kişisel verilerin nasıl kullanılacağını belirleyen kişi veya kuruluştur. Veri sorumlusu, kişisel verilerin ne için kullanılacağını, bu kişisel verilere kimin ulaşabileceğini, ne kadar süre ulaşılabileceğini belirlemektedir. Veri Sorumlusu veya veri kontrolör kavramı GDPR'da düzenlenmiştir. 4. maddenin 7.fıkrası uyarınca veri sorumlusu veya veri kontrolörü gerçek veya tüzel kişi olabilmektedir ve kamu kurumu olarak da karşımıza çıkabilmektedir. Veri işleme faaliyeti, GDPR veya üye devletin kurallarına göre yapılıyorsa veri sorumlusunun görevlendirmesi de aynı kurallar üzerinden yapılabilmektedir.[42] Veri sorumluları,

[40]GDPR Dibace 27.paragraf.
[41]Daha ayrıntılı bilgi için bakınız. Drechsler, L.,**Individual Rights in International Personal Data Transfers Under the General Data Protection Regulation. Review of European Administrative Law,** Cilt 16, Sayı 1, 2023, s. 35–56. https://doi.org/10.7590/187479823X16800083010347
[42]GDPR 4. madde 7. fıkra.

verileri ticaret, bilimsel araştırma, müşteri hizmetleri gibi nedenlerle düzenleyen gerçek veya tüzel kişiler olabilmektedir.[43]

Ayrıca yine GDPR'ın dibace kısmındaki paragraflardan 63. paragraf uyarınca veri sorumlusu, veri öznesinin kendi verisine ulaşabileceği bir sistem sunmalıdır ancak telif hakkı veya ticari sır gibi başka bireylerin haklarını engellememelidir.[44] Ayrıca iletişimde şeffaflığın veri öznesi ile veri sorumlusu arasındaki dengede önemi bulunmaktadır.[45] Veri öznelerinin hangi verilerinin işlendiğini bilmeye hakları olduğundan kendi kişisel verilerine güvenli bir şekilde erişebilmelerinin sağlanması öngörülmüştür.

Veri sorumlusu kavramı ile ilgili olarak ABAD, Fashion ID GmbH & Co. KG v Verbraucherzentrale NRW eV davasında, bir web sitesi işletmecisinin, Facebook "Beğen" eklentisi aracılığıyla kullanıcı verilerinin toplanmasına katkıda bulunması durumunda, bu işletmecinin veri sorumlusu olarak kabul edilebileceğine hükmetmiştir. ABAD, veri sorumlusu olmanın, yalnızca verilerin doğrudan kontrolüne sahip olmayı gerektirmediğini; verilerin işlenme amaç ve vasıtalarının belirlenmesine katkıda bulunmanın da yeterli olduğunu belirtmiştir.[46] Bu karar, veri sorumluluğu kavramının geniş yorumlanması gerektiğini ve birden fazla kişinin aynı veri işleme faaliyetinde sorumluluk taşıyabileceğini ortaya koymuştur.

GDPR dibacesinde bulunan 47. paragraf uyarınca kişisel veri işlenme sebebi olarak hukuki dayanağa sahip bir amacın bulunması konusunda özenli bir gözden geçirme yapılmalıdır. Veri sahipleri verilerinin işlenmesini beklemediği durumlarda veri

[43]Soysal, T., **Unutulma Hakkının Avrupa Birliği'nin Genel Veri Koruma Tüzüğü Çerçevesinde İncelenmesi,** Uyuşmazlık Mahkemesi Dergisi, Sayı 13, 2019, s. 339-422. https://dergipark.org.tr/tr/pub/mdergi/issue/45986/581902 , Erişim Tarihi 07.12.23.
[44] GDPR Dibace 63.paragraf.
[45]Daha ayrıntılı bilgi için bakınız. Green, D., **Strategic Indeterminacy and Online Privacy Policies: (Un)informed Consent and the General Data Protection Regulation**, Int J Semiot Law 38, 2025, s.701–729. https://doi.org/10.1007/s11196-024-10132-4
[46] Case C-40/17 (Court of Justice), Fashion ID GmbH & Co. KG v Verbraucherzentrale NRW eV [2019], ECLI:EU:C:2019:629, 69. paragraf.

sahiplerinin menfaati ve hakları, veri sorumlusunun menfaati ve haklarına ağır basabilmektedir.[47] Veri sorumlusunun birçok yükümlülüğü ilgili mevzuatta bu şekilde düzenlenmiştir. Veri sorumlusunun yanlış kişisel bilgileri zamanında silmesi veya doğrusunu kaydetmesi gerekmektedir.[48] Bunun sebebi ise doğruluk ilkesine uyum sağlanmasıdır. Kişisel verilerin doğru tutulmasına ilişkin doğruluk ilkesine ileride ayrı olarak değinilecektir.

Veri sorumlusu veya veri kontrolörü veri ihlali bildirimi ile yakından bağlıdır çünkü veri sorumlusu, veri ihlallerinin bildirimlerinin yapılmasında asıl karakterlerden biridir. Veri sorumlusu, veri ihlali bildiriminin yapılıp yapılmayacağına karar vermektedir. Denetim makamını veya veri öznelerini (veri sahiplerini) de bildirim ile haberdar etmektedir. İleride ele alınacak olan hesap verebilirlik ilkesine uygun davranmak amacıyla, veri ihlali bildirimi yapılsa da yapılmasa da veri sorumlusunun bütün veri ihlallerinin kaydını tutmak zorunda olduğu görülmüştür.

1.2.3. Veri İşleyen Kavramı

Veri işleyen, toplanan kişisel veriyi veri sorumlusunun belirttiği şekilde işleyen bir kişi veya kuruluştur. Veri işleyen kavramı, GDPR'da düzenlenmiştir. 4. maddenin 8.fıkrası uyarınca veri işleyen, kişisel verileri veri sorumlusuna bağlı olarak işleme faaliyetini gerçekleştiren kişi veya kuruluştur.[49] GDPR ile bireyler veri işleyene karşı da hukuki işlemler başlatabilmektedir.[50] Veri işleyen, veri sorumlusunun adına karar verememektedir, onun kararlarını takip etmektedir.[51] Veri işleyen, veri sorumlusunun

[47]GDPR Dibace 47.paragraf.
[48]Daha ayrıntılı bilgi için bakınız. Yücedağ, N., **Kişisel verilerin korunması kanunu kapsamında genel ilkeler**, Kişisel Verileri Koruma Dergisi, Cilt 1, Sayı 1, 2019, s. 47-63. https://dergipark.org.tr/en/pub/kvkd/issue/45759/566993 , Erişim Tarihi 12.12.23.
[49] GDPR 4. madde 8. fıkra.
[50] Bakırel, N. B., **Veri Sorumlusu Ve Veri İşleyen Arasındaki Sorumluluk Paylaşımı Avrupa Birliği Genel Veri Koruma Tüzüğü Ve Kişisel Verilerin Korunması Kanunu Çerçevesinde Değerlendirilmesi**, Seçkin, 2021. s.92.
[51]Daha fazla bilgi için bakınız. Mehta, B., Sau, S., Patel, D., Rai, A., Das, B., Takidar, S. K., **Transparency through the lens of data protection and privacy: A clinical research organisation**

talep ettiği şekilde verileri işlemektedir. Veri işleyen verilerin nasıl işleneceğine kendi karar vermemektedir. Veri sorumlusu bir patron, veri işleyen ise patronun yardımcısı gibi düşünülebilmektedir. Veri işleyenin, işleme faaliyetinin amacını değiştirme yetkisi yoktur.

Veri işleyen kavramına ilişkin ABAD, Jehovan todistajat –uskonnollinen yhdyskunta davasında, bir dini topluluğun mensuplarının kapı kapı dolaşarak kişisel veri toplamasında, verilerin işlenmesinin amacı ve vasıtaları üzerinde topluluğun etkisi olması halinde veri işleyen ya da veri sorumlusu sayılabileceğini belirtmiştir. Mahkeme, veri işleyen sıfatının yalnızca teknik hizmet sunan kişi ya da kuruluşlarla sınırlı olmadığını, veri işleme sürecine katkı sağlayan aktörlerin de bu kapsamda değerlendirilebileceğini vurgulamıştır.[52] Bu karar, veri işleyen kavramının yalnızca dış hizmet sağlayıcılarla sınırlı olmadığını, bazen bir topluluğun veya grup üyelerinin de bu sıfata sahip olabileceğini ortaya koyması açısından önemlidir.

Ayrıca veri işleyen sıfatı alınan durumlara bir örnek gösterilebilir. Elektronik iletişim sektöründeki bir şirket abonelerin verilerine sahip olduğundan veri sorumlusu olmaktadır. Bu abonelerdeki başka bireylere ait kişisel veriler örneğin mesaj gönderdiği kişilerin telefon numaralarına da erişilmesi ve bu numaraları kullanarak iletişim sağlaması sebebiyle veri işleyen sıfatı da almaktadırlar.[53] Örneğin bir online satış mağazası, finansal işleri için bir finans şirketiyle anlaşmış ise o şirket, müşterilerin finansal kişisel verilerini işleyeceği için veri işleyen konumunda olmaktadır. Veri işleyenin her zaman veri sorumlusu veya veri kontrolörüyle iletişim halinde bulunması gerekmektedir.

---

medical writing perspective, Medical Writing, Cilt 33, Sayı 4, 2024, s. 64–67. https://doi.org/10.56012/vmom7031

[52] Case C-25/17 (Court of Justice), Jehovan todistajat –uskonnollinen yhdyskunta v Tietosuojavaltuutetun toimisto [2018], ECLI:EU:C:2018:551, 66. paragraf.

[53] Balaban, M.F., **Elektronik Haberleşme Sektöründe İşlenen Kişisel Verilerin Korunması**, Adalet, 2023. s.81.

Veri sorumlusu veya veri kontrolörü veri ihlali bildirimini kendisi yapamamaktadır ancak bir veri ihlali yaşandığını fark ederse hemen veri sorumlusuna bildirmelidir. Veri sorumlusu gereken veri ihlali bildirimini yapacaktır. Veri işleyenin, denetim makamına veya veri öznelerine direkt bildirim yapmak için yetkisi bulunmamaktadır.[54] Veri işleyen, veri ihlali bildiriminin oluşturulabilmesi için veri sorumlusunun ihtiyacı olan bilgileri sağlamaktadır.

1.2.4. Veri Öznesi (Veri Sahibi) Kavramı

Veri öznesi veya veri sahibi kavramı, kişisel verileri işlenen gerçek kişi anlamına gelmektedir. Bir kişisel veriden kim olduğuna ulaşılabilen kişi veri öznesidir. GDPR hükümlerinin koruduğu kişinin veri öznesi (veri sahibi) olduğu görülmektedir. GDPR, veri öznesini kimliği tespit edilmiş veya edilebilir gerçek şahıslar olarak tanımlanmıştır.[55] GDPR dibacesinin 63.paragrafı uyarınca veri öznesinin kişinin kendisiyle ilgili işlenen verileri hakkında bilgi edinmeye ve meşru amaçlarla işlendiğini bilmeye hakkı bulunmaktadır. Bu hak, sağlık alanında veri öznesi ile ilgili işlenen verileri de kapsamaktadır.[56] Yapılan veri işleme faaliyetlerinin kayıtları, veri öznelerinin kendi kişisel verilerine erişimi açısından önem teşkil etmektedir.[57] Veri öznesinin kendisiyle alakalı kişisel verilere ulaşmasının önemi bu şekilde ayrıca vurgulanmıştır.

Yine veri öznesi kavramıyla ilgili olarak GDPR dibacesinin 61.paragrafında veri işleme faaliyetine ilişkin bilgilerin, kişisel veriler veri öznesinden toplanırken veya başka bir yerden toplanıyorsa da makul zaman periyodu içinde veri öznesine haber verilmesi gerektiği vurgulanmıştır.[58] Kişisel verilerin işlenmesi bildiriminin makul süre içinde yapılmasına dikkat çekilmiştir. "Makul süre" kavramı ise kesin ve net bir kavram

[54] Bu yetki GDPR 33. ve 34. maddede düzenlendiği üzere veri sorumlusuna verilmiştir.
[55] GDPR 4. madde 1. fıkra.
[56] GDPR Dibace 63. paragraf.
[57] Daha ayrıntılı bilgi için bakınız. Bârsan, M.-M., **A Partial Overview of the Data Subjects' Control over Their Personal Data under the General Data Protection Regulation,** Bulletin of the Transilvania University of Brasov, Series VII: Social Sciences & Law, 11 (60)(2), 2018, s.129–134.
[58] GDPR Dibace 61.paragraf.

olmamakla beraber veri işleyenler ve veri sorumluları tarafından da kötü niyetle kullanılmamalıdır. Veri öznesinin elektronik ortamda rızasının talebi hakkında ise veri işlemesinin kaç tane amacı varsa rıza hepsine dair verilmesi gerekmektedir. Elektronik olarak iletilecek rızanın kısa ve net olması gerekmektedir ve hizmetin kullanımını zorlaştırmamalıdır.[59]

Veri öznesi kavramı ile ilgili olarak ABAD, Google Spain SL and Google Inc. v AEPD and Mario Costeja González davasında, arama motorlarında kişisel verilerin işlenmesi sürecinde bireylerin kimliklerinin belirlenebilir olması halinde, bu bireylerin kişisel veriler üzerinde belirli haklara sahip olduğunu vurgulamıştır. ABAD, bireyin bir internet sitesinde yer alan ve arama sonuçlarında çıkan bir bilgiyle açıkça tanımlanabilir olması hâlinde veri öznesi sıfatını taşıdığını kabul etmiştir.[60] Böylece bir veriden bir birey tanımlanabiliyor ise o bireyin veri öznesi olacağı belirtilmiştir.

Veri öznesini korumak amacıyla zorlayıcı bir meşru menfaat bulunması durumunda ne yapılacağı ise GDPR dibacesinin 69.paragrafında düzenlenmiştir. İlgili fıkra uyarınca "Bununla birlikte, kamu yararına gerçekleştirilen bir görevin yerine getirilmesi ya da veri sorumlusuna verilen resmi yetkinin kullanılması amacıyla veya bir veri sorumlusunun ya da üçüncü kişilerin meşru menfaatleri gerekçelerine dayanarak kişisel verilerin hukuka uygun olarak işlenebildiği durumlarda, veri öznesi, kendi özel durumuyla ilgili herhangi bir kişisel verinin işlenmesine itiraz etme hakkına sahip olmalıdır. Zorlayıcı meşru menfaatlerinin, veri öznesinin menfaatlerine veya temel hak ve özgürlüklerine ağır bastığının gösterilmesi sorumluluğu veri sorumlusuna aittir."[61] Bu noktada da sorumluluğu veri sorumlusu üzerine bırakmıştır.

[59] GDPR Dibace 32.paragraf.
[60] Case C-131/12 (Court of Justice), Google Spain SL and Google Inc. v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González [2014], ECLI:EU:C:2014:317, 81.paragraf.
[61] GDPR Dibace 69.paragraf.

Veri ihlali, veri öznesini etkilemektedir. Zarar görme tehlikesi bulunduğunda veri ihlali bildirimi, veri öznesine yapılmaktadır. Veri öznelerinin kişisel verilerinin ne zaman ihlale uğradığını bilmeye hakları vardır. Bu bilgi de veri ihlali bildiriminin içinde verilmektedir. Veri ihlali bildiriminin gayesi, veri öznelerinin veri güvenliğini ve gizliliğini sağlayabilmektir.

1.2.5. Alıcı ve Üçüncü Kişi Kavramları

Alıcı, kişisel veriyi alan anlamına gelen bir kavramdır. Alıcı kavramı, GDPR'ın 4. maddesinin 9. fıkrasında düzenlenmiştir. 4. maddenin 9. fıkrası uyarınca alıcı, kişisel verinin paylaşıldığı kişi veya kuruluştur. Kişisel verileri AB hukuku çerçevesinde alan kamu kuruluşları ise alıcı sayılmaz ancak veri işlemesi yine GDPR'a uygun yapılmaktadır.[62] Aynı şirket içinde farklı bir departman da alıcı sayılabilmektedir. Şirket dışında olması gerekmemektedir. Ancak alıcı, kendisi ile paylaşılan kişisel veriyi sadece paylaşılma nedeninin sınırları içinde kalarak kullanmaktadır. Alıcı tarafından veri hangi nedenle alındıysa o nedenle kullanmaktadır.

Veri ihlali bir alıcı yüzünden gerçekleşse bile veri sorumlusu yine bir veri ihlali bildiriminde bulunmak zorundadır. Bu ihlalde alıcı, veri sorumlusu ile ortak çalışmalıdır. Verilerin fazla alıcı ile paylaşılması veri ihlali ve veri ihlali bildirimi olasılığını artırmaktadır.

Bu kavrama ilişkin ABAD, RW v Österreichische Post AG davasında (C-154/21), veri öznesinin kişisel verilerinin kimlere aktarıldığını öğrenme hakkını ele almıştır. ABAD, veri sorumlusunun, veri öznesinin talebi üzerine, kişisel verilerin aktarıldığı belirli alıcıların kimliklerini açıklamakla yükümlü olduğunu belirtmiştir. Bu yükümlülük, yalnızca alıcıların kimliklerinin belirlenmesinin imkânsız olduğu veya talebin açıkça temelsiz ya da aşırı olduğu durumlarda, alıcı kategorilerinin

[62]GDPR 4. madde 9. fıkra.

bildirilmesiyle sınırlanabileceğini açıklamıştır.[63] Bu karar, alıcı kavramının, kişisel verilerin ifşa edildiği her türlü gerçek veya tüzel kişi, kamu otoritesi veya diğer birimleri kapsadığını ve bu alıcıların üçüncü taraf olup olmamasının önemli olmadığını vurgulamaktadır.

Üçüncü kişi kavramı ise yine aynı maddenin 10.fıkrasında düzenlenmiştir. 4. maddenin 10.fıkrası uyarınca üçüncü kişi, kişisel verileri toplayan ancak verileri asıl işleyenlerin dışında bir kişi veya kuruluştur.[64] Üçüncü kişi kamu organı veya makamı da olabilmektedir. Yani üçüncü kişi kavramı, sadece gerçek kişileri ifade etmemektedir ve tüzel kişilerle kamu makamını, kuruluşlarını veya organlarını da kapsamaktadır. Üçüncü kişi, kişisel veriye ancak hukuki bir sebep veya veri öznesinin izni bulunduğunda ulaşabilmektedir. Üçüncü kişi bir veri ihlaline sebep olduğu durumlarda veri ihlali bildirimi yapılmak zorundadır. Veri ihlali üçüncü kişi tarafından gerçekleşse bile veri sorumlusunun yükümlülüğü devam etmektedir çünkü üçüncü kişi, GDPR 4. madde 10.fıkra uyarınca veri sorumlusunun otoritesindedir.

1.2.6. Rıza Kavramı

Rıza, kişisel verinin işlenmesi için verilen bir izin olarak görülmektedir. Rıza kavramı, GDPR 4. maddesinin 11. fıkrasında düzenlenmiştir. 11. fıkra uyarınca veri öznenin rızası, açık bir onaylama ile kişisel verilerinin işleme faaliyetine maruz kalmasının kabul edilmesi anlamına gelmektedir.[65] Bu kavram, kişisel veri alanındaki önemli kavramlardan birisidir. Rıza açık olmalıdır ve isteyerek verilmelidir. Sessiz kalınması rıza verilmesi anlamına gelmemektedir.

[63] Case C-154/21 (Court of Justice), RW v Österreichische Post AG [2023], ECLI:EU:C:2023:3, 48. paragraf.
[64]GDPR 4. madde 10. fıkra.
[65]GDPR 4. madde 11. fıkra.

Rızanın verilme şekli ile ilgili olarak, GDPR dibacesinin 32. paragrafında "Rıza, veri öznesinin kendisiyle ilgili kişisel verilerin işlenmesine ilişkin serbestçe verilmiş, spesifik, aydınlatılmış ve şüpheye yer bırakmayacak bir şekilde mutabakatının belirtilmesini sağlayan açık ve olumlu bir eylemiyle, örneğin elektronik araçlarla yapılanlar da dâhil olmak üzere yazılı bir beyanla veya sözlü bir ifadeyle verilmelidir. Bu, bir internet sitesini ziyaret ederken bir kutunun işaretlenmesini, bilgi toplumu hizmetleri için teknik ayarların seçilmesini ya da veri öznesinin kişisel verilerinin önerilen biçimde işlenmesini kabul ettiğini bu bağlamda açıkça gösteren başka bir beyan veya davranışı içerebilir."[66] şeklinde düzenlenmiştir.

Uygulamaya bakıldığında da gerçek hayatta kullandığımız internet sitelerinin çoğunda kutu işaretlenmesi veya ayarlama yapılması seçeneği karşımıza çıkmaktadır. Bu yöntem günümüzde oldukça sık kullanılmaktadır. Ancak şunu da belirtmek gerekir ki verilen rıza, yapılacak bütün işleme faaliyetleri için geçerli olacak şekilde verilmelidir.[67] Kişisel veri işleme faaliyetine verilecek rıza açık ve net olmalıdır.[68] Bu durum hem GDPR hem de KVKK için geçerlidir.

Bilimsel araştırma amacıyla kişisel verilerin işlenmesi durumunda ise bilimsel araştırmada veri işlemenin temel amacı kesin belirli olmayabilmektedir. Bu yüzden veri özneleri, etik kurallarına riayet edilecek bilimsel araştırmalara rıza verebilmelidirler.[69] şeklinde bir açıklama yapılmıştır.

Rızanın özgürce verilmesi gerekmektedir. Bu sebeple GDPR dibacesinin 43.paragrafına göre rızanın özgürce alındığından emin olmak için devlet kurumları tarafından alınan rızalarda veri işleme faaliyetinin nedeni açıkça belirtilmelidir. Her farklı veri işleme faaliyetine ayrı rıza verilebildiği halde ve bir anlaşmanın ediminin

[66]GDPR Dibace 32. paragraf.
[67]GDPR Dibace 32. paragraf.
[68] Erdoğmuş, E., 6698 Sayılı Kişisel Verilerin Korunması Kanunu Kapsamında Açık Rıza, Seçkin, 2022. s. 72.
[69]GDPR Dibace 33.paragraf.

verilmesi gerek olmadığı halde rıza gösterilmesi koşuluna bağlanmışsa rıza hür irade ile verilmemiş sayılmaktadır.[70] Veri öznesi rıza göstermediğinde veya rızasını geri aldığında herhangi bir müeyyideye tabi tutulması, rızanın özgürce alınmadığının göstergesi olmaktadır.[71] Ayrıca özel kişisel verilerin, veri öznesinin rızası aranmadan toplum sağlığı ile ilgili durumlarda halkın faydası için işlenmesi gerekebileceği şeklinde bir düzenleme ile kamunun sağlığını ilgilendiren durumlarda rıza aranmamak gibi istisnai bir durum olduğu da belirtilmiştir.[72]

Rıza kavramı ile ilgili olarak ABAD, Bundesverband der Verbraucherzentralen und Verbraucherverbände — Verbraucherzentrale Bundesverband eV v Planet49 GmbH davasında (C-673/17), kişisel verilerin işlenmesine yönelik rızanın geçerliliği için belirli kriterleri vurgulamıştır. ABAD, önceden işaretlenmiş kutucuklar aracılığıyla elde edilen rızanın geçerli olmadığını ve rızanın açık, özgür iradeyle, belirli bir konuya ilişkin ve bilgilendirmeye dayalı olarak verilmesi gerektiğini belirtmiştir.[73] Bu karar, rızanın yalnızca aktif bir davranışla ve yeterli bilgilendirme sonrasında verilmesi gerektiğine dikkat çekmektedir.

Rıza kişisel verinin paylaşılmasına izin vermektir ancak bir veri ihlali yaşandığında veri öznelerinin bu ihlalden yine de haberleri olmalıdır. Bu haber ise veri ihlali bildirimi ile gerçekleşmektedir. Ayrıca güven kaybedildiğinde rıza geri alınabilmektedir.

1.2.7. Kişisel Veri İhlali Kavramı

Kişisel veri ihlali, kişisel verilerin görmemesi gereken kişiler tarafından görülmesi, değiştirilmesi, yanlışlıkla silinmesi anlamına gelmektedir. Kişisel veri ihlali

[70]GDPR Dibace Kısmı 43.paragraf.
[71] Selek, O., **Genel Veri Koruma Tüzüğü Işığında Kişisel Verilerin İşlenmesinde Rıza Açıklaması**, Dokuz Eylül Üniversitesi Hukuk Fakültesi Dergisi Cilt 21, Sayı 2, 2019, s. 911-951. https://dergipark.org.tr/tr/pub/deuhfd/issue/51788/646330 , Erişim Tarihi 07.12.23.
[72] GDPR Dibace 54.paragraf.
[73] Case C-673/17 (Court of Justice), Bundesverband der Verbraucherzentralen und Verbraucherverbände — Verbraucherzentrale Bundesverband eV v Planet49 GmbH [2019], ECLI:EU:C:2019:801, 63.paragraf.

kavramı, GDPR 4. maddesinin 12. fıkrasında düzenlenmiştir. 12.fıkra uyarınca "kişisel veri ihlali iletilen, depolanan veya başka bir şekilde işlenen kişisel verilerin kazara veya hukuk dışı yollarla yok edilmesi, kaybı, değiştirilmesi, izinsiz şekilde açıklanması veya bunlara erişime yol açan bir güvenlik ihlalidir."[74] Siber güvenlik alanında bir ihlal, dışarıdan yetkisiz bir kişinin erişimi ile gerçekleşmektedir.[75]

GDPR dibace kısmının 85.paragrafı uyarınca kişisel veri ihlali, doğru şekilde adımlar atılmadığında veri öznelerinin kimlik hırsızlığına maruz kalmalarına, ırkçılık ve ayrımcılığa uğramalarına, maddi kayıplar yaşamalarına veya manevi zarar görmelerine sebebiyet verebilmektedir. Bu nedenle yüksek tehlike bulunmadığı kanıtlanabilen durumlar haricinde ihlalin öğrenilmesinden itibaren en geç 72 saat içinde ilgili denetim makamına bildirim yapılmalıdır.[76] Kişisel veri ihlali kavramının önemine istinaden Türk hukukundaki tanımından kısaca bahsedilecektir. Kişisel veri ihlali bildirimi konusunda 6698 sayılı KVKK da benzer şekilde düzenlenmiştir. Veri sorumlusunun, verileri başkalarının ele geçirmesi üzerine bildirim sorumluluğu bulunmaktadır. Bu sorumluluğun ihlali veri güvenliğinin ihlali olacağından idari para cezası verilebilmektedir.[77] Ayrıca Kişisel Verileri Koruma Kurumu tarafından verilen veri ihlali bildirimleri ile ilgili bir kararda GDPR'dan farklı olarak ihlalin ne zaman gerçekleştiği unsuruna da dikkat edilmiştir.[78]

Kişisel veri kavramına ilişkin ABAD, VB v Natsionalna agentsia za prihodite davasında (C-340/21), kişisel veri ihlali durumunda veri sorumlusunun sorumluluğunu ve veri öznesinin zararlarının tazminini ele almıştır. ABAD, bir siber saldırı sonucu kişisel verilerin yetkisiz üçüncü kişilere ifşa edilmesinin, veri sorumlusunun uygun

[74] GDPR 4. madde 12. fıkra.
[75] Daha fazla bilgi için bakınız. Utzerath, J., Dennis, R., **Numbers and statistics: data and cyber breaches under the General Data Protection Regulation**, Int. Cybersecur. Law Rev. 2, 2021, s. 339-348. https://doi.org/10.1365/s43439-021-00041-8
[76] GDPR Dibace 85.paragraf.
[77] Dülger (2021a).
[78] Dülger (2021b).

teknik önlemleri almadığı durumlarda, veri sorumlusunun tazminat sorumluluğunu doğurabileceğini belirtmiştir.[79] Ayrıca, veri öznesinin kişisel verilerinin kötüye kullanılmasından duyduğu korkunun da zarar kapsamında değerlendirilebileceğini vurgulamıştır. Bu karar, kişisel veri ihlali kavramının yalnızca verilerin yetkisiz erişimiyle sınırlı olmadığını, aynı zamanda veri sorumlusunun uygun önlemleri almaması durumunda tazminat sorumluluğunun doğabileceğini göstermektedir.

Kişisel veri; görmemesi gereken bir kişi tarafından görülürse gizlilik ihlali, değiştirilmemesi gerekirken değiştirilirse bütünlük ihlaline uğramaktadır. Bütünlük ihlalinden kasıt ihtiyaç olduğunda istenilen kişisel veriye ulaşılamaması anlamına gelmektedir. Kişisel veri ihlali ile veri ihlali bildiriminin bağlantısına değinirsek, kişisel veri ihlali, veri ihlali bildirimine sebep olan olayın kendisi olarak görülmektedir. Veri ihlali bildirimi, ihlalle doğru şekilde başa çıkılmasında bir faktördür. Bu iki kavram birbirine yakından bağlı görülmektedir. Kişisel veri ihlali bildirimi, ileride ayrıca ele alınacaktır.

1.2.8. Denetim Makamı Kavramı

Denetim makamı, her AB ülkesinde GDPR kurallarının uygulandığından emin olunmasını sağlayan bir makamdır. Bir üye devletteki resmi veri koruma kuruluşu olarak görülebilmektedir. Denetim makamı kavramı, GDPR 4. maddesinin 21. fıkrasında düzenlenmiştir. 21.fıkra uyarınca her üye devletin kendi sahip olduğu hür bir kamu kuruluşudur.[80] AB yasa koyucusu, denetim makamını GDPR uygulamasının koruyucusu olarak görmektedir.[81] İlgili denetim makamı ise aynı maddenin 22.fıkrasında düzenlenmiştir. 22.fıkra uyarınca ilgili denetim makamı,

[79] Case C-340/21 (Court of Justice), VB v Natsionalna agentsia za prihodite [2023], ECLI:EU:C:2023:11, 45. paragraf.
[80]GDPR 4. madde 21. fıkra.
[81] Daha ayrıntılı bilgi için bakınız. Hajduk, P., **The Powers of the Supervisory Body in the Gdpr as a Basis for Shaping the Practices of Personal Data Processing**, Review of European & Comparative Law, 45(2), 2021, s.57–75. https://doi.org/10.31743/recl.10733

a) veri sorumlusu veya veri işleyen üye devlet sınırları içinde ise,

b) üye devletteki veri öznelerinin kişisel veri işleme faaliyetinden önemli ölçüde etkilenecekse veya böyle bir ihtimal varsa,

c) o makama şikayet edilirse ortaya çıkmaktadır.[82]

Her üye devletteki denetim makamı, GDPR'ın yeknesak uygulanmasını sağlamaktadır.[83]

Denetim makamına ilişkin ABAD, Commission v Germany davasında (C-518/07), denetim makamlarının bağımsızlığını ele almıştır. ABAD, veri koruma denetim makamlarının, görevlerini yerine getirirken tam bağımsızlık içinde hareket etmeleri gerektiğini ve herhangi bir dış etkiden bağımsız olmalarının zorunlu olduğunu belirtmiştir.[84] Bu karar, denetim makamlarının sadece teknik olarak değil, aynı zamanda işlevsel ve kurumsal olarak da bağımsız olmaları gerektiğini vurgular niteliktedir.

Denetim makamı veri ihlal bildiriminin yapıldığı makamdır. Veri ihlal bildirimi veri sorumlusu için resmi bir yükümlülüktür. Bu bildirim sonrası veri ihlali ile başa çıkmak ise denetim makamının görevi olmaktadır. Denetim makamı bildirimle ilgili daha fazla detaylı bilgi isteyebilmektedir ve ihlalle ilgili bir soruşturma başlatabilmektedir. Gerekli gördüğünde tavsiyede de bulunabilmektedir.

1.2.9. Düzeltme Hakkı Kavramı

Düzeltme hakkı, yanlış, eksik olan veya güncel olmayan kişisel verilerin düzeltilmesi olarak açıklanmaktadır. Düzeltme hakkı kavramı ise GDPR 16. maddesinde düzenlenmiştir. 16. madde uyarınca veri öznesi, veri sorumlusundan kendisiyle ilgili yanlış olan veya artık güncel olmayan bilgileri geç kalınmadan düzeltilmesini isteyebilmektedir. Eksik olan bilgilerini ise bu düzeltme hakkı

[82] GDPR 4. madde 22. fıkra.
[83] Günay, B., **Kişiliğin Korunması Kapsamında Kişisel Verilerin Hukuka Aykırı Kullanılması Nedeniyle Hukuki Sorumluluk**, Seçkin, 2023. s.73.
[84] Case C-518/07 (Court of Justice), Commission v Germany [2010], ECLI:EU:C:2010:125, 25.paragraf.

kapsamında doldurulmasını talep edebilmektedir.[85] Bireyin hakkında yanlış bilgilerin depolanmasına karşı işe yarayacak bir haktır. Yanlış veya eksik halde işleme faaliyetine sokulan kişisel veriler, beklenen doğrulukta ve faydalılıkta bir sonuç vermeyecektir. Bu nedenle doğru ve tam olmaları işleme faaliyetinin yararına olacaktır.

Düzeltme hakkına örnek vermek gerekirse, kişisel verilerinizi işleyen bir şirketin adınızı ve soyadınızı yanlış veya eksik yazması, adresinizin eski ev adresiniz olarak gözükmesi gibi durumların düzeltme hakkı kullanılarak üstesinden gelinebilmektedir.

Düzeltme hakkına ilişkin ABAD, Deldits davasında (C-247/23), veri öznesinin kişisel verilerinin doğru ve güncel olmasını sağlama hakkını ele almıştır. ABAD, bir mültecinin cinsiyet kimliğinin yanlış kaydedilmesi durumunda, ilgili ulusal otoritenin bu verileri düzeltme yükümlülüğü olduğunu belirtmiştir. Ayrıca, mahkeme, veri öznesinin bu hakkını kullanabilmesi için cinsiyet değiştirme ameliyatı geçirdiğine dair kanıt sunmasının istenemeyeceğini vurgulamıştır.[86] Bu karar, düzeltme hakkının, veri öznesinin kişisel verilerinin doğruluğunu sağlama hakkını güvence altına aldığını göstermektedir. Bu karar, veri öznesinin kişisel verisi üzerinde hak sahibi olduğunu da kanıtlar niteliktedir.

Veri ihlal bildirimi ile düzeltme hakkının bağlantısı şu noktada ortaya çıkmaktadır: Olası bir veri ihlalinde; veri sorumlusu, veri öznesinin doğru iletişim bilgilerine sahip olmalıdır ki veri ihlali bildirimi ilgili veri öznesine ulaşabilsin. Ayrıca düzeltme hakkı, bir veri ihlali sonrası veri öznesinin bilgilerinin değiştirilmesi veya silinmesi nedeniyle de kullanılabilmektedir.

[85] GDPR 16. madde.
[86] Case C-247/23 (Court of Justice), Deldits v Országos Idegenrendészeti Főigazgatóság [2025], ECLI:EU:C:2024:747, 41. paragraf.

1.2.10. Unutulma Hakkı Kavramı

Unutulma hakkı temel olarak, veri öznesinin kişisel verisinin işlendiği kuruluşa verilerinin silinmesini talep edebilmesi olarak karşımıza çıkmaktadır. Unutulma hakkı kavramı, "kalıcı olarak silme hakkı" olarak da geçmektedir. Silme veya unutulma hakkı olarak da geçmektedir.[87] GDPR, kişisel verilerin korunmasını uygulamada sağlayabilmek için unutulma hakkının etkin şekilde kullanılmasını sağlamalıdır.[88] Unutulma yani kalıcı olarak silme hakkı, GDPR 17. maddesinde düzenlenmiştir. 17. maddenin 1. fıkrası uyarınca veri öznesi kişisel verilerinin silinmesini veri sorumlusundan talep edebilmektedir. Veri sorumlusu, şu hallerden birinde geç olmadan veriyi silmekle yükümlüdür:

a) veriler artık veri işleme amacıyla uyuşmuyorsa ve lüzum kalmamış ise,
b) rıza geri alınmış ise ve hukuken bir sebep de yoksa,
c) veri öznesi verinin işlenmesine itiraz etmişse veya verinin işlenmesi için meşru bir temel yok ise,
d) hukuka aykırı işleme faaliyeti yapılıyorsa,
e) kanundaki yasal bir sorumluluk sebebiyle kalıcı silinmesi zorunlu ise,
f) bilgi toplumu hizmeti için veriler toplanmış ise.[89]

Bu noktada veri sorumlusuna önemli görevler düşmektedir. Aynı maddenin 2. fıkrasında buna da ayrıca değinilmiştir. 2. fıkra uyarınca veri sorumlusu verileri kamuya duyurmuş ve kalıcı olarak silmek zorunda kaldığı durumlarda, maddi yönüne de dikkat ederek, silinmesi istenen verileri işleyen veri sorumlularını da kalıcı silinme talebi hakkında bilgilendirmektedir ve lazım olan önemleri almaktadır.[90]

---

[87] Çağlayan R., Koca, M., Saka, R., **Avrupa Birliği Hukuku, İdare Hukuku Ve Ceza Hukuku Açısından Kişisel Verilerin İmhası**,2022, s.207.
[88]Daha ayrıntılı bilgi için bakınız. Uncular, S**., The right to removal in the time of post-google Spain: myth or reality under general data protection regulation?**, International Review of Law, Computers & Technology, 33(3), 2019, s. 309–329. https://doi.org/10.1080/13600869.2018.1533752
[89]GDPR 17. madde 1. fıkra.
[90]GDPR 17. madde 2. fıkra.

Bu doğrultuda, unutulma hakkını, kısaca, kural olarak ilgili kişinin talebi üzerine kişisel verilerinin kalıcı olarak imha edilmesi şeklinde ifade etmek mümkündür. Ancak korunması gereken üstün bir menfaatin varlığı halinde, menfaat dengesi unutulma hakkı aleyhine bozulabilir.[91] Dolayısıyla bu noktada şu ayrıntıya değinmekte fayda vardır; mevzuatta da devamında yazıldığı üzere bazı durumlarda 1. ve 2. fıkralar uygulanmamaktadır yani unutulma hakkı (kalıcı olarak silme hakkı) kullanılamamaktadır. Bu durumlar ise şu şekilde açıklanmıştır: Veri işlemesi şu amaçlar için yapılıyorsa 1. ve 2. fıkralar uygulanmamaktadır:

a) ifade özgürlüğü ve bilgi edinme hakkının kullanılması durumunda,
b) kanuni bir sorumluluk veya kamunun faydası için resmi bir yetki söz konusu ise,
c) kamunun sağlık alanındaki menfaati için ise,
d) arşivleme, bilimsel veya tarihi gaye ile halk için hareket ediliyorsa,
e) bir hakkın gerçekleştirilmesi için ise.[92]

Unutulma yani kalıcı olarak silme hakkı ile ilgili bir görüşe göre ise kişisel verilerin internette tam olarak kimin sahipliği altında olduğunu bilebilmek zordur. Bu sebeple veriler bulunduğu asıl kaynaktan silinse bile tam olarak unutulmuş sayılamayabilir.[93]

Unutulma hakkı, Google Spain SL and Google Inc. v AEPD and Mario Costeja González davasında (C-131/12), veri öznesinin, arama motoru sonuçlarından kendi adıyla ilişkilendirilmiş bağlantıların kaldırılmasını talep edebileceği kabul edilerek, ABAD tarafından ilk kez tanınmıştır. ABAD, bireylerin kişisel verilerinin, zamanla güncelliğini ve kamusal ilgisini yitirmiş olması halinde, bu bilgilere erişimin

[91] Tepe, E., Kişisel Verilerin Korunması, Adalet, 2021. s.107.
[92] GDPR 17. madde 3. fıkra.
[93] Çelikel, S., **Kişisel Verilerin Korunması Hukuku Kapsamında Veri Sorumlusu Ve Veri Sorumlusunun Yükümlülükleri**, Seçkin, 2022. s.167.

sınırlandırılmasını talep edebileceğini belirtmiştir.[94] Bu karar, unutulma hakkını yalnızca içerik sağlayıcıya karşı değil, doğrudan arama motorunu işletenlere karşı da ileri sürebilme imkanını tanımıştır.

Unutulma hakkına başvurulabilecek bazı durumlar; şirketin o veriye artık ihtiyaç duymaması, verinin hukuka aykırı elde edilmiş olması, veri için verilmiş rızanın geri alınması gibi durumlardır. Bir veri ihlalinin ardından yapılan bir veri ihlal bildirimi ile veri özneleri ilgili kuruluşun verileri gerekmediği veya açıkça rıza alınmadığı halde sahip olduğunu fark edebilirler. Bu durumda veri özneleri unutulma haklarını kullanmak isteyeceklerdir. Bu durum veri ihlal bildirimi ile unutulma hakkının el ele çalıştığını göstermektedir. İki kavram bir aradayken veri öznelerinin veri güvenliğinin sağlanmasına yardımcı olmaktadırlar.

1.2.11. İşlemeyi Kısıtlama Hakkı Kavramı

İşlemeyi kısıtlama hakkı, veri öznesinin kişisel verilerinin sadece depolanmasını talep etmesi ve kullanıp değiştirilmesine izin vermemesi hakkıdır. İşlemeyi kısıtlama hakkı kavramı, kişisel verilerin işlenmesi aşamasında kullanılabilen bir hak olarak karşımıza çıkmaktadır. GDPR 18. maddesinde düzenlenmiştir. 18. maddenin 1. fıkrası uyarınca veri öznesi şu hallerde veri işlemesinin kısıtlanmasını talep edebilmektedir:

a) veri öznesi verilerin yanlış olduğunu öne sürerse,
b) kanuna aykırı işleme yapılması ve veri öznesinin verilerinin silinmesini kabul etmeyip sadece işlemenin kısıtlanmasını isterse,
c) veri sorumlusunun ilgili verilere artık ihtiyacının kalmamasına rağmen veri öznesi bir hakkın savunulması, gerçekleştirilmesi için ilgili verilere ihtiyacı olursa,

[94] Case C-131/12 (Court of Justice), Google Spain SL and Google Inc. v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González [2014], ECLI:EU:C:2014:317, 94.paragraf.

d) veri sorumlusunun hukuka uygun işleme sebeplerinin, veri öznesinin sebeplerine ağır gelip gelmediği belirlenene kadar işlemeye itiraz ederse.[95]

İşlemeyi kısıtlama hakkı kullanıldığında kişisel verileri işleyen kuruluş veri işlemeyi durdurup sadece güvenli biçimde depolamalıdır. Aksi yönde bir hareket yapılırsa bunu veri öznesine bildirmelidir. Örneğin bir bankada kart bilgilerinin yanlış kayıtlı olduğunu fark eden veri öznesi, veri işlemesinin kısıtlanmasını isteyebilmektedir. Veriler düzeltilene kadar işleme kısıtlı kalmaktadır ve kullanılamamaktadır.

İşlemeyi kısıtlama hakkı, FT v DW davasında (C-307/22) ABAD tarafından ele alınmıştır. ABAD, veri öznesinin, kişisel verilerinin doğruluğunu tartıştığı veya işlenmesinin hukuka aykırı olduğunu düşündüğü durumlarda, veri sorumlusundan bu verilerin işlenmesini kısıtlamasını talep edebileceğini belirtmiştir.[96] Bu kısıtlama, verilerin yalnızca saklanmasıyla sınırlı olup, başka herhangi bir işlem yapılmasını engeller niteliktedir. ABAD ayrıca, veri öznesinin, kişisel verilerinin işlenmesini kısıtlama hakkını kullanarak, verilerin silinmesini istemeden, belirli bir süre boyunca işlenmesini durdurabileceğini de açıklamıştır.

Bir veri ihlali yaşadıktan sonra veri ihlali bildirimi ile veri öznesine durum bildirildikten sonra, veri öznesi ihlalin etkileri çözülene kadar veri işlemesinin kısıtlanmasını isteyebilmektedir. İşlemeyi kısıtlama hakkı, veri öznesini ihlal sonrası gelecekteki zararlardan korumaya yardımcı olmaktadır.

1.3. Avrupa Veri Koruma Kurulu

Bu alt başlıkta Avrupa Veri Koruma Kurulu'na dair bilinmesi gereken noktalara değinilip veri ihlali bildirimi ile olan bağlantısından bahsedilecektir. Avrupa Veri Koruma Kurulu, kişisel verilerin korunması ve GDPR alanında kurallara ve hukuka dair bir açıklık getiren bir kuruldur. Kurul, GDPR hükümlerinin yorumlanmasında ve

[95]GDPR 18. madde 1. fıkra.
[96]Case C-307/22 (Court of Justice), FT v DW [2023], ECLI:EU:C:2023:11, 45. paragraf.

GDPR'ın sınır aşırı yetkisin açıklanmasında rehberlik etmektedir. Avrupa Veri Koruma Kurulu, GDPR ile kurulmuş olup tüzel kişiliğe sahiptir ve bir AB organıdır.[97] Kurulun orijinal adı *"European Data Protection Board"* olup "EDPB" şeklinde kısaltılmaktadır.

EDPB, GDPR'ın uygulanması için AB üye devletlerdeki veri koruma komisyonlarıyla birlikte çalışarak işbirliği ve tutarlılığı sağlamaktadır.[98] Yani kurul, GDPR'ın uygulanmasında yaşanabilecek durumlar da dahil olmak üzere kurumlar arası iş birliğine de katkıda bulunmaktadır. Örneğin veri ihlali bildirimi hakkında ve GDPR ile nasıl uyumluluk sağlanabileceğini gösteren bir yönerge yayınlanması Kurul'un yol gösterici özelliği ile ilgilidir.[99] GDPR'ın daha iyi anlaşılmasına yardımcı olmaktadır.

"Kurul her üye devletin bir denetim makamı başkanı ile Avrupa Veri Koruma Denetçisi veya bunların kendi temsilcilerinden oluşur."[100] Kurulda AB'deki üye devletler arasında ayrım yapılmamıştır. Her üye devletin sesinin temsil edilmesi sağlanmıştır.

EDPB bünyesinde bir Avrupa Veri Koruma Denetçisi bulunmaktadır. Avrupa Veri Koruma Denetçisi (EDPS), AB'nin bağımsız veri koruma otoritesidir.[101] Avrupa Veri Koruma Denetçisi'nin orijinal ismi *"European Data Protection Supervisor"*dır. "EDPS" şeklinde kısaltılmaktadır. EDPS, EDPB'nin bir üyesidir ve genelde tavsiye vermektedir. EDPS, şu anda bir denetçi tarafından yönetilen ve deneyimli avukatlar, BT uzmanları ve yöneticilerden oluşan bir ofis tarafından desteklenen, giderek etkili olan bağımsız bir denetim otoritesidir.[102] Avrupa Veri Koruma Denetçisi'nin genel amaçları; AB tarafından bireylerin verileri işlenirken ihlal yaşanmaması, veri koruma ile ilgili

[97] GDPR 68. madde 1. fıkra.
[98] Avrupa Veri Koruma Kurulu https://www.edpb.europa.eu/our-work-tools/support-cooperation-and-enforcement/gdpr-cooperation-and-enforcement_en Erişim Tarihi 23.04.2024.
[99] European Data Protection Board. (2021). Guidelines 01/2021 on examples regarding data breach notification – Version 2.0. https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-012021-examples-regarding-data-breach_e
[100] GDPR 68. madde 3. fıkra.
[101] Avrupa Veri Koruma Denetçisi https://edps.europa.eu/about-edps_en Erişim Tarihi 27.11.2023.
[102] Avrupa Veri Koruma Denetçisi https://edps.europa.eu/about-edps_en Erişim Tarihi 27.11.2023.

durumlarda AB organlarına gerekli önerilerde bulunmak, yeni çıkan ve veri koruma alanında etki yaratabilecek olan teknolojik gelişmeleri de takip etmek şeklindedir.[103]

Anlaşılacağı üzere, kurulun bir nevi danışma fonksiyonu bulunmaktadır. EDPB'nin tavsiyelerine AB üye devletleri, AB kurumları, ulusal veri koruma komisyonları danışmaktadır. Örneğin EDPB, verilere açıkça ulaşımın gerekliği olmadığı (örneğin depolama gibi) durumlarda verileri şifreleme yapılarak kaydedilmesini önermektedir.[104] Bu, EDPB'nin bulunduğu önerilere bir örnektir. Avrupa Veri Koruma Kurulu'nun Avrupa Ekonomik Alanı dışındaki üçüncü ülkelerin denetim makamları Avrupa Veri Koruma Kurulu üyeleri arasındaki iletişimi kolaylaştıracağı da düşünülmektedir.[105] Avrupa Veri Koruma Kurulu, AB dışındaki ülkelerin denetim makamları ile karşılıklı yardımlaşmayı ve doğrudan iletişim kurmayı teşvik eder durumda olduğu görülmektedir. AB'yi ve başka bir üçüncü ülkeyi ilgilendiren önemli bir veri ihlali yaşandığında bu iletişim kanallarının değeri daha net anlaşılacaktır. Bu sebeple EDPB, çoğu yönden veri koruma açısından yararlı işlevlere sahip bir kurum olarak görülmektedir.

Avrupa Veri Koruma Kurulu, 25 Mayıs 2018'de GDPR'ın yürürlüğe girmesiyle, 1995 tarihli 95/46 sayılı direktifin 29. maddesi ile kurulan Çalışma Grubu'nun yerini almıştır.[106] Yeni gelen GDPR ile bu eski kurum ve kuruluşlar da yenilenmiş ve yerlerine daha etkin, GDPR'ın işleyişi ile uyumlu bir kurul gelmiştir. Avrupa Veri Koruma Kurulu basit çoğunlukla büyük kararlar hakkında görüş verebilir ve

[103] Daha ayrıntılı bilgi için bakınız. Avrupa Veri Koruma Denetçisi https://www.edps.europa.eu/about-edps_en Erişim Tarihi 23.04.2024.
[104] Daha ayrıntılı bilgi için bakınız. Neuman, K. L., Kavanagh, P., Balbirnie, D., White, M., **Schrems II: European Data Protection Board Data Transfers Guidance**, Intellectual Property & Technology Law Journal, 33(3), 2021, s. 18–22.
[105] Daha ayrıntılı bilgi için bakınız. Kuner, C., Bygrave, L., Docksey, C., Drechsler, L**., The EU general data protection regulation: a commentary**, 2020, Update of Selected Articles (May 4, 2021), s.238.
[106] Avrupa Veri Koruma Kurulu https://www.edpb.europa.eu/about-edpb/who-we-are/legacy-art-29-working-party_en Erişim Tarihi 22.04.2024.

bilgilendirebilmektedir.[107] Bunlara ek olarak; Avrupa Veri Koruma Kurulu'nun kararlarına karşı Avrupa Birliği Adalet Divanı'na (ABAD) gidilebilmektedir.[108] Avrupa Veri Koruma Kurulu, GDPR'ın uygulanmasında mühim bir sorumluluğa sahip görülmektedir ve Kurul bu konuda yol gösterecek açıklayıcı yayınlarda bulunabilmektedir.[109] Bu duruma örnek vermek gerekirse, COVID-19 döneminde hastaların rızası alınmadan biyometrik ve sağlık kişisel verileri işlenebilecek olsa bile bunun yine kanunlara uygun ve adil şekilde yapılması gerektiğini ilgili sağlık kuruluşlarına, işverenlere hatırlatmıştır.[110] Avrupa Veri Koruma Kurulu'nun, kendi kurumsal yerleşimi açısından kişisel verilerin korunması alanında merkezi bir noktada bulunduğu görülmektedir.

Veri ihlali bildirimi ile EDPB bağlantısı, GDPR'a uyum, mutabakatın sağlanması ve GDPR'ın uygulama alanında kendini göstermektedir. Örneğin kurul, veri ihlali bildiriminin daha açıkça anlaşılabilmesi için ne zaman yapılması gerektiğine dair yönerge yayınlamıştır.[111] Veri ihlali bildirimi kurallarının AB'deki tüm veri koruma ve denetim makamları tarafından uygulandığından emin olunmaktadır. Yaşanan bir veri ihlalinde farklı veri koruma kurulları nasıl ilerlenmesi gerektiği konusunda bir anlaşmaya varamadıklarında EDPB hepsini bağlayıcı bir karar verebilmektedir ve bu karara uygun hareket edilmesiyle sorun ortadan kalkmaktadır.

EDPB, veri ihlali durumunda riskin önemini vurgulayarak veri ihlali bildiriminin yapılmasını teşvik eder bir konumda bulunmaktadır. EDPB, veri ihlali bildiriminin

[107]Daha ayrıntılı bilgi için bakınız. Bendiek, A., Römer, M., **Externalizing Europe: the global effects of European data protection. Digital Policy, Regulation and Governance,** 21(1), 2019, s. 38.
[108] Giakoumopoulos, C., Buttarelli G., O'Flaherty, M., **Handbook on European Data Protection Law**,Publications Office of the European Union, Luxembourg, 2018, s.201.
[109] Daha ayrıntılı bilgi için bakınız. Mustert, L., Santos, C., **The European Data Protection Board-a (non) consensual and (un) accountable role?**, 2024, s.33.
[110] Daha ayrıntılı bilgi için bakınız. Guida, S., **The European Data Protection Board's Position on the Processing of Personal Data In The Context Of Covid-19**, European Data Protection Law Review (EDPL), 6(2), 2020, s. 262-264.
[111] European Data Protection Board, Guidelines 9/2022 on Personal Data Breach Notification under GDPR – Version 2.0, 28 March 2023, https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-092022-personal-data-breach-notification-under_en

layığıyla yerine getirilmesini bir sorumlu davranma eylemi olarak görmektedir. Bu noktadan, EDPB'nin veri ihlali bildiriminin doğru ve gereğine uygun şekilde yapılmasında pozitif yönde etkisi olan bir kurul olduğu anlaşılmaktadır.

Bir sonraki alt başlıkta ise GDPR uygulanma alanına ve veri ihlali bildiriminin GDPR uygulanma alanındaki yerine değinilecektir.

1.4. Genel Veri Koruma Tüzüğü'nün Uygulanma Alanı

Bu alt başlıkta GDPR'ın uygulanma alanı ve veri ihlal bildiriminin bu alanda nereye düştüğü ele alınacaktır. GDPR'ın uygulanma alanı, GDPR'ın pratikte uygulanabildiği alanı kastetmektedir. GDPR'ın uygulanma alanı, dijital çağda kendi kendini yeniden tanımlar hale gelmiştir. Veri işleme faaliyetinin nerede yapıldığından çok kime yapıldığı önem arz etmektedir. GDPR, AB dışından gelen etkilere karşı kapsamını kullanarak kişisel verileri korumaktadır ve bunu büyük bir coğrafi kapsamda GDPR'a uygun davranılmasını sağlayarak gerçekleştirmektedir.[112] Uygulama alanı, yerel bir egemenlikten çok veri özneleri yani veri sahipleri odaklı bir görünümdedir.

Uygulama alanı GDPR'da "Bölgesel Kapsam" başlığı adı altında 3. maddede düzenlenmiştir. 3. maddenin 1. fıkrası uyarınca işlenen kişisel verilerin veri sorumlusu ya da veri işleyeni AB içinde bir kurum ise GDPR'ın uygulanacağı belirtilmiştir.[113] Bu noktada veri işlemesinin AB içinde veya dışında olmasının fark etmediği belirtilmiştir. Yine aynı maddenin 2. ve 3. fıkraları uyarınca GDPR'ın şu hallerde AB içindeki veri sahiplerinin verilerinin AB içinde olmayan bir veri sorumlusu ya da veri işleyenin işlemesi durumunda uygulanacağı belirtilmiştir:

---

[112] Daha fazla bilgi için bakınız. Kuner, C., **Territorial Scope and Data Transfer Rules in the GDPR: Realising the EU's Ambition of Borderless Data Protection,** Legal Studies Research Paper Series University of Cambridge Faculty of Law, Paper No. 20/2021, April 2021, s.16. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3827850 Erişim Tarihi 19.08.2024.

[113] GDPR 3. madde 1. fıkra.

a) Veri öznesi bir mali ödemede bulunsun veya bulunmasın, AB içindeki veri sahiplerine mal ve hizmet temin edildiğinde ya da

b) Hareketleri AB içinde gerçekleştiğince bu hareketlerin izlenmesinde.

GDPR, AB dışında olup da ilgili AB üyesi ülkenin hukukunun milletlerarası hukuk olarak uygulandığı yerde de veri işlemesine uygulanmaktadır.[114] Bu fıkralarda GDPR'ın sınır ötesi yani sınır aşan yetkileri ortaya konulmaktadır. AB içindeki veri öznelerine mal veya hizmet sunuluyorsa, Birlik içinde kurulu olmayan bir veri sorumlusu da olsa GDPR'a bağlı olacağı belirtilmiştir. GDPR 3. maddenin 2. fıkrası ile hedef yer kabul edilip veri işlemeden etkilenen bireylere dikkat çekilmiştir.[115] Hareketler AB içinde gerçekleştiği sürece ve AB dışında veri işleme faaliyeti AB'deki kişileri izlemekle ilgili ise GDPR uygulanmaktadır.[116] İlgili madde, GDPR'ın uygulama alanını daha önce görülmemiş bir şekilde genişletmiştir. Bu sınır ötesi uygulama, internetin de sınırsız, sınırları aşan, sınır ötesi özelliği sebebiyle de gerçekleşmektedir.[117]

Nitekim internete dünyanın her yerinden bağlantı sağlanabilmesinin getirdiği kelebek etkisi sonuçlardan birisi de GDPR'ın uygulama alanının genişlemesi olmuştur. GDPR 3. maddenin 2. fıkrası, internetteki kullanıcı bireylerin faaliyetlerini izleyen operatörleri, online hizmet verenleri ve arama motorlarını kapsayacak şekilde dizayn edilmiştir.[118] GDPR 3.maddenin 1.fıkrası, 95 direktifinden farklı olarak hem veri sorumlusuna hem de veri işleyene sorumluluk tanımlamıştır. Ayrıca GDPR'da veri işlemenin AB sınırları içinde yapılması şart değil iken 95 direktifinde bu durum bir

[114]GDPR 3. madde 2. ve 3. fıkra.
[115]Dal, s. 21-33.
[116]Daha ayrıntılı bilgi için bakınız. Azzi, A., **The challenges faced by the extraterritorial scope of the general data protection regulation,** Journal of Intellectual Property, Information Technology and Electronic Commerce Law, 9(2), 2018, s. 126-137.
[117] Azzi, s. 126-137.
[118] De Hert P., Czerniawski M., **Expanding the European data protection scope beyond territory: Article 3 of the General Data Protection Regulation in its wider context**, International Data Privacy Law, Cilt 6, Sayı 3, 2016, s. 230–243.

şarttı.[119] Önceden belirtildiği üzere dikkat edilen nokta artık veri öznesinin kendisi olmuştur.

GDPR ile gelen bu yeni kural doğal olarak GDPR'ın uygulama alanını yani bölgesel kapsamını genişletmiştir. Bir AB vatandaşının kişisel verisi işlendiğinde GDPR alanına girmektedir. Ayrıca veri öznesinin AB içinde bulunması, mal veya hizmetin verildiği veya izleme davranışının yapıldığı anda gerçekleşmelidir.[120] Kısaca temelini özetlemek gerekirse GDPR şu iki durumda geçerlidir:

- veri işlemenin AB içindeki bir kuruluşun faaliyetleri kapsamında yapılması veya

- AB'de bulunan kişilerin verilerinin AB'de kurulu olmayan bir veri sorumlusu ya da işleyen tarafından işlenmesi.[121]

GDPR'ın alanına giren bir örnek olarak şunu verebiliriz: Avrupa'da uçuşlar yapan ve biletleri online (çevrim içi) de satan bir İtalyan havayolu şirketi B, bu uçuşlardaki yolcuların bilgilerini C isimli bulut bilgi depolama servisini kullanmaktadır. Bu durumda B veri kontrolörü ve C ise veri işleyen sıfatını almaktadır. Böylece, B ve C'nin ikisi de GDPR'ın kapsamına girecektir.[122] Yine buna benzer bir örnek ise; Avustralya kökenli online (çevrim içi) bir mağazanın internet sitesine AB'den girildiğinde o üye devlet uzantılı internet adresine dönüşmektedir. AB vatandaşları da bu mağazadan alışveriş yapabilmektedir ve mağaza Birlik vatandaşlarının kişisel verilerini depolamaktadır. Dolayısıyla buraya da GDPR uygulanacaktır.[123]

---

[119] Alsenoy, B.V., **Reconciling The (Extra)Territorial Reach Of The GDPR With Public International Law**, Gert Vermeulen- Eva Lieve (Ed.), Data Protection And Privacy Under Pressure Transatlantic Tensions, EU Surveillance, And Big Data, 2017, s. 77-100. https://kuleuven.limo.libis.be/discovery/fulldisplay?docid=lirias1711958&context=SearchWebhook&vid=32KUL_KUL:Lirias&search_scope=lirias_profile&adaptor=SearchWebhook&tab=LIRIAS&query=any,contains,LIRIAS1711958&offset=0&lang=en , Erişim Tarihi 20.03.24.

[120] Alsenoy, s. 77-100.

[121] Voigt, von dem Bussche, s. 22.

[122] Daha ayrıntılı bilgi için bakınız: Voigt, von dem Bussche, s. 25.

[123] Daha ayrıntılı bilgi için bakınız: Voigt, von dem Bussche, s. 27.

GDPR'ın uygulanma alanına dair belirtilmesi gereken bir husus da "anonimizasyon"dur. Anonimleştirmek yani isimsizleştirmek anlamına gelmektedir. Toplanan veri ile kişi arasında bir bağ kalmıyorsa anonim hale getirilmiş olmaktadır. Bu anonim bilgilerin kullanımında ise GDPR uygulanmamaktadır. GDPR'ın uygulanma alanına girmemektedir.[124] Anonimizasyon genelde istatiksel araştırmalar için kullanılmakla beraber eğer veri işleyen veya veri kontrolörü veri öznesinden bağı koparılmış ve anonim hale getirilmiş bu bilgileri geri yüklerse tekrar GDPR'ın alanına girmektedir.[125] Veri öznesi ile kişisel veri arasında yeniden bağ kurulunca anonimizasyonun etkisi kaldırılmış hale gelmektedir. Kişisel veri istatiksel amaçlı toplanmış olsa da veri öznesinin kim olduğu ortaya çıkınca yani kişinin kimliği ile bağlantısı kurulduğu anda GDPR kapsamında bir kişisel veriye dönüşmektedir.

GDPR'ın uygulanma alanına dair ABAD kararları bulunmaktadır. Örneğin ABAD, Wirtschaftsakademie Schleswig-Holstein kararında, bir Facebook sayfası yöneticisinin, sayfa ziyaretçilerinin verilerinin toplanması ve Facebook tarafından işlenmesinde ortak veri sorumlusu olarak kabul edilebileceğine hükmetmiştir. ABAD, söz konusu veri işlemesinin Almanya'daki kullanıcıları hedeflemesi nedeniyle GDPR'ın uygulama alanı içinde yer aldığını belirtmiştir.[126] Bu karar, GDPR'ın yalnızca AB içinde yerleşik kuruluşlara değil; AB'deki veri öznelerine hizmet sunan veya davranışlarını izleyen yabancı işletmelere de uygulanabileceğini göstermiştir.

Uygulanma alanına ilişkin diğer bir kararda ise ABAD, Facebook Belgium kararında, veri denetim makamlarının yetki alanını tartışmıştır. ABAD, bir üye devletin veri koruma otoritesinin, veri işleme faaliyetleri o ülkede yürütülmese bile, o ülke vatandaşlarının temel haklarının ihlal edilme ihtimali varsa yetki kullanabileceğine

[124] GDPR Dibace 26.paragraf.
[125] Daha ayrıntılı bilgi için bakınız: Voigt, von dem Bussche, s. 13-14.
[126] Case C-210/16 (Court of Justice), Wirtschaftsakademie Schleswig-Holstein GmbH v. ULD [2018], ECLI:EU:C:2018:388, 57. paragraf.

hükmetmiştir.[127] Bu karar, GDPR'ın coğrafi olarak uygulanma alanını yalnızca veri sorumlusunun yerleşik ülkesiyle sınırlı tutmadığını, AB'deki bireyleri hedef alan faaliyetlerin tümünde geçerli olduğunu açıkça ortaya koymaktadır. Böylece GDPR'daki kapsam ile ilgili kuralın somut olayda nasıl uygulandığı gösterilmiştir.

GDPR'ın uygulanma alanı ve veri ihlali bildirimi önemli bir noktada bağlanmaktadır. GDPR'ın uygulanma alanı temel olarak iki maddede özetlenmiştir. Birincisi AB'de kurulu bir kuruluş ise, ikincisi AB dışında olup AB'deki kişileri gözetliyor veya onlara satış yapıyor ise GDPR'ın uygulanma alanına girmektedir. GDPR'ın uygulanma alanına giren her veri işleme faaliyeti ise bir veri ihlaline uğradığında veri ihlali bildirimini usulüne göre yapmakla yükümlü hale gelmektedir. Veri ihlalinin nerede yaşandığından çok kimin verileri ihlale uğradığı önemlidir çünkü GDPR kapsamındaki veri sahiplerinin verileri ihlale uğradıysa GDPR veri ihlali bildirimi yapılmasının zorunlu olduğu görülmektedir.

AB sınırları dışındaki devletlerin GDPR'a uyum sağlamalarının nedeni AB iç pazarında bulunmak istemeleridir.[128] Üçüncü ülkelerin ekonomik kaygıları birçok nedenden daha etkili olmaktadır çünkü AB ticari anlamda çok büyük bir iç pazardır ve gelir sağlamak isteyen tacirler de bu iç pazarda bulunmak istemektedirler. Şirketler, markalar, yeni girişimciler, start-up projeler belli bir etki yaratabileceklerini bildikleri AB iç pazarında yer almaktadırlar. Bu sebeple GDPR'a uyum için daha fazla çaba gösterecekleri ve gelecekte de uyum sürecinin gelişimine katkı sağlayacakları öngörülmekte olan bir durumdur. Bir sonraki başlıkta ise GDPR'ın uygulanmasında kılavuz görevi gören ilkelerden bahsedilecektir.

---

[127] Case C-645/19 (Court of Justice), Facebook Ireland Ltd and Others v Gegevensbeschermingsautoriteit [2021], ECLI:EU:C:2021:483, 68. paragraf.

[128] Daha ayrıntılı bilgi için bakınız. Ryngaert C, Taylor M., **The GDPR as Global Data Protection Regulation?** American Journal of International Law Unbound, Cambridge University Press, Cilt 114, 2020, s.9. https://www.cambridge.org/core/journals/american-journal-of-international-law/article/gdpr-as-global-data-protection-regulation/CB416FF11457C21B02C0D1DA7BE8E688 Erişim Tarihi 27.08.2024.

2. GENEL VERİ KORUMA TÜZÜĞÜ'NDE KİŞİSEL VERİLERİN İŞLENMESİNE İLİŞKİN İLKELER

GDPR'daki veri ihlalinin anlaşılmasını sağlayacak kavramlardan, Avrupa Veri Koruma Kurulu'ndan ve GDPR uygulanma alanından sonra, bu başlıkta GDPR'ın temel yapı taşları olan ilkeler ele alınacaktır. GDPR'da kişisel verilerin işlenmesine ilişkin maddelere yer verilmiştir. GDPR'ın uygulanmasında belli prensipler çerçevesinde hareket edilmesi amaçlanmıştır. Veri ihlali bildirimi ve GDPR ilkeleri birbiriyle ilişkilidir. Ver ihlali bildirimi, bu ilkelerin uygulandığı ve bu uygulama sonucu somut varlığa kavuştuğu bir olgudur. Zira bildirim yapılırken bu ilkelere riayet edilerek yapılmaktadır. Bu ilkeler GDPR'ın 5. maddesinde yer almaktadır. İlkeler tek tek açıklanmıştır ve bu GDPR oluşturulurken aslında nasıl saiklerle harekete geçildiğinin anlaşılması açısından aydınlatıcı bir görev görmektedirler. İlkeler, GDPR'daki madde sıralamasına göre incelenecektir.

2.1. Hukuka Uygunluk, Adalet ve Şeffaflık

Hukuka uygunluk, adalet ve şeffaflık ilkesi GDPR'ın uygulanmasında geçerli üç temel değerdir. Bu üç temel değer ilkelerin belkemiğini oluşturmaktadır. Veri ihlali bildirimi alanında yapılan her bildirim hukuka uygun, adil ve özellikle şeffaf olmalıdır. Veri işlenirken de bu değerlere dikkat edilmektedir. GDPR 5. maddenin 1. fıkrasına göre "kişisel veriler, veri öznesi ile ilgili olarak hukuka uygun, adil ve şeffaf bir biçimde işlenir. (hukuka uygunluk, adalet ve şeffaflık)."[129] Hukuka uygunluk daha ayrıntılı olarak yine GDPR'ın 6. maddesinin 1. fıkrasında açıklanmıştır. Kişisel verilerin işlenmesi;

a) veri öznesi kişinin önceden gösterilen amaç doğrultusunda işleme yapılmasına izin vermesi,

[129] GDPR 5. madde 1. fıkra.

b) taraflarından biri olduğu bir sözleşmenin yapılması için veri öznesinin talep etmesi,
c) veri sorumlusunun hukuki sorumlulukları olması,
d) veri öznesinin veya bir başkasının hayati anlamda bir menfaati olması,
e) kamu yararı olan bir görev için ya da veri sorumlusunun yetkisini kullanabilmesi için elzem olmasında,
f) çocuk veri öznelerinin temel hak ve özgürlüklerinin veri işleme faaliyetinden daha önemli görüldüğü durumlar haricinde hukuka uygun işlemedir.[130]

Burada şu detayı belirtmek gerekir ki 6. maddenin 1. fıkrasının f bendi uyarınca, kamu görevi için veri işlemelerinde kullanılmamaktadır.

Hukuka uygunluk, adalet ve şeffaflık ilkesi ile ilgili olarak ABAD, Latvijas Republikas Saeima davasında (C-439/19), kişisel verilerin işlenmesinin, veri öznesinin temel hak ve özgürlüklerine saygı gösterilerek, açık, meşru ve belirli amaçlarla gerçekleştirilmesi gerektiğini belirtmiştir. Ayrıca, veri işleme faaliyetlerinin, veri öznesinin makul beklentilerini aşmaması ve şeffaf bir şekilde yürütülmesi gerektiğini ifade etmiştir.[131] Bu karar hukuka uygunluk, adalet ve şeffaflık ilkesinin hayati önemini göstermektedir.

Hukuka uygunluğun veri ihlali bildirimi ile bağlantısı, veri işleyen bir kurumun bir ihlal olduğunda bunu bildirmesinde ortaya çıkmaktadır. Veri ihlali bildirimi yapılması gereken bir durumda bildirim yapılmaz ise veri işlemesi o zamana kadar hukuka uygun ilerlemiş olsa da bildirim yapılmadığı için hukuka aykırılık meydana gelmektedir.

Adalet ilkesi ile veri ihlali bildirimin bağlantısı olarak, veri ihlali bildirimi yapılırken veri öznelerine adil yaklaşılmalıdır ve yanlış yönlendirmelerde

[130] GDPR 6. madde 1. fıkra.
[131] Case C-439/19 (Court of Justice), Latvijas Republikas Saeima [2021], ECLI:EU:C:2021:504, 96. paragraf.

bulunulmaması gerekmektedir. Bir veri ihlali olduğunda veri özneleri ona göre davranışlarda bulunabilmeleri için, ihlal saklanmamalı ve veri öznelerine bildirilmelidir. Adalet ilkesi, verilerin korunmasında hak ve sorumlulukların dengede durmasında yer edinmektedir.[132] Adil bir şekilde veri işlemesi yapılması için veri işleme gizli yapılmamalı ve veri öznesinin muhtemel riskler hakkında bilgisi olmalıdır.[133] Adalet ilkesine uygun olarak veriler işlenirken oluşabilecek tehlikeli durumlar hakkında veri öznesi haberdar edilmelidir. Şeffaflık ilkesi açısından ise veri sorumlusunun kim olduğu, veri işlemesinin amacı gibi unsurlar bildirilip veri öznesine açık ve sade bir şekilde açıklanmalıdır.[134]

Veri ihlali bildirimi açısından, veri öznelerinin (veri sahiplerinin) ihlallerde şeffaf bir şekilde bilgilendirilmeleri gerekmektedir. Kişisel verilerine neler olduğunu bilmek veri öznelerinin hakkıdır ve bu durum şeffaflık ilkesine uyum sağlamalıdır. Hukuka uygunluk açısından ise uygulamada veri işleme faaliyeti gerçekleşirken ilgili hükümlere uygun davranılmalıdır. Veri işleme faaliyeti bir işleyici tarafından yapılıyorsa şirketlerin veri işleme ile ilgili sözleşmelerinin GDPR gerekliliklerini taşıyıp taşımadığı kontrol edilmelidir.[135] Bu süreç uyumluluk sürecinin bir parçası olarak görülebilir. Uyumluluk süreci, veri işleyen veya kişisel verilerle ilgilenen ve onları kullanan kurumların, kuruluşların veya şirketlerin yaptıkları işlerin usulünü GDPR'a uygun hale getirmeleridir. Böylece hukuka uygunluk gerçekleşmiş olacaktır.

[132] Clifford, D., Ausloos, J., **Data protection and the role of fairness**, Yearbook of European Law, 37, 2018, s. 140.
[133] Daha ayrıntılı bilgi için bakınız. Giakoumopoulos, Buttarelli, O'Flaherty, s.118.
[134] Daha ayrıntılı bilgi için bakınız. Giakoumopoulos, Buttarelli, O'Flaherty, s.117.
[135] Tikkinen-Piri, C., Rohunen, A., Markkula, J., **EU General Data Protection Regulation: Changes and implications for personal data collecting companies. Computer Law & Security Review**, 34(1), 2018, s.146. https://www.sciencedirect.com/science/article/pii/S0267364917301966 Erişim Tarihi 17.03.2025.

2.2. Amacın Sınırlandırılması

Amacın sınırlandırılması ilkesi, veri işleme faaliyetine hukuki sınırlar çizilmesi amacıyla var olmuştur. GDPR 5. maddenin 1. fıkrasının b bendinde amacın sınırlandırılmasının anlamına değinilmiştir. Kişisel veri, önceden açıklanan meşru amaçlar kapsamında depolanıp işlenmektedir ve daha sonra amaca aykırı şekilde işleme yapılamaz. Kamu faydası için depolama, bilimsel, tarihi ya da istatiksel araştırma amaçlarıyla işleme önceden belirtilen amaçlara uygun olmadığı şeklinde ölçümlenemez.[136]

Amacın sınırlandırılması ilkesi, layığıyla uygulandığında veri işlemede amaç dışında çıkılmasını engelleyebilecektir.[137] Amacın sınırlandırılması ilkesine göre, kişisel veriler işlenirken en başta belirtilen hukuki dayanak kapsamında işlenmelidir. Eğer işlenme sırasında başka bir işlem yapılacaksa bu işlemin de ayrı bir hukuki dayanağı bulunmalıdır. Hangi amaç ile işlenecek denildiyse o amaç doğrultusunda veri işleme faaliyeti gerçekleştirilmelidir. Kendi hukuki dayanağı ve işleme amacı olmayan her işlem hukuka aykırı hale gelmektedir.[138]

Bu noktada şunu belirtmek gerekir ki GDPR'da belirtildiği üzere kamu yararı amacı ile işleme, bilimsel araştırma amacıyla işleme bu ilkenin istisnası konumundadır ve başlangıçtaki hukuki amaçtan bağımsız olabilmektedirler. Bunların dışında yapılan her kişisel veri işleme faaliyetinin ayrı bir hukuki temeli, sebebi bulunmalıdır ve açık olmalıdır. Kişisel veri işleme için başta rıza alınması sebebiyle tüm kişisel veri işleme faaliyetleri yapılmaya uygundur gibi bir düşünce içine girilmemelidir. Her farklı veri işleme faaliyetinin kendi içinde bir mesnete sahip olması gerekmektedir. Dolayısıyla

[136] GDPR 5. madde 1. fıkra.
[137] Daha ayrıntılı bilgi için bakınız. Hahn, I., **Purpose limitation in the time of data power: is there way forward?**, European Data Protection Law Review (EDPL), 7(1), 2021, s.31-44.
[138] Daha ayrıntılı bilgi için bakınız. Giakoumopoulos, Buttarelli, O'Flaherty, s.122-123.

belirtilen hukuki mesnet doğrultusunda gerçekleştirilen işleme faaliyeti GDPR'a uygun olarak işlenmiş kabul edilecektir.

Amacın sınırlandırılması ilkesi ile ilgili olarak ABAD, Single Resolution Board (SRB) v EDPS davasında (T-557/20), kişisel verilerin daha sonra farklı bir amaçla işlenmesinin, yalnızca orijinal amaçla açıkça uyumlu olması durumunda mümkün olduğunu belirtmiştir.[139] Bu dava, özellikle aynı verilerin idari bir amaçla toplanıp daha sonra denetim veya yargı sürecinde kullanılmak istenmesi durumunda amacın sınırlandırılması ilkesine nasıl riayet edilmesi gerektiğini göstermesi bakımından önem teşkil etmektedir.

Veri ihlali bildirimi ile amacın sınırlandırılması ilişkisi ise amacına uygun yapılmayan bir işlemenin veri ihlali olduğu noktasında ortaya çıkmaktadır. Amaç dışına çıkıldığında ise veri ihlali bildirimiyle bildirilmektedir çünkü veri ihlali yaşanmış olmaktadır. Veri ihlali bildirimi, amacın sınırlandırılması ilkesinin uygulanmasını sağlamaktadır.

2.3. Veri Minimizasyonu

Veri minimizasyonu toplanan kişisel veriler ile ilgili bir ilke olarak ortaya çıkmaktadır. GDPR 5. maddenin 1. fıkrasında veri minimizasyonu ilkesinde de yer vermiştir. Kişisel verilerin işlenmesi önceden belirlenen amaca uygun olarak bu amaç için toplanan verilerle ve amaçla sınırlı olacak şekilde yapılmalıdır.[140] GDPR, veri minimizasyonu ilkesine önem vermektedir ve ayrıca belirtmiştir.[141]

Amacın sınırlandırılması ilkesinde kişisel veri işleme işleminin hukuki dayanağa sahip olması aranırken veri minimizasyonu ilkesinde ise kişisel veri işleme işleminin

[139] Case T-557/20 (General Court), Single Resolution Board (SRB) v European Data Protection Supervisor (EDPS) [2023], ECLI:EU:T:2023:66, 72. paragraf.
[140] GDPR 5. madde 1. fıkra.
[141] Daha ayrıntılı bilgi için bakınız. Russo, A., Lax, G., Dromard, B., **A System to Access Online Services with Minimal Personal Information Disclosure**, Inf Syst Front 24, 2022, s. 1563–1575. https://doi.org/10.1007/s10796-021-10150-8

sadece amacı gerçekleştirecek veriler ile sınırlı kalınması gerektiği vurgulanmaktadır. Amacın sınırlandırması ilkesinde veri işlemesi yaparken başta belirtilen amaca sadık kalınması, veri minimizasyonu ilkesinde ise işleme için gerekli olan veri dışında veri toplanmaması gerektiği belirtilmektedir. Örneğin veri işlemesi için kişinin adı ve soyadı yeterli ise, yaşı veya adresiyle ilgili kişisel veriler toplanmamalıdır. Bu veri minimizasyonu ilkesine uygun davranmaya bir örnektir.

Veri işleme, işleme amacı başka yollarla yerine getirilemediğinde yapılmalıdır ve ilgili çıkarlara, haklara ölçüsüz müdahale edememelidir.[142] Veri işleme faaliyetinin orantılı şekilde gerçekleşmesi için de veri minimizasyonuna ihtiyaç vardır. Başta belirtilen veri işleme amacına riayet edilerek ve bu amacın sınırları içerisinde kalarak gerçekleştirilen veri işleme, gerekliliklere uygun olarak yapılmış şeklinde görülecektir.

Veri minimizasyonu ilkesine ilişkin ABAD, Deutsche Telekom AG v Federal Almanya Cumhuriyeti davasında (C-152/22), devletin genel ve yaygın biçimde kişisel veri toplamasının, veri minimizasyonu ilkesine aykırı olabileceğini belirtmiştir. Mahkeme, yalnızca belirli, sınırlı ve gerekli olan verilerin toplanabileceğini, veri işleme faaliyetlerinin kapsamının aşırı geniş olmasının temel haklara orantısız müdahale teşkil edeceğini açıklamıştır.[143] Bu karar, veri minimizasyonu ilkesinin uygulamada nasıl yorumlandığını göstermektedir.

Veri minimizasyonu ilkesinin veri ihlali bildirimi ile ilişkisi şu şekildedir: Ne kadar az veri toplanırsa, bir ihlal yaşandığında, veri ihlali bildirimi yapılmasına gerek olmayan durumlardan birine dönüşme ihtimali o kadar artmaktadır. Yine ne kadar az veri toplanırsa o kadar az veri risk altında olmaktadır. Böylece, zarar ihtimali de düşük

[142] Giakoumopoulos, Buttarelli, O'Flaherty, s.125.
[143] Case C-152/22 (Court of Justice), Deutsche Telekom AG v Bundesrepublik Deutschland [2024], ECLI:EU:C:2024:226, 61. paragraf.

tutulmaktadır. Gerekli olmayan veya artık kullanılmayan verilerin silinmesi de geçmiş verilerin risk altında olmasını engellemektedir.

2.4. Doğruluk

Doğruluk ilkesi, kişisel verilerin toplanması, depolanması veya işlenmesinde, verilerin doğru olduğundan emin olunması gerektiğini göstermektedir. GDPR 5. maddenin 1. fıkrası uyarınca kişisel veri doğru, güncel olmalıdır ve yanlış kişisel veriler silinmelidir.[144] Doğruluk ilkesinin tüm veri işlemelerde veri sorumlusu tarafından uygulanması gerekmektedir.[145] Ayrıca bu ilkeye göre, kişisel veriler güncel tutulmalıdır ve ihtiyaç olduğunda güncellenmelidir.

Kişisel verilerin doğru olarak kaydedilmesi makul bir prensip iken yanlış kaydedilen kişisel verilerin silinmesine de ayrıca vurgu yapılmıştır. Veri işleme faaliyetine yanlış haliyle giren bir veri, yanlış sonuçlara varılmasına yol açacaktır. Bu durum da o faaliyeti değersizleştirmektedir çünkü yanlış verilerin sonuçları anlamsız olacaktır. Zaman ve kaynakların boşuna harcanmaması için bu özelliğe dikkat edilmelidir. Yanlış kaydedilen kişisel verilerin silinmesi, doğru olan verilerin güncel olduğundan emin olunması ile yapılacak işlem, daha gerçekçi ve doğru sonuçlara ulaştıracaktır.

Doğruluk ilkesi ile ilgili olarak, FF v CRIF GmbH davasında (C-487/21), kişisel verilerin doğruluğu ve güncelliği ABAD tarafından ele alınmıştır. Mahkeme, veri öznesinin, kendisiyle ilgili işlenen kişisel verilerin bir kopyasını alma hakkının, verilerin doğruluğunu ve güncelliğini kontrol etme imkânı sağlamak amacıyla olduğunu belirtmiştir.[146] Bu kapsamda, veri sorumlusunun, veri öznesine, işlenen kişisel verilerin

[144] GDPR 5. madde 1. fıkra.
[145] Giakoumopoulos, Buttarelli, O'Flaherty, s.127.
[146] Case C-487/21 (Court of Justice), FF v CRIF GmbH [2023], ECLI:EU:C:2023:369, 45. paragraf.

açık ve anlaşılır bir kopyasını sağlaması gerektiğini ifade etmiştir. Bu karar ile kişisel verilerin doğru ve güncel tutulması için önlemler alınması gerektiği vurgulanmıştır.

Veri ihlali bildirimiyle doğruluk ilkesi bağlantısı, bir veri ihlali yaşandığında veri öznelerinin doğru iletişim bilgileri depolandıysa onlara ulaşılabilmesinde ortaya çıkmaktadır. Güncel ve doğru iletişim bilgilerine sahip olunması, veri öznelerine yapılacak veri ihlali bildirimin zamanında ve etkili şekilde yapılmasını sağlamaktadır. Aynı zamanda doğru toplanan veriler sayesinde, veri ihlali bildirimi yapılırken ihlale uğrayan veriler hakkında yanlış açıklama yapılmasının önüne geçilmektedir. Son olarak eğer veriler doğru değilse, bu veriler ihlale uğradığında veri sorumlusu kişi bu ihlali gerektiği şekilde yönetemeyecektir. Bu nedenle doğruluk ilkesi veri ihlali bildirimleri konusunda etkisini gösteren bir ilke olarak görülmektedir.

2.5. Depolamanın Sınırlandırılması

Depolamanın sınırlandırılması, depolanan kişisel verilerin depolama sürelerinin sınırlı olması ve bir hukuki dayanağa sahip olması gerektiğine dair bir ilke olarak karşımıza çıkmaktadır. GDPR 5. maddenin 1. fıkrasına göre kişisel veriler sadece veri işlemesi yapıldığı süre içinde veri öznelerinin kim olduklarının tanınmasını sağlayacak şekilde depolanabilir.[147] Bu ilkede vurgu yapılan nokta depolamanın yapılabileceği zaman periyodudur.

Ayrıca artık ihtiyaç duyulmayan verilerin de anonimleştirilerek yasal şekilde depolanabileceği belirtilmiştir.[148] GDPR'da bu ilke ile ilgili istisnai olarak depolanan kişisel verilerin kamu yararı, bilimsel, tarihi, istatiksel amaçlarla araştırma için kullanılacaksa daha uzun zaman saklanabileceği belirtilmiştir.[149] Depolama, veriye sahip kişilerin tanımlanabilmesini sağlamaktadır ancak veri işleme faaliyeti devam

[147] GDPR 5. madde 1. fıkra.
[148] Giakoumopoulos, Buttarelli, O'Flaherty, s.129.
[149] GDPR 5. madde 1. fıkra.

ettikçe yapılabileceği belirtilmiştir. Böylece veri öznelerine veya veri sahiplerine bir güven duygusu aşılanmıştır. Anonimleştirerek saklanmasında ise kişisel veri, veri öznesinden veya veri öznesinden kopup tek başına bir kişisel veri olarak kalmaktadır. Kişisel verinin üzerinden verinin öznesine veya öznesine ulaşılamayacak hale getirilip saklanması söz konusudur. Böylece veri öznesi anonim kişi olarak kalmaktadır ve anonimizasyon gerçekleşmiş olmaktadır.

Depolamanın sınırlandırılmasına ilişkin ABAD, Digi Távközlési és Szolgáltató Kft. v Nemzeti Adatvédelmi és Információszabadság Hatóság davasında (C-77/21), kişisel verilerin yalnızca belirli, açık ve meşru amaçlar için işlenmesi gerektiğini ve bu verilerin, işleme amaçları doğrultusunda gerekli olan süreyle sınırlı olarak saklanması gerektiğini belirtmiştir. Mahkeme, bir internet servis sağlayıcısının, abone verilerini test ve hata düzeltme amacıyla ayrı bir veri tabanında işlemesinin, orijinal veri toplama amacıyla yeterince bağlantılı olduğu ve bu nedenle amacın sınırlandırılması ilkesine aykırı olmadığı değerlendirilmiştir. Ancak, ABAD bu verilerin test ve hata düzeltme amacıyla işlenmesinin, yalnızca bu işlemlerin gerçekleştirilmesi için gerekli olan süreyle sınırlı olması gerektiğini açıklamıştır.[150] Karar, verilerin amaçlarla uyumlu olmayan şekilde daha sonra işlenmemesini gerektirdiğini de ortaya koymaktadır.

Veri ihlali bildirimiyle depolamanın sınırlandırması arasındaki bağlantı, veri öznelerinin kişisel verileri uzun zaman aralıklarıyla tutulmadığı için bu bilgileri hakkında veri öznelerine bildirim yapılma olasılığının azalması noktasında ortaya çıkmaktadır. Depolama süresi dolan bilgi silinerek ihlal sırasında ele geçirilme riski de ortadan kaldırılmaktadır. Depolamanın sınırlandırılması ilkesine riayet edilmesi, ihlal durumunda ilgili kurumun sorumlu davrandığının bir kanıtı olarak görülmektedir.

[150] Case C-77/21 (Court of Justice), Digi Távközlési és Szolgáltató Kft. v Nemzeti Adatvédelmi és Információszabadság Hatóság [2022], ECLI:EU:C:2022:817, 45. paragraf.

2.6. Bütünlük ve Gizlilik

Bütünlük ve gizlilik ilkesi, kişisel verileri yetkisiz erişimlerden ve değişikliklerden, verilerin kaybolmasından korumak anlamına gelmektedir. Bütünlük ve gizlilik ilkesi, GDPR 5. maddenin 1. fıkrasında kısaca açıklanmıştır. Bu maddeye göre kişisel veri bir bütünlük içinde işlenir ve bu işleme sırasında yetkisi olmayan veya yasaklı otoritelere, kazai kayıplara, hasara, imhaya, uygun olmayan veri işleme yöntemlerine karşı korunur.[151] Veri güvenliği ilkesi olarak da bilinmektedir. Kişisel veriler sadece onları işlemeye yetkili otoriteler tarafından işlenmelidir. Yetki olmadan işlendiğinde hukuka uygunluk ilkesi de ihlal edilmiş olmaktadır.

Veri güvenliğinde bilinmesi gereken bir yöntem de "maskeleme/takma ad verme"[152]dir. GDPR'ın 4. maddesindeki tanımlarda bu kavram "takma ad kullanımı" olarak geçmektedir. Kişisel veri sabit kalırken verinin sahibi hakkındaki bilgi (örneğin isim gibi) başka bir kelime, sayı ya da kısaltma ile maskelenmiş veya takma ad verilmiş olmaktadır. Veri öznesi bilgisi ne kadar belirsizleştirilirse o kadar tahmini zor hale gelir ve veri öznesinin kimliği de o kadar korunmuş olur. Örneğin "Ahmet Demir 1998 tarihinde iki çocuklu bir ailenin büyük çocuğu olarak dünyaya gelmiştir." verisi "A.D. 1998 tarihinde iki çocuklu bir ailenin büyük çocuğu olarak dünyaya gelmiştir." veya "XT44 1998 tarihinde iki çocuklu bir ailenin büyük çocuğu olarak dünyaya gelmiştir." şeklinde maskelenebilir.

Bu noktada ikinci örnek daha iyi bir seçimdir çünkü bir kişinin isim baş harflerinden tanınma olasılığı varken ikinci örnekte böyle bir tahmin dahi yapılamamaktadır.[153] Maskeleme yani ad takma ne kadar iyi yapılırsa veri öznesinin kişisel verileri o kadar güvende olmaktadır. Tahmin gibi bir yöntemle kişisel verinin öznesinin ya da sahibinin kim olduğu bilinememektedir. Tesadüfen denk gelip de doğru

[151] GDPR 5. madde 1. fıkra.
[152] Bu kavramın GDPR metnindeki orijinal tabiri "*pseudonymisation*" olarak geçmektedir.
[153] Daha ayrıntılı bilgi için bakınız. Giakoumopoulos, Buttarelli, O'Flaherty, s.132-132.

çıkma ihtimali de yok denecek kadar az olduğundan işlenen kişisel verilerin bütünlüğü ve gizliliği sağlanmış olmaktadır.

Bütünlük ve gizlilik ile ilgili olarak ABAD, Schrems II davasında (C-311/18), kişisel verilerin üçüncü ülkelere aktarımında yeterli düzeyde veri korumasının sağlanmasının önemini vurgulamıştır. Mahkeme, kişisel verilerin aktarımında, özellikle bütünlük ve gizlilik ilkelerinin gözetilmesi gerektiğini belirtmiştir. Bu kapsamda, verilerin yetkisiz erişim, ifşa, değişiklik veya yok edilme risklerine karşı korunması için uygun teknik önlemlerin alınmasının zorunlu olduğunu açıklamıştır.[154] Bu durum, bütünlüğün ve gizliliğin korunmasına da yardımcı olacaktır.

Bütünlük ve gizlilik ilkesine uygun davranılmaması örneğin yetkisiz kişilerin verilere erişim sağlaması, veri ihlali bildirimine ihtiyaç duyulmasına sebep olmaktadır zira veri ihlali gerçekleşmiş olmaktadır. Bütünlük ve gizlilik ilkesine uyulmadığından kaybedilen kişisel veriler de veri ihlali yaşanmasına neden olabilmektedir. Bu da veri ihlal bildirimi yapılmasına yol açabilmektedir. Kişisel veriler, usulsüz şekilde değiştirilip bütünlüğü bozulmamalıdır, bu durum da veri ihlali ve bildirimi gerektirecek hale gelebilmektedir. Veri ihlali bildiriminin, kökünde bütünlük ve gizlilik ilkesine uyum sağlanmaması sonucu ortaya çıktığı görülmektedir.

2.7. Hesap Verebilirlik

Hesap verebilirlik ilkesi kişisel verilerle ilgili yükümlülük taşıyan kişinin veri işleme faaliyeti hakkında gerektiğinde gerekli açıklamaları yapabilmesi ve kanıtlarını gösterebilmesi anlamına gelmektedir. Hesap verebilirlik ilkesi, GDPR 5. maddenin 2. fıkrasında "Veri sorumlusu, 1. paragrafa uygunluktan sorumludur ve bunu gösterebilmelidir."[155] şeklinde düzenlenmiştir. Burada hesap verebilirlik ilkesi diğer

[154] Case C-311/18 (Court of Justice), Data Protection Commissioner v Facebook Ireland Ltd and Maximillian Schrems [2020], ECLI:EU:C:2020:559, 133. paragraf.
[155] GDPR 5. madde 2. fıkra.

tüm ilkelere uygun davranılmasının sağlanması amacıyla diğer tüm ilkeleri kapsayıcı bir yaklaşımda bulunmaktadır. Büyük ölçekte veri işleme faaliyetlerinde hesap verilebilirlik ilkesine uyum sağlanmayabilmektedir.[156] Bu sebeple büyük veri işleme faaliyetlerinde sorumlu kişilerin hesap verilebilirlik noktasına ekstra özen göstermeleri gerekmektedir.

Veri sorumluları, veri işlemenin GDPR'a uygun gerçekleştirilmesinden sorumludur ve bu uygunluğu gerektiğinde ispatlayabilmelidir.[157] Bu noktada GDPR, veri sorumlularına ve veri işleyenlere ayrı bir sorumluluk daha getirmektedir ve bunun önemini vurgulamak için ayrı bir fıkrada belirtmiştir. Olası bir denetim yapılması halinde, gerçekleştirilen işlemlerin hukuka uygun yapıldığını ispatlayabilecek, gösterebilecek veya rapor verebilecek şekilde faaliyetlerine devam etmelidirler. Bunları gerçekleştiremeyen bir veri işleyeninin hukuka aykırı veri işleme ihtimali ortaya çıkmaktadır. Veri ihlali bildirimi yapılmayan veri ihlallerinde bile ihlalin mutlaka belgelenmesi gerekmektedir. Veri sorumluları, sadece uyumu sağlamakla kalmayıp uyumu belgelemek zorundadırlar. Bu sebeple gerekli uygunluk gösterilebilecek halde çalışılmalıdır. Böylece hesap verebilirlik ilkesinin gerekleri yerine getirilmiş olacaktır.

Hesap verebilirlik ilkesine ilişkin ABAD, UZ v Bundesrepublik Deutschland davasında (C-60/22), veri sorumlularının, GDPR kapsamında öngörülen yükümlülüklere uyum sağlamak ve bu uyumu belgelemekle sorumlu olduklarını vurgulamıştır. Özellikle ortak veri sorumluluğu sözleşmesi yapma yükümlülüğü ile veri işleme faaliyetlerinin kayıt altına alınması yükümlülüğünün, hesap verebilirlik ilkesinin somut örnekleri olduğunu belirtilmiştir.[158] Bu karar, GDPR'a uyum sağlanmasının belgelerle kanıtlanabilmesi önemine dikkat çekmektedir.

---

[156] Daha fazla bilgi için bakınız. Vedder, A., Naudts, L., **Accountability for the use of algorithms in a big data environment**, International Review of Law, Computers & Technology, 31(2), 2017, s. 206–224. https://doi.org/10.1080/13600869.2017.1298547

[157] Giakoumopoulos, Buttarelli, O'Flaherty, s.134.

[158] Case C-60/22 (Court of Justice), UZ v Bundesrepublik Deutschland [2023], ECLI:EU:C:2023:370, 45. paragraf.

Veri ihlal bildirimi ve hesap verilebilirlik ilkesi birbirine yakın kavramlardır. Veri ihlali yaşandığında önceden alınan önlemlerin var olduğunu kanıtlayıp hesap verebilmek gerekmektedir. Veri ihlali bildirimi ile veri özneleriyle açıkça iletişime geçilmektedir bu da hesap verebilirlik ilkesinin bir getirisi olarak görülmektedir. Veri ihlali bildirimi, hesap verilebilirlik ilkesinin gerçek hayattaki hali gibidir çünkü veri öznelerine veya denetim makamına hesap verilir niteliğinde bir bildirim yapılmaktadır. Hesap verilebilirlik ilkesi, ihlal bildirimleriyle bu şekilde bağlıdır.

3. KİŞİSEL VERİ İHLALİNE VE GENEL VERİ KORUMA TÜZÜĞÜ'NE İLİŞKİN GÜNCEL TARTIŞMALAR

GDPR ilkelerinin ardından, bu başlıkta kişisel veri ihlalinin ve GDPR'a ilişkin güncel tartışmalar ve bunların veri ihlali bildirimi ile bağlantısı belirtilecektir. GDPR, yapısı gereği insanların hayatındaki pek çok alana nüfuz eden bir hukuki düzenlemedir. Kişisel verilerin işlenmesini düzenlemesi ve kişisel verilerin insanların kullandığı uygulamalar, internet siteleri ve benzeri araçlar aracılığıyla işlenmesi bu duruma sebep olmuştur. GDPR'ın dünya gündemindeki yeri ile veri ihlal bildirimlerinin bağlantısının ise GDPR yürürlüğe girdikten sonra, bildirimin hangi durumlarda ve nasıl yapılacağı gibi unsurların net hale gelmesi sebebiyle bildirimlerin çoğalması olduğu görülmektedir. Ayrıca iki konunun da kişisel verilerin koruması alanında şeffaflık ve hukuki sorumluluk kavramlarına vurgu yapılarak kişisel verilerin korunmasını, dünya genelinde kabul edilmesi gereken bireylerin temel haklarından biri haline getirme amacı bulunmaktadır. Ayrıca GDPR kişilerin haklarına olan duyarlılığın artmasını sağlamıştır.

Dünya gündemine yansımasına sebep olan tartışmalar ise kişisel verilerin korunması amacıyla AB tarafından yapılan hukuki düzenlemelerin hükümlerine dayanmaktadır. Bu duruma büyük teknoloji şirketlerinden biri olan arama motoru Google'ın davası örnek olarak verebilir.

GDPR yürürlüğe girdikten sonra en çok ses getiren kısımlarından biri uygulama alanıydı çünkü GDPR'ın 3. maddesinin 2. fıkrası GDPR'ın AB dışındaki ülkelerde de AB vatandaşlarının verileri işlendiğinde uygulanması gerektiğini belirtmekteydi. Google İspanya davası ile de bu gündem gittikçe daha çok dikkat çekmiştir.[159] Google İspanya davası[160] bu duruma oldukça uygun somut bir örnek teşkil etmektedir. 2014 yılında ABAD, Google'ın bir Amerika Birleşik Devletleri şirketi olmasına rağmen

[159] Daha ayrıntılı bilgi için bakınız. Dal, s. 21-33.
[160] Case C-131/12 (Court of Justice) Google Spain SL and Google Inc. v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González [2014] ECLI:EU:C:2014:317.

AB'de bir kuruluşu bulunması sebebiyle 1995 tarihli Veri Koruma Direktifi'nin Google'a uygulanabileceği şeklinde önemli bir karar vermiştir. Unutulma hakkının öne çıktığı davada bu karar daha sonra yürürlüğe giren GDPR ile doğrulanmıştır.[161]

GDPR'a aykırı davranmak sebebiyle 2024 yılında verilen en büyük cezalardan biri LinkedIn şirketine verilen 310 milyon € cezadır.[162] İrlanda Veri Koruma Komisyonu reklamcılık ve davranış analizi amaçlı kişisel veri işleyen LinkedIn'ın bazı GDPR maddelerini ihlal ettiğini tespit etmiştir. Bunun üzerine kınama ve para cezası verilmiştir.[163] GDPR, zamanla diğer teknolojik alanlarla da ilişkili hale getirilmiştir. Buna örnek olarak Estonya'da bir start-up şirketi GDPR'a uyumluluk sağlanması için yapay zeka kullanmaya başlamıştır. GDPR hükümleri altında çalışan şirketler birçok belgeleme ve bu belgeleri güncel tutma işi ile uğraşmaktadırlar. Güncelleme ve kolayca belgeleme sağlama amacıyla yapay zekâ kullanmaktadırlar ve böylece zamandan da tasarruf eder hale gelmişlerdir.[164]

Kişisel verilerin korunmasının ve kişisel veri ihlallerinin önüne geçilmesinin önemli olmasına bir örnek, kişisel verilerin ülkelerin seçim sonuçlarını etkilemek adına kullanılmasıdır. Seçimlerin ve seçim sonuçlarının etkilenmesi sadece bir hipotez değil, gerçek hayatta da gerçekleşmiş bir durumdur. Cambridge Analytica isimli bir şirketin kişisel verileri kullanarak ve kişileri hedefleyerek oy sayısını artırmak amaçlı çalışmaları bu duruma önemli bir örnektir. Örneğin 2016 yılındaki Amerika Birleşik Devletleri başkanlık seçimlerinde Donald Trump'ın başkanlık kampanyası için Facebook üzerinden kişi hedefli reklamlar yapılmıştır. İnsanların kişilik özelliklerine göre dünya görüşü analiz edilmiş ve Trump'a oy vermeye yatkın olabilecek kişilere özel

[161] Daha ayrıntılı bilgi için bakınız. Ryngaert, Taylor, s.5-6.
[162] Ireland Data Protection Commission https://www.dataprotection.ie/en/news-media/press-releases/irish-data-protection-commission-fines-linkedin-ireland-eu310-million Erişim Tarihi 07.04.2025.
[163] Daha ayrıntılı bilgi için bakınız. https://www.skillcast.com/blog/biggest-gdpr-fines-2024 Erişim Tarihi 03.01.2025.
[164] Daha ayrıntılı bilgi için bakınız. https://www.gdprregister.eu/news/startup-uses-ai-for-gdpr-compliance/ Erişim Tarihi 03.01.2025.

reklamlar yapılmıştır. Yatkınlıkları ise kişilerin Facebook üzerindeki kişisel verilerinden ve Facebook üzerindeki aktivitelerinin işlenmesinden elde edilmiştir. Bu işlemeler sonucu kullanıcıların manipüle edilmesi kolaylaşmıştır. Bu şekilde gerçekleşen bir olayı GDPR yürürlükte olsa bile engelleyemeyeceğini belirten görüş de bulunmaktadır. GDPR'da belirtilen haklar bile Cambridge Analytica'nın müdahalesini muhtemelen durdurulamayacaktı, bunu durdurabilecek muhtemel şey unutulma haklarını savunmak olabilecekti.[165] Bu görüş de durumun ciddiyetini gözler önüne sermektedir.

Snowden olayı olarak bilinen, Edward Snowden isimli eski CIA çalışanının kitlelerin nasıl izlendiğine dair gizli belgeleri ifşa etmesi olayı ile veri güvenliği önemli gerekliliklerden biri haline gelmiştir. Snowden ifşalarından önce Avrupa'nın veri gizliliği adımları şirketler tarafından düzenlenirken Snowden ifşalarından sonra GDPR'a uygunluk tercih edilmeye başlanmıştır.[166] Bu örnekten de anlaşıldığı üzere tarihte yaşanan olaylar hukuki düzenlemeleri ve devletlerin konuya bakış açılarını da etkilemektedir.

Bu yaşanan örnek olaylar sonrasında, veri ihlali bildirimi açısından, uygulamada bildirimin kurum içinde gizlice düzenlenip bildirilmesi gibi olası negatif olasılıkların önü kesilmiştir. Bahsedilen örneklerde kişilerin gizliliği ihlal edilmiştir. Verilerin işlenmesinde rızanın gerektiği gibi alınmaması, şeffaf davranılmaması, siyasi çıkarlar gözetilmesi GDPR için veri ihlali bildirimi yapılması gerekebilecek hallerdendir. Bu örneklerdeki riskler, veri ihlali bildiriminin önlemeye çalıştığı tehlikelerdir. Veri ihlali bildiriminin GDPR'a göre, ileride detaylı şekilde değinileceği üzere, şeffaf, hızlı ve açık şekilde yapılması öngörülmüştür. Veri ihlalinden etkilenen bireylerin de bilgilendirilmesi gerektiğinden şeffaf ve doğru bilgilerin ulaştırılması bir kural haline

[165] Daha ayrıntılı bilgi için bakınız. Ward, A., **The Oldest Trick in the Facebook: Would the General Data Protection Regulation Have Stopped the Cambridge Analytica Scandal?**, Trinity College Law Review, 25, 2022, s. 241.
[166] Daha ayrıntılı bilgi için bakınız Rossi, A., **How the Snowden revelations saved the EU general data protection regulation**, The International Spectator, 53(4), 2018, s. 95-111.

gelmiştir. Böylece veri ihlali bildirimine olan medyanın ilgisi de artmıştır ve dünya genelinde bu konuda duyarlılık artmıştır. Veri güvenliğine dikkat edilip gerekli özenin gösterilmesine katkıda bulunulmuştur. Yüksek seviyedeki ihlaller, dünya genelinde yapılacak tartışmaları tetiklemektedir. GDPR'ın veri ihlali bildirimi, küresel olarak veri gizliliği ve güvenliği konusunda merkezi bir pozisyondadır. GDPR, dünyanın başka bölgelerinde çıkacak veri güvenliği veya veri korunması kurallarına ilham vermektedir. GDPR, teknoloji ve sosyal medya alanını ilgilendiren düzenlemelere sahip olduğundan GDPR'ın uygulandığı yerlerde gündemde kalmaya devam edecektir.

Bir sonraki bölümde kişisel veri ihlali bildirimi detaylı bir biçimde ele alınacaktır.

İKİNCİ BÖLÜM

1. KİŞİSEL VERİ İHLALİ BİLDİRİMİ

Bu bölümün ilk başlığında kişisel veri ihlali bildirimi ile ilgili bilinmesi gerekenler aktarılacaktır. "Veri ihlali bildirimi nedir?" sorusu, veri ihlalinin denetim makamına ve veri öznesine (veri sahibine) bildirilmesi alt başlıklarında incelenecektir. İnceleme sırası, GDPR hükümlerinin sırası takip edilerek yapılmıştır. Kişisel veri ihlali, GDPR'ın 4. maddesinin 12. fıkrasında tanımlanmıştır. 4. maddenin 12. fıkrası uyarınca "kişisel veri ihlali iletilen, depolanan veya başka bir şekilde işlenen kişisel verilerin kazara veya hukuk dışı yollarla yok edilmesi, kaybı, değiştirilmesi, izinsiz şekilde açıklanması veya bunlara erişime yol açan bir güvenlik ihlalidir."[167] şeklinde tanımlanmıştır.

Kişisel veri ihlali, verilere yetkisiz kişilerin ulaştığında gerçekleşmektedir. Yetkisi olmayan kişiler, ulaşmamaları gereken verileri ele geçirdiklerinde kendi menfaatleri için kötüye kullanma ihtimali doğmaktadır. Bu da veri öznelerinin veya veri sahiplerinin zarar görmesine yol açmaktadır. Bu zararın gerçekleşme ihtimali veya gerçekleşmiş olması sebebiyle veri öznelerine veya veri sahiplerine veri ihlali bildirimi yapılmaktadır. Veri ihlali bildirimi bu sebeple önem arz etmektedir.

1.1. Kişisel Veri İhlali Bildirimi

Veri ihlal bildirimi, ihlalin yaşanmasından itibaren denetim makamına yapılmak üzere veri sorumlusunun bir yükümlülüğüdür.[168] Veri ihlali, zamanında ilgilenilmezse veri öznelerinin kendi kişisel verileri üzerindeki kontrolü kaybetmelerine ve dolayısıyla finansal veya psikolojik zararlara sebebiyet verebilir.[169] Kişisel Veri İhlali Bildirimi, bu

[167] GDPR 4. madde 12. fıkra.
[168] Sevindi, Ordu, s.12-22.
[169] GDPR Dibace 85. paragraf.

sebeple GDPR'da düzenlenmiştir. Kişisel veri ihlali bildiriminin maddi unsurları veri ihlal bildiriminde bulunması gereken unsurlardır. Bu maddi unsurlar; kişisel veri ihlalinin önemi, ihlalden etkilenen kişi sayısı, ihlalin gerçekleştiği veri ve veri sahipleri kategorisi, veri koruma görevlisinin iletişim bilgileri, ihlalin tahmini sonuçları, alınabilecek önlemler ve denetim makamına bildirilirken geç bildirildiyse gecikme sebepleridir.[170] Bu maddi unsurlara ilerde Kişisel Veri İhlalinin Denetim Makamlarına Bildirilmesi başlığı altında değinilecektir.

Kişisel veri ihlali bildiriminin maddi unsuru ihlalin bir güvenlik açığı sonucu şeklinde gerçekleşmiş olmasıdır. Veri ihlali bildirimi denetim makamına veya veri öznesine (veri sahibine) internet üzerinden bir e-posta, bildirim, mesaj veya posta şeklinde yani haberi olması gereken kişi ve makamlara en açıkça ve hızlıca ulaştırabileceği şekilde haberdar edilmelidir. Denetim makamlarının kendi internet sitesinde veri ihlali bildiriminin yapılabileceği bir portalı olması durumunda bu portaldan veri ihlali bildirimi yapılmaktadır.

GDPR'da veri ihlali bildirimlerinin yapılış usulü üzerinde durulduğunda etkili bildirim nasıl yapılabilir ve etkili bildirim yapmanın önemi nedir, iyileştirmek için neler yapılabilir problemleri karşımıza çıkmaktadır. Örneğin veri ihlalinden etkilenen bir veri öznesine (veri sahibine) e-posta, mesaj, bildirim yoluyla ulaşılamıyorsa veri öznesi (veri sahibi) aranıp bilgilendirilebilir. Bu noktada amaç, yukarıda bahsedilen maddi ve şekli unsurlara uygun olarak bir bilgilendirmenin gerçekleştirilmesidir. Veri öznesine yapılacak bildirim, veri öznesinin anlayacağı şekilde açık ve net bir dille yapılmalıdır. Veri öznesine (veri sahibine) yapılacak bildirim, denetim makamına yapılacak bildirimdeki gibi hukuki bir dile ağırlık vermekten çok, herhangi bir veri öznesinin ya da veri sahibinin anlayabileceği şekilde yapılması bildirimi daha anlaşılabilir ve etkili kılacaktır.

[170] GDPR 33. madde 3. fıkra.

Veri ihlali bildirimini kimin yapacağı bildirilmiştir. Kişisel veri ihlali bildirimini veri sorumlusu yapmaktadır. GDPR'ın 33. maddesinde "Kişisel veri ihlalinin denetim makamlarına bildirilmesi" ve 34. maddesinde ise ""Kişisel veri ihlali hakkında veri öznesinin bilgilendirilmesi" düzenlenmiştir.

Veri ihlali bildiriminin nereye yapılacağı düzenlenmiştir. Kişisel veri ihlali bildirimi, GDPR 33. ve 34. maddede belirtildiği üzere ilgili denetim makamına veya veri öznesine yapılmaktadır. Yüksek tehlike bulunması durumunda veri öznesine de bildirim yapılması öngörülmüştür.

Veri ihlali bildiriminin hangi sürede yapılacağı belirtilmiştir. Kişisel veri ihlali bildiriminin en geç 72 saat içinde yapılması gerekmektedir. 33. maddenin 1. fıkrası uyarınca "Bir kişisel veri ihlali olması durumunda, kişisel veri ihlalinin gerçek kişilerin hakları ve özgürlükleri açısından bir riske sebebiyet vermesinin muhtemel olmadığı haller dışında, veri sorumlusu, fazla gecikmesizin ve uygun olması hâlinde, ihlalden haberdar olduktan itibaren en geç 72 saat içinde, kişisel veri ihlalini 55. madde uyarınca yetkili denetim makamına bildirir. Denetim makamına yönelik bildirimin 72 saat içinde yapılmadığı hallerde, bu bildirimle birlikte gecikme sebeplerine de yer verilir."[171] Burada karşımıza 72 saat kuralı çıkmaktadır. GDPR, veri ihlalinde veri sorumlusuna rapor verme görevi yüklemiştir ve bu ihlal teknik veya fiziki bir sebeple oluşabilmektedir.[172]

Ayrıca gecikmeden bildirim yapılması, kişilerin hakları ve özgürlükleri açısından bir risk olması durumunda diye belirtilmiştir ancak risk bulunmayan veri ihlallerinin de bildirilmesi sistemin işleyişi açısından daha faydalı olabilir mi? Örneğin risksiz görülen veri ihlalleri, diğer riskli olabilecek veri ihlallerinin önünün açılmasını

[171] GDPR 33. madde 1. fıkra.
[172] Voigt, von dem Bussche, s. 4.

kolaylaştırabilir mi? İlerleyen fıkralarda bu bildirimin içinde bulunması gereken bilgiler de sayılmıştır ancak bunlar yeterli midir? 72 saat kuralı ise süre olarak uygulamaya döküldüğünde kısa veya uzun bir süre olarak görülmekte midir?

Bu konuların irdelenmesi, GDPR'ın veri ihlali yaşandığında yapılacak bildirimlerin ve takip edilecek adımların uygulanmasına katkıda bulunacak ve daha etkin şekilde uygulanmalarını sağlayacaktır. Risk bulunmayan hallerde de veri öznesine veri ihlali bildirimi yapılması, veri öznesinde bir güven duygusu yaratacaktır. Risksiz görünen veri ihlallerinin riskli hale dönüşme ihtimali bulunabilmektedir. Veri ihlali bildiriminin içindeki unsurlar ise ihlalin mahiyetine göre değerlendirilmelidir. Büyük risk teşkil eden veri ihlallerinde ise 72 saat uzun bir süre olarak görülebilirken daha az riskli veri ihlalleri için ideal bir süre olarak görülebilir.

1.2. Kişisel Veri İhlalinin Denetim Makamlarına Bildirilmesi

Bu alt başlıkta denetim makamına bildirim ele alınacaktır. Kişisel verilerin denetim makamına bildirilmesi, kişisel veri kaybolduğunda veya sızdırıldığında, riskli olduğunda ilgili denetim makamına haber verilmesi anlamına gelmektedir. Kişisel veri ihlalinin denetim makamlarına bildirilmesi, önceden de belirtildiği üzere GDPR'ın 33. maddesinde düzenlenmiştir. Veri sorumlusunun veri ihlalini tespit ettikten sonra denetim makamına bildirme yükümlülüğü bulunmaktadır ancak veri ihlali gerçek kişilerin hak ve özgürlükleri için bir tehlike oluşturmuyorsa bildirmeyebilir. Bu durum istisnai bir hüküm olarak geçmektedir.

Ayrıca veri sorumlusu veri ihlalinden haberdar olduğu andan itibaren 72 saat içinde denetim makamına bildirmekle yükümlüdür. Eğer bildirme süresi 72 saati aşar ise bildirim yapıldığı vakit gecikme sebeplerine, neden gecikildiği bilgisine de yer

verilmelidir.[173] Böylece kişisel veri ihlali bildiriminin gereklilikleri yerine getirilmiş olmaktadır.

Kişisel veri ihlali bir güvenlik olayı olarak açıklanmıştır. Her kişisel veri ihlali bir güvenlik olayı iken her güvenlik olayı kişisel veri ihlali değildir.[174] Yani kişisel veri ihlali dışında farklı şekilde güvenlik olayları meydana gelebilmektedir ancak bu noktada bizi ilgilendiren güvenlik olayının kişisel veri ihlali şeklindeki güvenlik olayı olduğudur. Bir sistemdeki sunucunun çevrimdışı hale gelip saatlerce o şekilde kalması bir güvenlik olayıdır ancak bir kişisel veri ihlali değildir. Örneğin bir hacker tarafından kişisel verilerin bulunduğu bir veri deposu hacklendiğinde bir veri ihlali meydana gelmektedir ve veri ihlali bildirimi yapılması gereksinimi doğmaktadır. Bu örnekteki gibi bir veri ihlali yaşandığı durumlarda önceden değinilen veri depolamanın sınırlandırılması ilkesinin işlevi gündeme gelmektedir. Depolanan verilerin ilgili ilkeye uygun olarak sadece veri sahipleriyle eşleştirilecek şekilde ve veri işlemesi yapıldığı müddetçe depolanması, veri ihlali sonucunda meydana gelecek zararı en aza indirmeye yardımcı olacaktır.

Başka bir veri ihlali olan güvenlik olayı ise örneğin bir şirkette önceden çalışan bir çalışanın erişimi olduğu verileri, şirketten ayrıldıktan sonra mali kazanç elde etmek amacıyla satmasıdır. Bu bir iç tehdit örneğidir. İç tehdit, ihlalin şirketin içindeki veya önceden içinde bulunmuş bir şahıstan ve güvenlik açığından dolayı gerçekleşen tehdittir. Çalışanların yol açtığı ihlaller insan hatası şeklinde gerçekleşmektedirler. Bu örnekteki gibi kötü niyetli olmasa da bir e-postanın çalışan tarafından yanlış kişiye gönderilmesi de veri ihlaline yol açabilmektedir.

[173] GDPR 33. madde 1. fıkra.
[174] Daha ayrıntılı bilgi için bakınız. Article 29 Working Party (2017), Guidelines on Personal data breach notification under Regulation 2016/679, WP250, 3 October 2017, s.7. https://www.edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-personal-data-breach-notification-under_en Erişim Tarihi 05.01.2025.

İnternetteki sistem üzerinden değil de gerçek hayatta fiziki olarak gerçekleşme ihtimali olan bir veri ihlali ise, hassas bilgilerin bulunduğu bir belleğin çalınması veya yine hassas bilgilerin depolandığı şifresi de bulunmayan bir dizüstü bilgisayarın fiziki olarak ele geçirilmesi, çalınmasıdır. Bu örnekte veri ihlali belleğe veya dizüstü bilgisayara koyulabilecek bir şifre ile önlenebilirdi veya geciktirilebilirdi. Şifreleme bu noktada bir önleme aracı olarak görülebilmektedir.

Diğer bir veri ihlali şekli ise örneğin bir şirketteki çalışanın yaptığı işle hiç alakası olmadığı halde yetkisiz şekilde sadece merak edip görmek istediği için kişilerin adreslerine, sipariş geçmişlerine, tıbbi veya adli kayıtlarına açıp bakmasıdır. Bu durum, yukarıda da belirttiğimiz iç tehdit kavramına bir örnektir. Şirketin içinde bir veri ihlali yaşandığından şekli olarak bir iç tehdit sayılmaktadır. Bu ihlalde ilgili çalışanın yetkisi gözden geçirilip çalışanlar tekrardan bu konun önemi hakkında eğitilebilmektedir. Sonuç olarak, veri ihlali bildirimine bu gibi durumlar konu olabilmektedir ve denetim makamına bildirim ihtiyacını ortaya çıkarmaktadır.

Bir kişisel veri ihlali bildiriminde bulunması gereken unsurlar GDPR'ın 33. maddesinin 3. fıkrasında detaylı olarak belirtilmiştir. "Kişisel veri ihlalinin mahiyeti, etkilenen veri sahiplerinin kategorileri ve yaklaşık sayıları, etkilenen veri kayıtlarının kategorileri ve yaklaşık sayıları bulunmalıdır. Veri koruma görevlisi memurunun ismi ve iletişim bilgileri veya daha fazla bilgi alınabilecek bir irtibat yerinin iletişim bilgileri bulunmalıdır. Yaşanan kişisel veri ihlalinin muhtemel sonuçları bulunmalıdır. Veri sorumlusu tarafından alınan veya alınması teklif edilen zararlı, olumsuz etkileri hafifletecek önlemler de kişisel veri ihlalinde bulunmalıdır."[175]

Veri ihlali bildiriminin içeriğine ilişkin şekli unsurlar bu maddede tek tek sayılmıştır. Veri ihlali bildiriminin maddi unsuru ise kişisel verilerle ilgili bir ihlal

[175] GDPR 33. madde 3. fıkra.

olması, risk teşkil etmesi ve kapsamı ve etkisidir. Bu durumlara göre veri ihlali bildirimi yapılmaktadır. GDPR, yaşanan kişisel veri ihlali sonrası en etkili şekilde hareket edilmesine uygun tasarlanmıştır. Olası bir kişisel veri ihlalinde bir sürü ayrıntılı bilgiyi aynı anda verip asıl önemli noktaların gözden kaçırılması bu fıkra ile engellenmiştir. Bildirilmesi kişisel veri ihlali sonrası atılacak adımlar için elzem olan bilgilere öncelik ve önem verilmiştir. Bu durumla ilgili olarak da bilgilerin hepsi aynı anda ulaştırılamadığı durumlarda gecikme de yaşatılmayacak şekilde kalan iletilecek bilgilerin aşamalı olarak iletilmesine izin verilmiştir.[176]

Ayrıca veri sorumlusu kişisel veri ihlalini belgelerken ihlalle ilgili bilgilere ek olarak ihlal sonrası yapılanları da belgeler.[177] Veri ihlali bildirimi, tehlikelerin önlenmesi ve somut zarara dönüşmesini önleyebilmek için yararlı bir alet haline gelmiştir.[178] Böylece sadece veri ihlali değil, veri ihlalinin vereceği zararı azaltmak veya engellemek için neler yapıldığı da ayrıca belgelenecektir. Hukuka uygunluk ilkesine ve hesap verebilirlik ilkesine de bu belgeleme yöntemleriyle uyum sağlanacaktır. İşbu belgeler, veri ihlali sırasında ve sonrasında hukuka uygun davranılarak hareket edildiğine dair bir kanıt olacaktır.

Veri ihlali bildiriminde bulunması gereken unsurlarda verilerin kategorisinden kasıt kişilerin adı ve soyadı, telefon numaraları, e-posta adresleri ve kart bilgileri kategorileridir. İhlal sonucu bu kategorilerden hangisinin veya hangilerinin ele geçirildiği belirlenmektedir ve ona göre denetim makamına bildirilmektedir. Alınabilecek önlemlerde ise örneğin veri ihlali tek bir hesap üzerinden yaşandıysa o hesabın hemen kapatılması veya tüm sistemde yaşandıysa bütün var olan hesapların şifrelerinin sıfırlanması gibi yollar görülebilmektedir. Ayrıca bulunması gereken

[176] GDPR 33. madde 4. fıkra.
[177] GDPR 33. madde 5. fıkra.
[178] Daha ayrıntılı bilgi için bakınız. Schmitz-Berndt, S., **Edpb adopts updated guidelines on personal data breach notification under gdpr: the end of the one-stop-shop reporting mechanism for non-eu establishments**, European Data Protection Law Review (EDPL), 8(4), 2022, s.517-520.

unsurlardan biri var olan ihlalden etkilenen yaklaşık kişi sayısının da denetim makamına belirtilmesidir. Örneğin ülke genelinde birçok kişiyi etkileyen bir ihlal olması durumunda kamuoyuna açık bir duyuru şeklinde de bildirim yapılabilmektedir.

1.3. Kişisel Veri İhlalinin Veri Öznesine (Veri Sahibine) Bildirilmesi

Bu alt başlıkta veri öznesine ya da veri sahibine yapılan bildirim ve bu bildirime gerek bulunmayan durumlar incelenecektir. Veri ihlalinin veri öznesine bildirilmesi, veri öznesinin verileri ona zarar verebilecek şekilde bir ihlale uğradığında veri öznesinin bu durumdan haberdar edilmesidir. Bu madde ile veri öznesi, kendisini muhtemel zararlardan koruyabilmesi için uyarılmaktadır. Kişisel veri ihlalinin veri öznesine ya da veri sahibine bildirilmesi GDPR'ın 34. maddesinde açıklanmıştır. Veri ihlali gerçek kişilerin temel hak ve özgürlükleri bakımından yüksek seviyede bir tehlike arz ediyorsa veri sorumlusu gecikmeden veri sahibine bildirim yapar.[179] AB'de veri güvenliğinde risk faktörünün etkisi veri ihlali bildiriminden anlaşılmaktadır.[180] Yüksek risk durumunda veri öznesine bildirim bu duruma örnektir. GDPR 34. maddesine göre veri öznesine veya sahibine net ve açık bir şekilde veri ihlaline bilgilendirme yapılmalıdır.

Veri öznesine yapılacak bildirimin içereceği unsurlar 34. maddede belirtilmiştir. Tıpkı kişisel veri ihlalinin denetim makamına bildiriminde olduğu gibi veri öznesine ya da sahibine bildirimde de veri koruma görevlisinin iletişim bilgileri veya başka bir irtibat noktasının iletişim bilgileri, ver ihlalinin muhtemel sonuçları, veri ihlali sonrası alınan önlemler veri öznesine bildirilmektedir.[181] Veri öznesine yapılacak bildirimde alınabilecek önlemler ise veri öznesini bildirimle bilgilendirirken örneğin isim, telefon gibi hangi kategorideki bilgilerinin ihlale uğradığının belirtilmesidir. Başka bir önlem ise veri öznesini şüpheli bir durum gördüğünde veri sorumlusuna en kısa zamanda haber

[179] GDPR 34. madde 1. fıkra.
[180] Daha fazla bilgi için bakınız. Alunge, R., **Breach of security vs personal data breach: effect on eu data subject notification requirements**. International Data Privacy Law, 11(2), 2021, s.163-181.
[181] GDPR 34. madde 2. fıkra.

vermesi gerektiği konusunda bilgilendirmek ve veri öznesinin gördüğü tuhaf internet bağlantılarına güvenli olmaması sebebiyle tıklamaması gerektiğini iletmektir.

Veri ihlali sonrası, veri ihlaline uğrayan şirketin kendisi taklit edilerek veri öznesinin daha fazla bilgi paylaşması talep edilebilir. Bu tuzağa düşülmemesi adına bu konuda da veri öznesinin haberdar edilmesi alınabilecek önlemlerden birisidir. Böylece veri ihlali yaşandığına dair bildirimde veri öznesi karanlıkta bırakılmamaktadır. Veri öznelerine veya veri sahiplerine yol gösterilerek doğru şekilde ilerlemek amaçlanmıştır. Avrupa Veri Koruma Kurulu tarafından yayınlanan rehberde, bir veri ihlalini veri öznelerine bildirmenin, ihlal sonucu oluşabilecek risklere karşı veri öznelerinin kendilerini korumak için atabilecekleri adımlar hakkında bilgi sağlayacağı belirtilmiştir. Bildirimin odak noktasının veri öznelerini ve onların kişisel verilerini korumak olduğu vurgulanmıştır. Böylece veri ihlali bildiriminin, kişisel verilerin korunmasında uyumluluğu artıran bir araç olduğu açıklanmıştır.[182]

Kişisel veri ihlali veri öznesine ya da veri sahibine bildirilmesi gerekli olmayan bazı durumlar bulunmaktadır. Bu durumlar GDPR'ın 34. maddesinin 3. fıkrasında üç grup olarak düzenlenmiştir. Birincisi veri sorumlusu olan kişinin teknik ve kurumsal tedbirlerinin ve şifreleme gibi yöntemlerin kişisel veri ihlaline uğrayan kişisel verilere uygulanmış olmasıdır.[183] Şifreleme yöntemi ise kişisel veri ihlaline uğrayan verilerin, bu verilere erişim yetkisi olmayan kişilere karşı anlaşılamaz hale getirilmesi anlamına gelmektedir. Böylece yetkisiz şekilde kişisel verileri kullanmak isteyen kişiler verileri ele geçirse bile anlaşılmaz halde olmasından dolayı kendi lehlerine kullanamamaktadırlar. Kişisel veri bilinmez bir şekilde ortaya çıkmaktadır ve kullanılamamaktadır.

[182] European Data Protection Board, Guidelines 9/2022 on Personal Data Breach Notification under GDPR – Version 2.0, 28 March 2023, https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-092022-personal-data-breach-notification-under_en

[183] GDPR 34. madde 3. fıkra.

Şifrelemeye bir örnek olarak uçtan uca şifreleme verilebilmektedir. Uçtan uca şifrelemede örneğin mesajlar sadece gönderen ve alıcıya yani bir uçtan diğer uca sadece iki uçta net olarak gözükmektedir. Bu iki uç arasında üçüncü bir kişi veya saldırgan bu mesajlara ulaşmak isterse mesajlar ona karşı şifreli durumda bulunmaktadır.

İkinci veri öznesine ya da veri sahibine bildirilmesine gerek olmayan durum ise veri sorumlusunun yüksek tehlikeyi engelleyici ek tedbirler almış olmasıdır. Bu durumda da bildirimden muafiyet bulunmaktadır.

Üçüncü ve sonuncusu ise veri öznesi ya da veri sahibinin bilgilendirilmesinin orantısız bir uğraş gerektirmesi durumudur. Bu durumda yine aynı etkiyi yaratabilecek kamuya yönelik bir duyuru yapılabilir.[184] Ülke çapında ihlalden etkilenen kişi sayısı çok fazla olduğu veri ihlali durumlarında, herkese açık ve tüm halkın görebileceği şekilde bir duyuru ile bildirim yapılabilmektedir. Bildirilmesinde muafiyet bulunmasına rağmen kişisel veri sahiplerinin de güvenceye alınması unutulmamıştır. Aşırı gayret sarf edilmesi gereken bir bildirim ise bildirimi hiç yapmamak yerine duyması gereken veri öznelerine veya veri sahiplerine ulaşması açısından kamuya açık bir bilgilendirme veya bir uyarı yapılabileceği ayrıca belirtilmiştir. Bu bilgilendirmenin yapılması ise veri öznelerinin veya veri sahiplerinin, kurumlara ve kanunlara karşı güven duymalarını sağlamaktadır. Sonuç olarak sayılan bu üç durumda veri öznesine ihlali bildirimi yapılmasına gerek yoktur.

1.4. Veri Koruma Etki Değerlendirmesi

Bu alt başlıkta veri koruma etki değerlendirmesi; tanımı, yapılması gerektiği durumlar ve veri koruma görevlisine değinilerek açıklanacaktır. Veri koruma etki değerlendirmesi, yüksek risk içeren veri işlemelerine başlanmadan önce yapılan bir değerlendirmedir. Veri ihlalini önleyici bir araç olarak görülmektedir. Veri koruma etki

[184] GDPR 34. madde 3. fıkra.

değerlendirmesi GDPR 35. maddede ayrıntılı olarak açıklanmıştır. Veri koruma etki değerlendirmesi, özellikle yapılacak olan kişisel veri işleme faaliyeti gerçek kişilerin haklarına ve özgürlüklerine zarar verebilecek yüksek riskli bir veri işlemesi olacak ise veri işlemesi yapılmadan önce veri sorumlusu tarafından gerçekleştirilen bir değerlendirmedir. Ayrıca tek seferde birden çok kişisel veri işleme faaliyeti değerlendirilebilmektedir.[185] Veri koruma etki değerlendirmesi, teknolojik ilerlemelerin tetiklediği veri işlemesinde güvenliğin sağlandığından emin olunması ihtiyacını karşılayan bir araçtır.[186]

Veri koruma etki değerlendirmesinin, yüksek risk teşkil eden veri işlemelerinde yapılması gerektiği belirtilmiş olsa da sadece yüksek riskte değil, veri işlemesi yapılacak herhangi bir durumda yapılması güven sağlayacak bir durumdur. Veri koruma etki değerlendirmesi belgesi, veri işlemeden önce dikkatli davranıldığının kanıtı olan bir belgedir. Bu işleme önem verildiğini de kanıtlamaktadır. Örneğin bir şirkette gerçekleşecek veri işlemelerinin hepsinde bu değerlendirmenin gerçekleştirilmesi; şirketin müşterilerine, hissedarlarına, çalışanlarına bir güven sağlayacaktır. Ayrıca, veri işlemesi öncesi, varsa farkına varılmayan tehlikelerin de günyüzüne çıkması sağlanacaktır. Unutulmamalıdır ki, bugün düşük risk olarak değerlendirilen bir veri işleme faaliyeti ilerde yüksek risk teşkil edecek hale gelebilmektedir. Veri koruma etki değerlendirmesi yapılmasının ise eksi bir tarafı bulunmayıp sadece artı yönleri bulunmaktadır.

[185] GDPR 35. madde 1. fıkra.
[186] Daha ayrıntılı bilgi için bakınız. Boban, M., **GDPR and Data Protection Impact Assessment (DPIA),** Economic and Social Development, International Scientific Conference on Economic and Social Development, 61, 2020, s. 215-223.

Veri koruma etki değerlendirmesi, veri güvenliğinin sağlanması alanında tesiri kuvvetli bir alet olarak görülebilmektedir.[187] GDPR'da ayrıyeten veri sorumlusu bu görevi yerine getirirken önceden belirlenmiş ise veri koruma görevlisinin tavsiyesine başvurmaktadır.[188] Veri koruma görevlisi, kişisel veri işleyen kurumlarda kurallara uygunluk konusunda tavsiye veren görevlidir ve hesap verilebilirliğin ana unsurlarındandır. Ayrıca denetim makamı, veri öznesi (veri sahibi) veya çalışmak için atandıkları kuruluş arasında aracı görevi görmektedir. [189] Veri koruma görevlisine DPO denilmektedir. GDPR'da 37. maddede geçmektedir. DPO kısaltması ile kastedilen *"data protection officer"* yani "veri koruma görevlisi"dir.

Veri koruma görevlisinin aracı görevi, onu bulunduğu kurum içinde GDPR için bir yerel iletişim noktası haline getirmektedir. Denetim makamıyla kurum arasındaki bir bağlantı yeri olarak görülmektedir. Veri koruma görevlisi hem görevli olduğu kurumu hem de o kurumda çalışanları GDPR sorumlulukları ile ilgili bilgilendirmektedir ve gerekli olan noktalarda tavsiyelerde bulunmaktadır. Veri koruma görevlisi ile veri ihlali bildiriminin bağlantısı şu şekildedir; veri koruma görevlisi, bildirimi kendisi yapmamakla birlikte bildirimi yapacak olan veri sorumlusuna hukuka uygun ve vaktinde karar vermesi konusunda yol gösterip yardımda bulunmaktadır.

GDPR 37. maddede veri koruma görevlisinin atanmasının zorunlu olduğu üç durum olduğu belirtilmiştir. Birincisi eğer kişisel veri kendi yetkisinin alanı içinde çalışan mahkememeler hariç bir kamu organı tarafından işlenecekse veri koruma görevlisi atanmalıdır. İkinci olarak ise kişisel veri işlemenin temel faaliyeti bu veri sahiplerinin (veri öznelerinin) sürekli olarak izlenmesini gerektiriyorsa veri koruma

[187] Daha ayrıntılı bilgi için bakınız. Yordanov, A., **Nature and ideal steps of the data protection impact assessment under the general data protection regulation**, European Data Protection Law Review (EDPL), 3(4), 2017, s. 486-495.
[188] GDPR 35. madde 2. fıkra.
[189] Giakoumopoulos, Buttarelli, O'Flaherty, s.175.

görevlisi atanmalıdır. Üçüncüsü ise ana görev olarak mahkûmiyet kararları ve suçlara ilişkin kişisel veriler işlenecekse yine veri koruma görevlisi atanması beklenmektedir.[190]

Bu üç durumda GDPR'ın veri koruma görevlisinin atanmasını zorunlu tutması anlaşılabilir bir durumdur çünkü hassas veya büyük miktarda kişisel veri işlenmesi söz konusudur. Özellikle veri sahiplerinin ya da veri öznelerinin sürekli olarak izlenmesi, onlar hakkında oldukça detaylı ve değerli kişisel verilere ulaşılmasına neden olacaktır. Bu değerde bir kişisel veri tabanına, sistemsel bir arıza sebebiyle oluşabilecek kişisel veri ihlaline ek olarak bizzat bu toplanan verilerin ele geçirilmesi amacıyla yetkisiz üçüncü şahıslar tarafından saldırı düzenlenme ihtimali de vardır. Zira toplanan kişisel veriler örneğin hedefli reklamcılık gibi alanlarda çalışan şirketler için altın değerinde olmaktadır. Hedefli reklamcılık ise belirli reklamların o reklamların etki edeceği emin oldukları kişilere yapılmasıdır.

Hedefli reklamcılığa kısaca değinecek olursak örneğin sosyal medya şirketleri kullanıcılarından genel olarak bir ödeme almamaktadırlar ancak bu gelirleri kendi sitelerindeki veya uygulamalarındaki hedefli reklamcılık sayesinde kazanmaktadırlar. Reklam veren kişiler, internet sitesindeki kullanıcıların cinsiyeti, yaşı ve ilgileri hakkında verilere ulaşarak reklamın doğru hedefe ulaşmasını sağlamaktadırlar.[191]

Bu duruma örnek olarak yeni nişanlanıp ilişki durumunu "nişanlı" olarak değiştiren sosyal medya uygulaması kullanıcı bireyin daha sonra sosyal medyayı kullanırken önüne çıkan reklamlar yaşadığı yerdeki gelinlikçiler, çiçekçiler olmaktadır.[192] Başka bir örnek olarak ise arama motorunda aratılan veya fiyat araştırılması yapılan bir ürün, daha sonra sosyal medya uygulamalarının reklamlarında tekrar o kullanıcının önüne çıkarılmaktadır veya önceden satın alınan ürün benzeri

[190]GDPR 37. madde 1. fıkra.
[191] Giakoumopoulos, Buttarelli, O'Flaherty, s.361.
[192] Giakoumopoulos, Buttarelli, O'Flaherty, s.362.

ürünler o kullanıcıya gösterilmektedir. Kullanıcının yaşına, ırkına, cinsiyetine göre gösterilen içerikler bile değişebilmektedir. Hedefli reklamcılığın amacı da tam olarak budur ve bu yöntemlerle hedefine ulaşmayı amaçlamaktadır.

Veri koruma görevlisi atanması gereken somut durumlardan birine örnek olarak hastanelerdeki hastaların verilerin işlenmesini verebiliriz. Sigorta şirketlerinin sağlık alanında çalışanları, hastaneler özel nitelikte verilerin sorumlularıdırlar. AB, biyometrik ve genetik verileri de özel nitelikli olarak nitelendirmiştir.[193] Sağlık kuruluşları veya sigorta şirketleri gibi bu tarz verileri işleyen kurumların veri koruma görevlisi ataması zorunlu bir görev haline gelmiştir. Zira bu kurumlar tarafından oldukça detaylı ve büyük bir ölçekte veri işlenmektedir. Hastanelerin, sigorta şirketlerinin bireylerin doğum tarihi, kimlik numaraları, ev veya iş adresleri, telefon numaraları, hastalıkları ile ilgili detayları veya geçirdikleri kaza ilgili bilgiler gibi pek çok bilgiye yaptıkları iş mahiyetiyle ulaşma imkânları bulunmaktadır. Bu ulaştıkları kişisel verileri ise yetkisiz üçüncü şahıslara satmamak veya sistemsel bir veri ihlali yaşanmasını önleyebilecek tedbirleri almak bu kurumların sorumluluğu altında bulunmaktadır.

Veri sorumlusu veya veri işleyen, veri koruma görevlisinin kişisel verileri korunması ile ilgili konulara uygun ve zamanında dahil olmasını sağlamakla yükümlüdür. Veri koruma görevlisinin ihtiyacı olan kaynakları da sağlamalıdırlar. Ayrıca veri koruma görevlisi işini yaparken kimseden emir almamalıdır.[194] GDPR, veri koruma görevlisine güvence sağlayarak onun veri sorumlusu veya veri işleyen tarafından işten çıkarılamayacağını ve cezalandırılamayacağını vurgulamıştır. Veri koruma görevlisi raporunu da direkt en üst yönetim kademesine vermektedir.[195]

[193] Giakoumopoulos, Buttarelli, O'Flaherty, s.176.
[194] GDPR 38. madde 1. ve 2. fıkra.
[195] GDPR 38. madde 3. fıkra.

Veri koruma görevlisi, işini gerektiği şekilde yaptığı sebebiyle cezalandırılmamalıdır. Veri koruma görevlisinin tarafsızlığını etkileyecek şekilde, örneğin veri koruma görevlisinin çalıştığı bir şirket tarafından veri koruma etki değerlendirmesinin sonucunun düşük risk çıkmasını sağlamasına dair görevliye bir baskı yapılması gibi eylemlerde bulunulmaması gerekmektedir. Bu noktada GDPR, bu güvenceleri veri koruma görevlisine sağlayarak onun tarafsız bir şekilde işini yapmasını sağlamıştır. Bağımsız ve tarafsızca, görevli oldukları kurumun olası yönlendirmelerine karşı bir koruma ile beraber görevlerini yerine getirmelerine olanak sağlanmıştır.

Veri koruma görevlisi aynı zamanda birkaç işini birlikte yürütebilmektedir ancak yaptığı işler arasında çıkar çatışması olmamasına dikkat etmekle yükümlü kılınmıştır.[196] Veri koruma görevlisi, arasında çıkar çatışması olan iki tarafın işlerini yaparsa yaptığı işler çelişeceğinden böyle bir hüküm koyulmuştur. Gelecekte oluşabilecek karışıklıkları engellemek amacıyla hareket edilmiştir. Veri koruma görevlileri denetim sırasında, GDPR yükümlülüklerini yerine getiren şirketleri, çalışanları bilgilendirir ve tavsiyelerde bulunurlar.[197] Veri koruma görevlisi depolanan verilerin görevli olduğu şirkete nasıl giriş yaptığını, şirkette nasıl işlendiğini ve nasıl çıkış yaptığını da incelemektedir. Bu veri akışı her şirketin veya kurumun kendisine göre düzenlediği bir olgudur. Farklı şirketlerde farklı şekillerde veri işlenmesi veya farklı önlemlerin kullanılması karşılaşılabilecek bir durumdur. GDPR'a uyulduğu sürece bu durum sorun teşkil etmeyecektir. GDPR'a uyulmadığında ise veri koruma görevlisi gerekli uyumun sağlanmasını sağlayabilecektir veya uyum için yapılması gerekenler hakkında tavsiye verecektir.

Veri koruma görevlisi, görevli olduğu kurumun içinden bir çalışan veya dışardan bir görevli olabilmektedir. Ancak kurumun içinden bir görevli olduğunda, yönetim veya

[196] GDPR 38. madde 6. fıkra.
[197] GDPR 39. madde 1. fıkra.

karar verici pozisyonlardaki çalışanlardan biri veri koruma görevlisi olmaması gerekmektedir. Zira mantıken yönetici bir görevlinin karar verdiği bir konuda aynı zamanda değerlendirmeler de yapması çıkar çatışmasına yol açacaktır. Ayrıca veri koruma görevlisine işini yapabilmesi için zaman verilmesi, finansal destek sağlanması veya ihtiyacına göre görevlinin yanına çalışanlar verilmesi gerekmektedir. Sadece bir veri koruma görevlisi atandığını belirtmek yeterli değildir, veri koruma görevlisi işini layığıyla yerine getirebilmelidir. Bu iş için gerekli ortamın veri koruma görevlisinin çalıştığı kurum tarafından sağlanması gerektiği sonucuna ulaşılmaktadır. Böylece veri koruma görevlileri, veri koruma etki değerlendirmesini yaparak görevlerini yerine getirmiş olmaktadırlar. Bu bilgilendirme ve tavsiyeler sadece yönetici pozisyonundaki çalışanları değil diğer çalışanları da etkiler durumdadır.

Veri ihlal bildirimi açısından ise veri koruma görevlisinin gözetiminde işleme yapılması sebebiyle olası bir ihlal durumunda, hızlı bir şekilde ihlalin farkına varılmaktadır ve veri ihlali bildiriminin süratli ve etkin bir şekilde yapılmasını sağlamaktadır. Veri koruma görevlisinin veri koruma etki değerlendirmesi ile bağlantısı ise, verdiği zorunlu tavsiyeleri ve uzmanlığı ile veri koruma etki değerlendirmelerinin GDPR'a uygun, etkin ve eksiksiz olmasını sağlamasında ortaya çıkmaktadır.

Denetim makamları, düzenli olarak yapılan veri koruma etki değerlendirmelerinin sonuçlarının gözden geçirilmesini desteklemelidir.[198] Veri koruma etki değerlendirmesi veri ihlali oluşmasını engellemeye yöneliktir ve veri ihlali bildirimi ise ihlal oluştuktan sonraki veri güvenliği aletidir. İkisi de veri güvenliği alanında faaliyet göstermektedir ve kişilerin gizliliğine önem vermektedirler. Veri koruma etki değerlendirmesi ve veri ihlali bildirimi birbirini tamamlayan iki kavramdır. Bir sonraki başlıkta kişisel veri ihlali bildirimi sonrası karşılaşılan olgular ele alınmıştır.

[198] Daha fazla bilgi için bakınız. Binns, R., **Data protection impact assessments: meta-regulatory approach**, International Data Privacy Law, 7(1), 2017, s. 22-35.

2. KİŞİSEL VERİ İHLALİ BİLDİRİMİ SONRASI

Kişisel veri ihlali bildiriminin nasıl yapıldığına ve ilgili durumlara ilişkin incelemelerden sonra bu başlıkta kişisel veri ihlali yaptırımları ve etkililiklerine değinilecektir. Kişisel veri ihlali bildirimi sonrasında denetim makamı tarafından duruma göre bazı yaptırımlar uygulanabilmektedir. Denetim makamı olan kuruluş tarafından alınabilecek somut olaya uygun tedbirler olabilir. Tedbirler dışında idari para cezaları yaptırımı da uygulanabilmektedir. GDPR'da belirtildiği üzere GDPR kurallarına uyumun önemine istinaden, ihlal durumunda alınan tedbirlere ek olarak idari para cezaları verilmektedir. Hafif seviyede bir ihlal varsa veya idari para cezası gerçek kişiye ölçülülük ilkesine aykırı bir yük olacaksa idari para cezası yerine kınama cezası verilebilmektedir.[199] Görüldüğü üzere yaptırım uygulanırken ölçülülük ilkesine uygunluk koşulu da vurgulanmıştır. Adil davranılarak adillik ilkesine de uygun hareket edilmiştir.

GDPR Dibacesi 148.paragrafa göre GDPR ihlali sebebiyle verilecek ceza AB hukukunun genel ilkelerine riayet etmelidir.[200] AB hukuku ise; insan onuruna saygı, özgürlük, demokrasi, eşitlik, hukukun üstünlüğü ve insan haklarına riayet gibi temel ilkelere dayanmaktadır.[201] Örneğin GDPR'ın ihlali nedeniyle idari ceza verilirken veya ulusal hukuk kurallarının da ihlali sebebiyle adli ceza verilirken aynı suçtan dolayı iki kez yargılanmamalıdır. "Ne bis in idem" yani "aynı suç nedeniyle aynı kişi iki kere yargılanamaz." ilkesi burada da geçerli olmaktadır.[202] Hukuka uygunluğu sağlayan önemli ilkelerden biri olan "Ne bis in idem"e veri güvenliği alanında da yer verilmesi, bu alanın temel haklarla ne kadar ilişkili olduğunu gözler önüne serer niteliktedir.

[199] GDPR Dibace 148.paragraf.
[200] GDPR Dibace 148.paragraf.
[201] Charter of Fundamental Rights of the European Union, OJ C 326, 26.10.2012, s. 391–407.
[202] GDPR Dibace 149.paragraf.

Bu alan, doğası gereği hukuk ve bilişim ile el ele gitmektedir. Birbirinden farklı disiplinlerin birleştiği bir ortak nokta haline gelmiştir. Veri ihlali bildiriminin bağlantılı olduğu AB genel ilkesi ise temel haklardır. AB Temel Haklar Şartı 8. maddedeki "Kişisel verinin korunması hakkı", AB hukuk düzeninde korunan bir haktır.

2.1. Kişisel Veri İhlali Yaptırımları

Bu alt başlıkta kişisel veri ihlalinin yaptırımları ele alınacaktır. Kişisel veri ihlali yaptırımları, kişisel veriler gerektiği şekilde korunamayıp ihlale uğradıklarında uygulanmaktadır. GDPR, kişisel veri ihlali yaptırımı olarak idari para cezasını öngörmüştür. GDPR'ın 83. maddesinde bu idari para cezalarının verilip verilmeyeceğine veya verilecekse miktarının nelere göre belirleneceğine dair ayrıntılı düzenlemelere yer verilmektedir.

GDPR 83. maddeye göre; idari para cezası verilirken, kişisel veri ihlalinin önemi (etkilenen veri sahipleri sayısı ve etkilenme dereceleri), ihlalin kasıtlı mı yoksa ihmalle mi gerçekleştiği, veri sorumlusu veya veri işleyen tarafından zararın azaltılması için yapılanlar, onların sorumluluk dereceleri ve daha önce böyle bir ihlal olayı olup olmaması kıstaslarına bakılmaktadır.

Ayrıca, ihlal sonrası denetim makamıyla ne kadar işbirliği içinde bulundukları, etkilenen kişisel veri kategorisi, denetim makamının ihlalden haberdar olma şekli (veri sorumlusu veya veri işleyenin ihlali bildirip bildirmediği, bildirdiyse ne ölçüde bildirdiği gibi.) de idari para cezası kararında etkilidir. Önceden alınan tedbirlere uyma şekilleri ve ihlalden doğrudan veya dolaylı elde edilen fayda veya kaçınılan zarar gibi kıstaslara dikkat edilmektedir.[203] Bu kıstaslarda dikkat çekilmesi gereken detaylardan biri önceden belirlenen tedbirlere uyumdur. Kişisel veri ihlali yaşanmaması için önceden alınan tedbirler varsa ve bunlara uyum sağlanmayıp kişisel veri ihlali

[203] GDPR 83. madde 1. ve 2. fıkra.

gerçekleştiyse idari para cezasının ağırlaşabileceği öngörülmüştür. İdari cezayı belirlerken tüm bu kriterlere dikkat edilerek adil ve ölçülülük ilkesine de uygun olacak bir idari ceza verilmektedir.

2.1.1. Para Cezaları

GDPR'ın koyduğu kuralların ihlali sonucuna yaptırım olarak idari para cezaları da öngörülmektedir. Bu cezalar daha önce açıklanan yukarıdaki kriterlere bakılarak hesaplanmaktadır. GDPR, ayrıyeten mali hesaplamaların yapılmasına yol göstermek için ayrıntılı düzenlemiştir.

GDPR'ın 83. maddesinin 4. ve 5. fıkralarında veri ihlali kaynaklı idari cezaların nasıl hesaplama yapılacağı belirtilmiştir. Öncelikle denetim makamı tarafından, GDPR'ın ihlali halinde 20.000.000 €'ya kadar veya bir teşebbüsün söz konusu olması halinde dünya çapındaki cirosunun %4'üne kadar idari para cezası verilmektedir. Bunlardan hangisi yüksekse o ceza verilmektedir. Bu cezanın verilebilmesi için veri işlemenin ana kurallarına ve rızanın koşullarına yönelik ihlal, veri sahibinin (veri öznesinin) haklarının ihlal ve kişisel verilerinin üçüncü ülkelere aktarımını düzenleyen hükümleri ihlal, durumları gerçekleşmiş olmalıdır.[204] Ayrıca denetim makamı tarafından verilen bir talimata veya getirilen geçici ya da kesin işleme sınırlamasına veya veri akışlarını askıya almasına uygun hareket edilmemesi veya ihtiyaç duyulan bilgilerin sağlanmasında veri sorumlusu veya veri işleyenin temsilcisine talimat verilmesi ihlali durumunda da bu belirtilen ceza verilebilmektedir.[205]

Diğer ihlallerde ise denetim makamı tarafından, 10.000.000 €'ya kadar para cezası veya bir teşebbüs söz konusuysa dünya çapındaki cirosunun %2'sine kadar para cezası verilebilmektedir. Burada da bu iki seçenekten hangisi yüksekse o ceza

[204] Daha ayrıntılı bilgi için bakınız. Giakoumopoulos, Buttarelli, O'Flaherty, s.248.
[205] GDPR 83. madde 5. fıkra.

uygulanmaktadır.[206] GDPR 83. maddede bu durum düzenlenmiştir. İdari para cezası seçeneklerinden en fazla olanın seçilip verilmesi, idari para cezalarının üst sınırdan verildiğini göstermektedir. Bu yaptırım miktarlarının bu kadar yüksek meblağlarda olması, AB'nin veri korunmasını ne kadar ciddiye aldığını göstermektedir. AB hukuk sisteminin içinde çok da önemli olmayan bir ihlal olarak gözükmesine izin verilmeyip bireye ait olmasından dolayı değerli olan verilerin önemi vurgulanmıştır.

Ayrıca AB üyesi devletler içinde Danimarka ve Estonya'da bu GDPR'a göre idari para cezası verilememektedir. Bu iki ülkede kendi hukuklarına uygun bir adli ceza şeklinde yaptırım uygulanmaktadır ancak bu verilecek ceza aynı idari para cezaları gibi caydırıcı ve etkili olmak zorundadır.[207] Danimarka ve Estonya bu kuralın istisnası olmuş durumdadır ancak yine de aynı etkiyi sağlayan yaptırımlar sağlanacağının garantisi verilerek eşitlik sağlanmıştır. Böylece diğer AB ülkeleriyle aynı pozisyonda olmuşlardır. AB üye devletleri arasında aynı mevzuat uygulanmadığı durumlarda bile AB vatandaşları arasında adalet sağlanması ve ayni adil sonuca ulaşılabilmesi için gerekli düzenlemeler yapılmıştır.

2.1.2. Para Cezalarının Etkililikleri ve Somut Örnekleri

GDPR'ın uygulanmasında verilen idari para cezaları etki yaratmaktadır. Kişisel veri işleyen şirketlerin yaptıkları işlem sırasında GDPR'a uygun davranmaya teşvik etmektedir. Önceden belirtilen miktarlarında görüldüğü üzere caydırıcılık seviyeleri yüksektir.

Veri sahipleri (veri özneleri), veri koruma hukukuna ilişkin ihlallerin iç hukuk yollarıyla giderilememesi hâlinde, son merci olarak Avrupa İnsan Hakları Mahkemesi'ne bireysel başvuruda bulunabilmektedir.[208] GDPR kapsamındaki kişisel veri ihlallerine karşı, veri öznesi öncelikle ilgili ulusal denetim makamına ve ardından iç

[206] Daha ayrıntılı bilgi için bakınız. Giakoumopoulos, Buttarelli, O'Flaherty, s.248.
[207] GDPR Dibace 151. paragraf.
[208] Daha ayrıntılı bilgi için bakınız. Giakoumopoulos, Buttarelli, O'Flaherty, s.236.

hukuk yollarına başvurmalıdır. Ancak iç hukuk yollarının etkisiz kalması veya hakkaniyete aykırı bir karar verilmesi hâlinde, veri öznesi, Avrupa İnsan Hakları Sözleşmesi'nin 8. maddesi kapsamında özel hayatın ve kişisel verilerin korunması hakkının ihlal edildiğini ileri sürerek Avrupa İnsan Hakları Mahkemesi'ne bireysel başvuruda bulunabilir.[209] Ancak bu durum ülke içindeki yargı yolları tüketilmiş olduğu zaman mümkündür. Verilen idari para cezalarının caydırıcılıklarının yanı sıra ortada ciddi hukuksuzluk ve adaletsizlik bulunduğu düşünülüyorsa bu şekilde bir yol olduğu da belirtilmiştir.

Denetim makamı tarafından kendisiyle ilgili bağlayıcı bir karar verilen kişi, kararı mahkemeye götürebilmektedir. Denetim makamının bulunduğu AB üye devletinin mahkemelerinde bu dava açılmalıdır.[210] Veri sorumlusu veya veri işleyene karşı açılacak dava ilgili veri sorumlusu veya veri işleyenin bulunduğu üye devlette açılacaktır. Ayrıyeten kamu kurumuna dava açılacaksa veri öznesinin mutat meskeninin bulunduğu üye devlette açılabilmektedir.[211] Mutat mesken kavramı ise bireyin yaşama niyetiyle fiilen oturduğu yer anlamına gelmektedir.

Para cezalarının somut örnekleri içinde şimdiye kadar en büyük ceza Meta şirketine verilen 1.2 milyar € para cezasıdır.[212] İrlanda Veri Koruma Komisyonu tarafından verilen ceza GDPR'a aykırı davranılmasından dolayı verilen en büyük cezalardandır. Meta şirketi Instagram, WhatsApp gibi dünya genelinde oldukça popüler uygulamaların sahibidir.[213] Milyonlarca kullanıcıya sahip olan bu uygulamalar, bu kişilerle ilgili birçok önemli bilgiye sahiplerdir. Kişinin yaşı, ırkı, cinsiyeti, adresi, telefon numarası gibi temel bilgilere ek olarak o kişinin ne tarz müzik sevdiği, alışveriş

[209] Avrupa İnsan Hakları Sözleşmesi, 8. madde ve 34. madde. https://echr.coe.int/documents/convention_eng.pdf Erişim Tarihi 04.06.2025.
[210] GDPR 78. madde.
[211] GDPR 79. madde.
[212] Case T-325/23 (General Court) Meta Platforms Ireland v EDPB [2023] 62023TN0325.
[213] Daha ayrıntılı bilgi için bakınız. Data Privacy Manager https://dataprivacymanager.net/5-biggest-gdpr-fines-so-far-2020/

yapma alışkanlıkları, nerelere gitmeyi sevdiği gibi çok spesifik bilgilere de sahip oldukları aşikârdır. Kişiye özel gösterilen reklamlarda da bu bilgiler göz önünde bulundurulmaktadır. Dolayısıyla bu uygulamaların sahibi olan şirketler veya kurumlar oldukça kullanışlı kişisel veri depolarına sahiplerdir.

Bu ve bunun gibi para cezaları ülkeleri GDPR'a uygun davranmaya teşkil etmektedir. GDPR'a uygun davranmamanın ciddi mali sonuçlara sebep olabileceğinin somut örneklerinden biridir.[214]

Hedefli reklamcılık konusunda verilmiş ve yine en büyük idari para cezalarından biri 746 milyon €'luk cezadır.[215] Bu ceza, Amazon isimli şirkete Lüksemburg Ulusal Veri Koruma Komisyonu tarafından verilmiştir. Ceza, 10.000 kişinin bir Fransız gizlilik hakları grubuna Amazon'u şikâyet etmesi üzerine incelenip verilmiştir.[216] Yine İrlanda Veri Koruma Komisyonu tarafından Meta şirketine verilen büyük cezalarından biri 405 milyon €'luk cezadır.[217] Bu idari ceza ise 13-17 yaş arası çocukların verisini kamuya açık göstermekten dolayı verilmiştir. Ayrıca muhtemel yüksek tehlike olduğunda Veri Koruma Etki Değerlendirmesi de yapılmamıştır.[218] Bu durum da ilgili idari para cezasının miktarının belirlenmesinde rol oynamıştır.

Örneklerde de belirtildiği üzere idari para cezaları GDPR'ın doğru uygulanmasını sağlamak için etkilidir. Ancak bu idari para cezaları verilirken tabii ki ölçülülük ilkesine riayet edilmektedir. Salt caydırıcı olması amacıyla bu büyüklükte idari para cezaları verilmemekte, somut olayın özelliklerine göre hesaplaması

[214] Daha ayrıntılı bilgi için bakınız. Data Privacy Manager https://dataprivacymanager.net/5-biggest-gdpr-fines-so-far-2020/
[215] CNPD decision regarding Amazon Europe Core S.À R.L. https://cnpd.public.lu/en/actualites/national/2025/03/amazon-decision.html Erişim Tarihi 07.04.2025.
[216] Daha ayrıntılı bilgi için bakınız. Data Privacy Manager https://dataprivacymanager.net/5-biggest-gdpr-fines-so-far-2020/
[217] Ireland Data Protection Commission (DPC Inquiry Reference: IN-20-7-4) https://dataprotection.ie/en/news-media/press-releases/data-protection-commission-announces-decision-instagram-inquiry Erişim Tarihi 07.04.2025.
[218] Daha ayrıntılı bilgi için bakınız. Data Privacy Manager https://dataprivacymanager.net/5-biggest-gdpr-fines-so-far-2020/

yapıldıktan sonra bu büyüklüğe ulaşmaktadır. Bir sonraki başlıkta ise veri sorumlusunun ihlal bildirimindeki yükümlülükleri ve etkili bildirimden bahsedilecektir.

3. KİŞİSEL VERİ İHLALİ BİLDİRİMİNDE VERİ SORUMLUSUNUN YÜKÜMLÜLÜKLERİ VE ETKİLİ BİLDİRİM YAPMANIN ÖNEMİ

Kişisel veri ihlali yaptırımlarından sonra bu başlıkta veri sorumlusunun yükümlülükleri ve veri ihlali bildiriminin etkisinin önemi ele alınacaktır. Kişisel verilerin işlenmesinde önemli sorumluluklardan biri veri işleyenin veya veri sorumlusunun üzerindedir. Öyle ki veri sorumlusu veya veri işleyen yaptıkları veri işleme eylemlerinin kayıtlarını tutmalıdır. Gerektiğinde ise bu kayıt bilgilerini denetim makamına sunabilmelidirler.[219] Kişisel veri ihlali yaşanan bir durumda bildirimin yapılması için gerekli olan bilgiler açısından da bu kayıtların tutulması önem arz etmektedir. Ayrıca ihlalin büyüklüğünün anlaşılması açısından yardımcı olacaktır.

Veri güvenliğinin risk seviyesi belirlenirken nelere dikkat edilmesi gerektiği GDPR Dibacesinde 83.paragrafta belirtilmiştir. Veri sorumlusu veya veri işleyenin olası risklere karşı bazı önlemler alması gerektiği belirtilmiştir. Buna örnek olarak şifreleme yöntemi verilmiştir.[220] Şifreleme yöntemi, mesajların sadece iletişim kuran kişiler arasında anlaşılabilmesi anlamına gelmektedir.[221] Şifreleme, gizliliği koruması sebebiyle veri koruma alanında yeni teknolojiye uyum açısından da yararlı görülmektedir.[222]

[219] GDPR Dibace 82.paragraf.
[220] GDPR Dibace 83.paragraf.
[221] Daha ayrıntılı bilgi için bakınız. Giakoumopoulos, Buttarelli, O'Flaherty, s.185.
[222] Daha ayrıntılı bilgi için bakınız. Spindler, G., Schmechel, P., **Personal data and encryption in the european general data protection regulation. Journal of Intellectual Property, Information Technology and Electronic Commerce Law**, 2016, 7(2), s. 163. https://heinonline.org/HOL/Page?collection=journals&handle=hein.journals/jipitec7&id=174&men_tab=srchresults Erişim Tarihi 06.03.2025.

Ayrıca GDPR, bu şifreleme işleminin yapıldığına dair kanıtlar bulunmasını istemektedir. Örneğin, bir bilgisayarda diskinde yapılan şifreleme işlemi gibi.[223] GDPR, şifreleme yöntemini bir veri ihlalini hafifletmeye yarayacak temel yöntemlerden biri olarak görmektedir.[224] Bunun gibi yöntemlerle tedbirler önceden alınmış olmalıdır ve güvenlik sağlanmış olmalıdır. Risk seviyesi belirlenirken dikkat edilecek hususlar ise; iletilen, depolanan veya başka şekilde işlenen kişisel verilerin; özellikle fiziksel, maddi veya manevi zarara yol açabilen, kazara veya hukuka aykırı olarak yok edilmesi, kaybı, değiştirilmesi, izinsiz olarak açıklanması veya bunlara erişilmesi gibi işleme faaliyetinin yol açtığı risklerin gözetilmesi olarak belirtilmiştir.[225] Kişisel veriler işlenirken bahsedilen bu riskler oldukça önemli risklerdir. Örneğin kişisel verilerin izinsiz olarak açıklanması ve bunlara erişim sağlanması durumunda veri sahipleri veya veri özneleri adeta ifşa edilmiş olmaktadırlar. Bu da bu kişileri pek çok dolandırıcılık, tehdit, kimlik hırsızlığı ve daha birçok tehlikeye açık hale getirmektedir. Özel hayatlarıyla, sağlık bilgileriyle veya adres, telefon gibi iletişim verileriyle ilgili olabilecek bu veriler kötü niyetli üçüncü kişilerin elinde tabiri caizse kendilerine kâr sağlayacak bir silaha dönüşmektedir.

Ayrıca kimlik bilgileri, sağlık bilgileri veya kişinin ekonomik durumuyla ilgili finansal bilgilerin ele geçirilmesi tek başına o kişiye zarar verebilir ancak bunların birden çoğunun ele geçirilmesi ise kimlik hırsızlığı gibi daha da büyük ve önemli bir zarara yol açabilmektedir.[226] Dikkat edilmesi gereken, ilk başta belki de önemsiz bir veri ihlali gibi gözüken olayların devamının yaşanması halinde topaklanarak büyüyen

[223] Daha ayrıntılı bilgi için bakınız. Mansfield-Devine, S., **Meeting the needs of GDPR with encryption. Computer Fraud & Security**, 2017(9), s.18. https://www.sciencedirect.com/science/article/abs/pii/S1361372317301008 Erişim Tarihi 06.03.2025.
[224] Daha ayrıntılı bilgi için bakınız. Whitworth, M., **Data at Rest Encryption and Key Management in GDPR**, IDC Analyze the Future, 2018, s. 6. Erişim tarihi 06.03.2025.
[225] GDPR Dibace 83.paragraf.
[226] Daha ayrıntılı bilgi için bakınız. Article 29 Working Party (2017), Guidelines on Personal data breach notification under Regulation 2016/679, WP250, 3 October 2017, s.24. https://www.edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-personal-data-breach-notification-under_en Erişim Tarihi 06.03.2025.

bir çığ gibi daha büyük olumsuz olaylara sebebiyet verebileceği gerçeğidir. Verileri ihlale uğrayan bireyin çocuk olması durumunda ise çocukların kişisel bilgilerinin gizli tutulması gerektiğinden çok daha önemli bir veri ihlaline dönüşebileceği de akılda tutulmalıdır.

Kişisel veri işlenmesi öncesi yapılan veri koruma etki değerlendirme raporunun sonucuna göre kişisel veri işleme faaliyeti, veri sorumlusunun hâlihazırda bulunan teknolojisine ve uygulayabileceği tedbirlere rağmen yüksek risk içeriyorsa kişisel veri işleme faaliyeti öncesi denetim makamı ile istişare edilmelidir.[227] Bu istişare sonucuna göre kişisel veri işleme faaliyetine devam edilmelidir.

Kişisel veri ihlali bildiriminin etkili şekilde yapılmasının önemi GDPR'da da belirtildiği üzere şu konularda önem arz etmektedir: zamanında ve usulüne uygun şekilde elle alınmayan kişisel veri ihlalleri, veri öznelerinin kimlik verilerinin kontrolünü kaybetmelerine sebep olabilir. Kişilerin ırkçılığa ve ayrımcılığa maruz kalmaları, insanlık onurlarının zedelenmesi, mesleki sırlarının ortaya çıkarak kişilerin maddi ve manevi zarara uğraması gibi olumsuz sonuçlar doğurabilir.[228] Bu sebepledir ki kişisel veri ihlalinin etkili olabilmesi için denetim makamına söz konusu ihlal bildirimi yapılırken 72 saat içinde yapılması gerektiği belirtilmiştir. Veri sahibine veya veri öznesine söz konusu ihlalin yaşandığının bildirimi de gecikmeden yapılması işaret edilmiştir.

Kişisel veri ihlali bildirimi yapıldıktan sonra yapılacak bilgilendirmede verileri ihlale uğrayan gerçek kişiye ne yapması gerektiğine dair önerilerde bulunulmalıdır. Bu tavsiyeler muhtemel menfi tesirlerin yumuşatılması açısından da önem arz etmektedir.[229] Veri ihlali bildiriminin etkili şekilde yapılmasının yollarından biri de bu

[227] GDPR Dibace 84.paragraf.
[228] GDPR Dibace 85.paragraf.
[229] GDPR Dibace 86.paragraf.

püf noktasıdır. Bildirimin sadece haber vermek amaçlı değil aynı zamanda ihlalin etkisini hafifletmeye yarayacak şekilde yapılması öngörülmüştür. Böylece olası kötü sonuçlardan en azından bir kısmının önüne geçilebilmesi sağlanmaktadır. Bir sonraki başlıkta veri ihlali bildirimlerinin iyileştirilmesine odaklanılacaktır.

4. KİŞİSEL VERİ İHLALİ BİLDİRİMLERİNİN İYİLEŞTİRİLMESİ

Kişisel veri ihlalinde veri sorumlusunun yükümlülüklerinden ve etkili bildirimden sonra, bu başlıkta kişisel veri ihlali bildirimlerinin iyileştirilmesi incelenecektir. Kişisel veri ihlali bildirimlerinin iyileştirilmesi kavramı, veri ihlali bildiriminin GDPR'da düzenlenmiş haline ek olarak nelerin en yüksek fayda sağlayacağına dair fikirler olarak açıklanabilir. Bu kavram şu anki düzenlemenin faydasız olduğu anlamına gelmemektedir. Kişisel veri güvenliğinin temel amacına bakıldığında amacın bir kişisel veri ihlalinin yaşanmasını önlemek ve bir kişisel veri ihlali yaşandıysa da makul süre içinde zamanında harekete geçilmesi olduğu görülmektedir.[230] Bu temel amaç doğrultusunda veri ihlali bildirimi zaman içinde sürekli geliştirilerek bildirimin gelişen teknolojiye de ayak sağlaması sağlanacaktır. Böylece yararlı işlevini kaybetmemiş olacaktır.

Her kişisel veri ihlali aynı risk seviyesinde olmamaktadır. Örneğin bir hastanenin kişisel verilerine bir ihlalden ötürü anlık ulaşılamaması o hastanede acil ameliyata alınacak bir hastanın kişisel sağlık geçmişi bilgilerine ulaşılamaması sebebiyle hastanın hayatını kaybetme riskinin doğmasına bile yol açabilmektedir. Başka bir risk seviyesine örnek olarak da örneğin bir medya haber şirketinin saatlerce takipçilerine haberlerini ulaştıramaması verilebilir.[231] Bu iki örnek de farklı sebeplerle oluşabilecek kişisel veri ihlalleridir ancak risk açısından bakıldığında hastane örneğinde insan hayatı söz konusu olabilecek kadar ileri bir risk seviyesi görülmektedir.

Medya haber şirketi örneğinde ise şirketin medya haber platformlarının takipçilerinin azalmasına, etkileşimlerinin azalmasına ve uzun vadede şirketin sponsorlarının çekilmesi gibi maddi zararlara sebep olabilecek bir risk seviyesi görülmektedir. İki örnekte de bir kişisel veri ihlali bulunmasına rağmen birisi gerçek

[230] Daha ayrıntılı bilgi için bakınız. Article 29 Working Party, s.6.
[231] Daha ayrıntılı bilgi için bakınız. Article 29 Working Party, s.9.

kişilerin hak ve özgürlüklerine karşı yüksek risk içermektedir. Ancak diğer örnekte aynı seviyede risk olmaması, o kişisel veri ihlalini o şirketin ve şirkette çalışanların ekonomik durumu için daha az önemli hale getirmemektedir. Her kişisel veri ihlali, kendi içinde verileri ihlale uğrayan veri öznesi için önem teşkil etmektedir. Bu sebepledir ki aynı özen bu şekildeki kişisel veri ihlallerinin bildiriminde de gösterilmelidir.

Veri ihlalinin gerçekleştiğinin çabuk bir şekilde tespiti için teknolojik ve kurumsal önlemlerin tümü uygulanmalıdır.[232] Bildirimin gecikmeksizin yapılması, veri ihlalinin niteliğine ve veri sahibinde yarattığı negatif yansımalarına bağlı olarak değerlendirilmelidir. Bu bildirim, denetim makamının duruma müdahalede bulunması ile sonuçlanabilir.[233] Şöyle ki kişisel veri ihlali bildiriminin iyileştirilmesinin yollarından biri de ihlalin mahiyetine göre süre konusunda yeterince hızlı mı yoksa ihlalin büyüklüğüne göre bildirimin hızı yavaş mı kalmış şeklinde bir sorgulama yapılmasıdır. Zira normal tehlike seviyesindeki bir kişisel veri ihlalinde makul sürede bildirim yapılması veri sahibinin zararının karşılanması için harekete geçecek kadar yeterli süre verebilirken, yüksek tehlike seviyesindeki bir kişisel veri ihlalinde geçen her zaman birimi değerlidir. Veri öznesine ve denetim makamına ne kadar erken ulaşılabilirse onların o kadar lehine hareket edilebilecektir. Bu durumda kısacası "Zararın neresinden dönülürse kârdır." yaklaşımı ile çözüme ulaşmak daha etkili olacaktır.

Bir kişisel veri ihlali yaşanıp yaşanmadığına dair veri sorumlusu herhangi bir ilk uyarıda bu durumu araştırmalı ve gerekli sonuca ulaşmalıdır. Araştırmasında gerekli kanıtları toplayıp bir veri ihlalinin yaşandığına dair yeterli yani makul kanıya ulaştıktan

[232] GDPR Dibace 87.paragraf.
[233] GDPR Dibace 87.paragraf.

sonra ilgili denetim makamına bildirmelidir.[234] Bu noktada şüphe üzerine harekete geçip ilgili soruşturmaları yapmak veri sorumlusunun yükümlülüğü olarak ortaya çıktığı görülmektedir. Veri sorumlusu "birlikte veri sorumluları *(joint controller)*" olabilmektedir. Birlikte veri sorumluları, birden fazla veri sorumlusu bulunduğunda ortaya çıkmaktadır. Kişisel verilerin işlenme gayesine ve usulüne iki veya daha fazla veri sorumlusu birlikte karar veriyorsa bunlar birlikte veri sorumlusu olmaktadırlar.[235] Bahsedilen sorumluluğu ise aralarında nasıl paylaşacaklarını bir sözleşmeyle belirlemeleri önerilmektedir. Bir veri ihlali yaşandığında kim liderlik yapacak veya kim sorumluluk alacak gibi konularda önceden belirlenmelidir.[236] Böylece birlikte sorumluluk halinde de veri ihlali bildiriminin zamanında ve etkili bir şekilde yapılması sağlanacaktır. Bir sonraki başlıkta yargı kararlarına değinilecektir.

[234] Daha ayrıntılı bilgi için bakınız. Article 29 Working Party, s.12-13.
[235] GDPR 26. madde.
[236] Daha ayrıntılı bilgi için bakınız. Article 29 Working Party, s.13.

5. KİŞİSEL VERİLERİN KORUNMASI İLE İLGİLİ YARGI KARARLARI

Veri ihlali bildirimlerinin incelenmesinden sonra, burada yargı kararları ele alınacaktır. Bu kararlar, veri korumaya yönelik kuralların uygulamaya döküldüğünde gerçek hayata olan yansımaları olarak değerlendirilebilmektedir. GDPR ile GDPR'dan önceki dönemlerle ilgili ABAD tarafından verilen yargı kararları bulunmaktadır. Bu kararlar, GDPR'ın getirdiği ve GDPR'dan önceki kuralların gerçek hayatta uygulamaya geçirildiğinde veya bu kuralların gerektiği gibi uygulanmadığında ortaya çıkan olaylar üzerine verilmiş kararlardır. Bazıları ise kişisel verileri koruma alanında diğerlerinden daha çok ses getirmiş emsal niteliğinde kararlar olarak görülmektedir.

Bu kararlardan biri Google İspanya v AEPD davasında[237] verilen karardır. AEPD, İspanya'nın Veri Koruma Ajansı'dır. Dava, Bay Gonzáles isimli şahsın borçlarını ödemesine rağmen kendi adını Google arama motorunda arattığında hala eskiden kalan haciz açık arttırma ilanının en başta çıkmasını İspanya Veri Koruma Ajansı'na şikâyet etmesiyle başlamıştır. Ulusal mahkemenin ilgili ilanı kaldırmayıp arama motorunda çıkan bağlantılarla ilgili bölümü onaylaması üzerine, Google temyize başvurmuştur ve İspanya Ulusal Yüksek Mahkemesi, ABAD'a ön karar prosedürü ile sorular sormuştur.[238] Daha sonra ABAD'a taşınan olayda Google için 10 Milyon € para cezası kararı verilmiştir.[239] ABAD, arama motorunda çıkan bilgilerin kişisel verileri

[237] Case C-131/12 (Court of Justice) Google Spain SL and Google Inc. v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González [2014] ECLI:EU:C:2014:317.

[238] Daha ayrıntılı bilgi için bakınız. Saygın, D., Yılmaz, Y. E., **C-131/12- Google İspanya v. AEPD Davası ve 2014/19685 Numaralı C.K. Anayasa Mahkemesi Bireysel Başvurusu Kapsamında Avrupa Birliği Hukukunda Unutulma Hakkı ve Türk Hukuk Sistemine Yansıması**, Anadolu Üniversitesi Sosyal Bilimler Dergisi, 23(3), 2023, s. 685-700. https://doi.org/10.18037/ausbd.1257429 Erişim Tarihi 07.03.2025.

[239] Clifford Chance Article https://www.cliffordchance.com/insights/resources/blogs/talking-tech/en/articles/2022/05/spanish-data-protection-agency-imposes-10-million-euro-fine-on-g.html Erişim Tarihi 07.03.2025.

içermesi sebebiyle bu sonuçların da kişisel veri sayılmasına ve bahsedilen bağlantıların kaldırılmasına karar vermiştir.[240]

Bu davanın odak noktası ise önceden bahsedilen unutulma hakkı olmuştur. Davadaki hali ise artık geçerli olmayan haberlerin/bilgilerin kişinin faydasına olacak şekilde unutulabilmesi olarak ortaya çıkmıştır. Veri ihlali sonucu kişinin haysiyetine zarar verebilecek sonuçlara ulaşılması ve kamuya açık şekilde görülmesi tehlikesinden önceden bahsedilmişti. Bu davada da unutulma hakkına riayet edilmemesi sebebiyle benzer bir sonuç gerçekleşmiştir. Bu durum, kişisel verileri koruma gayesinin, verilerin bireye ait olmasından dolayı onlara atfedilen değere dayandığını göstermektedir.

Bu noktada değinmek gerekir ki Google gibi büyük teknoloji şirketleri, dünya üzerinde hemen hemen çoğu insanın kullandığı uygulamaların sahibidir. Teknoloji liderlerinin uygulamalarından uzak kalmak öğrenciler, çalışanlar gibi kişiler için mümkün gözükmemektedir çünkü bu teknoloji iş ve okul hayatında gerekli olmaktadır. Bu nedenle kişiler kendi verilerini kendileri bu teknoloji liderlerine vermektedir.[241] Uygulamalar, resmi olarak bir zorunluluk olmamasına rağmen iş hayatında veya sosyal hayatta adeta bir zorunluluk, bir gereklilik haline gelmiştir. Bu uygulamaları hayatına dahil eden kullanıcılar, ilgili uygulamaları kullanmak için gizlilik sözleşmesi ve kişisel verilerinin işleneceğine dair sözleşmeleri kabul etmek zorunda kalmaktadırlar. Gerçekten istemese bile uygulamayı kullanmak için bu sözleşmeleri kabul eden kullanıcı bireyler, kendi rızalarıyla kişisel verilerini paylaşmış sayılmaktadırlar. Uygulamada gerçekleşen olası bir veri ihlalinde ise bu paylaştıkları bilgilere yetkisi olmayan kişilerce ulaşım sağlanabilmektedir. Bu dava GDPR'ın kapsamı açısından veri ihlal bildiriminin çerçevesiyle uyuşmaktadır. GDPR veri ihlali bildiriminde gözetilen

[240] Case C-131/12 (Court of Justice) Google Spain SL and Google Inc. v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González [2014] ECLI:EU:C:2014:317.
[241] Dilsiz, V., **Dijital Dünyada Kişisel Veri Kavramı ve KVKK/GDPR Kapsamında Bir Değerlendirme**, 2021. s.5

hesap verebilirlik ilkesinin ve veri sorumlusunun yükümlülüklerinin temelinin atılmasında etkili olmuştur.

Bir diğer örnek ise TR v Land Hessen[242] kararıdır. Davanın tarafları TR ve Land Hessen'dir. TR bir gerçek kişidir ancak kararda adı anonimleştirilmiştir. Bu sebeple adı TR olarak geçmektedir. Hessen ise Almanya'nın bir eyaletidir. Dava ABAD önüne Hessen'in başkenti olan Wiesbaden'deki idare mahkemesinin sorusu üzerine gelmiştir. Somut olay 2019 yılında Sparkasse isimli Alman bankasının kendi bünyesinde gerçekleşen bir veri ihlalini Hessen Veri Koruma Otoritesi'ne bildirmesi ile başlamıştır. GDPR 33. maddeye göre denetim makamına bildirim yapılmıştır. Veri ihlali Sparkasse çalışanlarından birinin hukuka aykırı şekilde TR'nin verilerine erişimi sonucu gerçekleşmiştir.[243]

Sparkasse Bankası bu veri ihlalini sadece denetim makamına bildirmiş ve yüksek risk teşkil etmediğine kanaat getirdiğinden veri öznesine bildirimde bulunmamıştır. Bunun üzerine veri öznesi 2020 yılında TR ise Hessen Veri Koruma Otoritesi'ne kendisine GDPR 34. maddeye uygun bir bildirim yapılmadığına ve otoritenin gerekli yaptırımı Sparkasse Bankası'na uygulamadığına dair şikâyette bulunmuştur. Hessen Veri Koruma Otoritesi ise Sparkasse Bankası'nın 34. maddeyi ihlal etmediği, yüksek risk olmadığı için bildirmediği ve veri ihlalini yapan çalışanın eriştiği bilgileri kopyalamadığı veya paylaşmadığı ve bankanın gerekli disiplin işlemlerini uyguladığı belirtmiştir.[244]

TR bu yanıta karşılık Wiesbaden İdare Mahkemesi'nde dava açmıştır. Hessen Veri Koruma Otoritesi'nin, şikâyeti gerektiği gibi değerlendirmediğini ileri sürüp Hessen Veri Koruma Otoritesi'nin Sparkasse Bankası'na yaptırım uygulamasını talep

[242]Case C-768/21 (Court of Justice) TR v Land Hessen [2024] ECLI:EU:C:2024:785.
[243]Case C-768/21 (Court of Justice) TR v Land Hessen [2024] ECLI:EU:C:2024:785. 14.paragraf.
[244]Case C-768/21 (Court of Justice) TR v Land Hessen [2024] ECLI:EU:C:2024:785. 16.paragraf.

etmiştir.[245] Wiesbaden İdare Mahkemesi ise ABAD'a, veri korunmasına aykırı olarak bir veri ihlali yaşandığında GDPR'a aykırılık sebebiyle, denetim makamının düzeltici yetkilerini kullanıp idari para cezası gibi yaptırımlar uygulamasının gerekip gerekmediğini sormuştur.[246] ABAD ise denetim makamlarının her veri ihlalinde idari para cezası gibi yaptırımlar uygulamak zorunda olmadıklarına ve bu tür önlemlerin gerekli, ölçülü olduğundan emin olmaları gerektiğine karar vermiştir.[247] Kararın somut bir analizi yapılır ise, Sparkasse Bankası GDPR 33. madde kapsamında denetim makamına bildirim yükümlülüğünü yerine getirmiştir. GDPR 34. madde açısından ise banka, yüksek risk olmadığından veri sahibine haber vermemiştir. ABAD'ın kararı, bu değerlendirmelerin incelemeye tabi olduğunu göstermiştir.

Eleştirel bir değerlendirme yapılır ise bu kararda, uygulanacak önlem ve yaptırımların denetim makamının takdir yetkisine bağlı olduğu görülmüştür. Veri sorumlusu yeterli önlemleri aldıysa daha fazla aksiyonun haksız olduğuna karar verebileceği belirtilmiştir. Ancak fark edilmelidir ki bu takdir yetkisi veri korumasının ve güvenliğinin sürdürülmesi ihtiyacı ile sınırlanmıştır. Verilerin korunması amacı gözden çıkarılamamaktadır. Bu karar ile veri öznesi açısından, bir veri öznesi gereğine uygun karar verilmediğini düşündüğünde uygun makamlara başvurabileceğinden emin olunması sağlamıştır. Karara dair başka bir değerlendirmede bulunulur ise ilgili karar ile GDPR 33. ve 34. maddelerinin nasıl uygulanması gerektiği ayrıntılı şekilde açıklanmıştır. Uygulanacak yaptırımların ise her davaya göre ayrı değerlendirilmesi ve ölçülü olması gerektiği vurgulanmıştır.

[245]Case C-768/21 (Court of Justice) TR v Land Hessen [2024] ECLI:EU:C:2024:785. 18.paragraf.
[246]Case C-768/21 (Court of Justice) TR v Land Hessen [2024] ECLI:EU:C:2024:785. 20.paragraf.
[247]Case C-768/21 (Court of Justice) TR v Land Hessen [2024] ECLI:EU:C:2024:785. 51.paragraf.

Başka bir örnek ise VKI v Amazon[248] davasıdır. VKI, Verein für Konsumenteninformation yani Tüketici Bilgilendirme Derneği anlamına gelmektedir. Davanın tarafları VKI ve Amazon'dur. Bu davada ABAD'a Amazon tarafından kişisel verilerin işlenmesinin Amazon'un ticari faaliyette bulunduğu her üye devletin kurallarına uyması gerekip gerekmediği konusunda gidilmiştir.[249] ABAD ise Amazon'un ticari faaliyetlerini yönlendirdiği diğer ülkelerin veri koruma kurallarına tabi olacağına dair karar vermiştir.[250] Ticari faaliyetlerine bir örnek olarak ise Amazon'un yaptığı reklamlar verilebilir. Amazon'un işlediği kişisel veriler, veri öznelerinin (veri sahiplerinin) bulundukları üye devletin kurallarına uyması, muhtemel bir veri ihlalinde o şahıslara ve ilgili denetim makamına yapılacak bildirim usule uygun yapılacağı için etkili olacağını temin etmektedir. Dava, veri sorumlularının AB içinde veri ihlal bildiriminde de bulunan şeffaflık ilkesine ve yükümlülüklerine önem vermesi gerektiğini vurgulamıştır.

Weltimmo[251] davası olarak bilinen bir diğer dava ise Slovakyalı bir şirket olan Weltimmo ile Macaristan Ulusal Veri Koruma ve Bilgi Edinme Özgürlüğü Kurumu arasındadır. İnternet sitelerinde Macaristan'daki mülklere ilişkin ilanların, reklamların bulunması Macaristan'daki veri koruma kurallarına aykırı olup idari para cezası verilmesi üzerine konu ABAD'a taşınmıştır. İlgili incelemeler sonunda Weltimmo'nun Macaristan'da sabit bir kuruluşa sahip olduğunun gözlemlenmesi üzerine ilgili Macar veri koruma kurallarının uygulanacağına karar verilmiştir.[252] Veri ihlali açısından Macaristan'daki gayrimenkul sahiplerinin verilerinin bu şekilde güvenceye alındığı

[248]Case C-191/15 (Court of Justice) Verein für Konsumenteninformation v Amazon EU Sàrl [2016] ECLI:EU:C:2016:612.
[249] Daha ayrıntılı bilgi için bakınız. Case C-191/15 (Court of Justice) Verein für Konsumenteninformation v Amazon EU Sàrl [2016] ECLI:EU:C:2016:612,72.paragraf.
[250] Daha ayrıntılı bilgi için bakınız. Case C-191/15 (Court of Justice) Verein für Konsumenteninformation v Amazon EU Sàrl [2016] ECLI:EU:C:2016:612, 81.paragraf.
[251] Case C-230/14 (Court of Justice) Weltimmo s.r.o. v Nemzeti Adatvédelmi és Információszabadság Hatóság [2015] ECLI:EU:C:2015:639.
[252] Daha ayrıntılı bilgi için bakınız. Giakoumopoulos, Buttarelli, O'Flaherty, s.196.

görülmektedir. Bir veri sorumlusunun AB ülkesinde ne zaman yaptırıma tabi olacağını belirtmesiyle dolaylı yoldan veri ihlal bildirimi kuralları ile örtüşmektedir.

Toplanan kişisel verilerin kurallara uygun depolanması gerektiğine dair bir örnek ise Uber isimli taşımacılık şirketine Hollanda Veri Koruma Otoritesi tarafından kesilen 290 Milyon € cezadır.[253] Hollanda merkezli Uber isimli şirketin sürücülerinin hassas ve önemli bilgilerini bir koruma olmadan Amerika Birleşik Devletleri'nde depoladığının ortaya çıkması üzerine bu para cezası verilmiştir.[254] Sürücülerin Uber sürücüsü olarak çalışabilmesi için alınan kimlik bilgileri, adres bilgileri gibi kişisel veriler korunarak işlenmesi gereken verilerdir. Uber sürücülerinin kişisel verilerinin gerekli önlemler olmadan ve habersiz depolanması veri ihlaline davetiye çıkarmaktadır. Bu bilgilerin sızdırılması gibi durumlarda ilgili veri özneleri veya veri sahipleri kötü niyetli kişilerin hedefi haline gelebilmektedir. Bundan ötürü ilgili veri koruma kurulu tarafından gereken yaptırım olan idari para cezası uygulanmıştır. Bir sonraki başlıkta GDPR'ın etkilerine ve Türk hukukunda veri ihlali bildirimine değinilecektir.

[253] The Autoriteit Persoonsgegevens (The Dutch data protection authority) https://autoriteitpersoonsgegevens.nl/en/current/dutch-dpa-imposes-a-fine-of-290-million-euro-on-uber-because-of-transfers-of-drivers-data-to-the-us Erişim Tarihi 07.04.2025.

[254] Daha ayrıntılı bilgi için bakınız. Data Privacy Manager https://dataprivacymanager.net/5-biggest-gdpr-fines-so-far-2020/ Erişim Tarihi 07.03.2025.

6. GENEL VERİ KORUMA TÜZÜĞÜ'NÜN ETKİLERİ VE TÜRK HUKUKUNDA VERİ İHLAL BİLDİRİMİ

Bu başlıkta GDPR'ın etkilerinden ve Türk hukukunda, KVKK'da veri ihlali bildiriminden bahsedilecektir. Öncelikle GDPR'ın sınır aşırı etkisinden bahsedilecektir.

6.1. GDPR Sınır Aşırı Etkisi

Bu alt başlıkta GDPR'ın sınır aşırı etkisi ve veri ihlali bildirimi ile ilişkisi incelenecektir. GDPR'ın sınır aşırı yetkisi, AB sınırları dışındaki yerlere de GDPR'ın ulaşması ve o noktalarda da geçerli olması anlamına gelmektedir. İç Pazar ile finansal olarak yaşanan bütünleşme, hem kamu hem de özel sektör arasında veri akışını artırmıştır.[255] Bu sebeple GDPR sınır ötesi etkiye sahip olmuştur.

GDPR'ın 3. maddesinde bölgesel kapsamdan bahsedilmiştir. Önceden değinildiği üzere, 3. madde uyarınca veri işlemelerinin GDPR uygulama alanına girmesi için ya AB sınırları içindeki bir kurum tarafından gerçekleşmelidir ya da AB dışında olup AB'deki bireylere mal veya hizmet satışı yapılmalı veya AB'deki bireyleri izliyor olmalıdır.[256] Bu maddeden anlaşıldığı üzere; Türkiye'de kurulan şirketler, AB'dekilere satış yapmak, onları izlemek veya AB'deki bir kişiyle iletişimde bulunmakta, verilerini işliyorlarsa GDPR'a tabi olacaklardır. Bu şirketler hem GDPR'a hem de KVKK'ya uyum sağlamakla yükümlü olacaktır.[257] AB'deki bireylerle ekonomik faaliyetlerine devam etmek isteyen kuruluşların, GDPR yükümlülüklerini yerine getirmeleri gerekmektedir. Ayrıca ek bir bilgi olarak, AB'ye üyelik müzakerelerinde ise kişisel verilerin korunmasına ilişkin düzenlemeler, 23.fasıl olan "Yargı ve Temel Haklar" fasılı altına girmektedir.[258]

---

[255] GDPR Dibace 5. paragraf.
[256] GDPR 3. madde.
[257] KVKK Asistan https://www.kvkkasistan.com/Haberler/turkiye%E2%80%99de-kurulu-sirketlerin-gdpr-uyum-sorumlulugu/79 Erişim Tarihi 03.01.2024.
[258] Katılım Sürecinde Müzakere Fasılları (AB Başkanlığı) https://www.ab.gov.tr/files/rehber/07_rehber.pdf Erişim Tarihi 03.01.2024.

GDPR'ın sınır aşırı etkisinin veri ihlali bildirimine yansıması da şu şekilde olmuştur; örneğin Türkiye'de bulunan ancak AB'deki bireylere hizmet sağlayan bir hastane veya güzellik merkezi olduğunu varsayalım. Bu kuruluş, yaptığı iş gereği AB'deki bireylere dair hassas kişisel veri sayılacak olan tıbbi kişisel verilere sahip olacaktır ve bunların işlemesini gerçekleştirecektir. İşte bu noktada GDPR'ın sınır aşırı etkisi devreye girmektedir. Artık bu ilgili kuruluş, AB'deki bireylerin kişisel verilerini işlerken GDPR hükümlerine uyum sağlamakla yükümlüdür. Bir veri ihlali yaşadığında ise ihlale göre denetim makamına ve veri öznelerine veri ihlali bildirimi yapmak zorundadır. Veri ihlal bildiriminin ise önceden değinilen gerekli unsurları içerecek şekilde yapılması gerekmektedir.

6.2. Türk Hukukunda Kişisel Verilerin Korunması ve Veri İhlali Bildirimi

Bu alt başlıkta Türk hukukundaki kişisel verilerin korunması kuralları ve veri ihlal bildirimine değinilecektir.

6.2.1. 6698 Sayılı Kişisel Verilerin Korunması Kanunu

Bu terim ile ülkemizde uygulanan 6698 sayılı Kişisel Verilerin Korunması Kanunu kastedilmektedir. "KVKK" şeklinde kısaltılmaktadır. Kişisel veri güvenliğine önem verilmediğine dair toplumdaki olumsuz algının değişmesi, veri işlemenin şartlarının belirlenmesi ve tek bir kanun ile düzenleme yapılması, veri işleme faaliyetinin güven içinde gerçekleştirilmesi ve AB üyeliği için veri güvenliğinin önem arz etmesi sebebiyle 2016 yılında KVKK yürürlüğe girmiştir.[259]

Kişisel Verileri Koruma Kanunu 24 Mart 2016 tarihinde kabul edilmiştir. Kişisel verilerin korunması ve kişisel veri işleyenlerin uyacakları usul ve esasları belirlemek

[259] Ural Uslan, Y., Değirmenci, S., **Avrupa Birliği Genel Veri Koruma Tüzüğü Işığında Türkiye'de Kişisel Verileri Koruma Kurumu**, Optimum Ekonomi Ve Yönetim Bilimleri Dergisi, Cilt 10, Sayı 1, 2023, s. 23-38. https://dergipark.org.tr/en/pub/optimum/issue/74376/1106817 , Erişim Tarihi 07.12.23.

amacıyla hareket edilmiştir.[260] 7 Nisan 2016 tarihinde Resmi Gazete'de yayımlanarak yürürlüğe girmiştir. Kişisel verilerin korunması alanında Türkiye'deki ilk kanundur. Bu kanun öncesinde sadece Türkiye Cumhuriyeti Anayasası'nda 2010 yılında eklenen bir fıkrada kişisel verilerin korunmasına ilişkin düzenleme yer almaktaydı. İlgili fıkrada her bireyin kişisel verilerinin korunması hakkına ve kendi isteği ve bilgisi dahilinde verilerinin işlenebilme hakkına sahip olduğuna, kişisel verilerin kanunla düzenleneceğine değinilmiştir.[261] Bu düzenleme "Özel Hayatın Gizliliği" başlığı altına yerleştirilmiştir. Daha sonra ise öncesinde belirtildiği üzere yeni bir kanun düzenlenerek bu alanda ayrıntılı çalışmalar yapılmıştır. KVKK, GDPR'a göre daha kısa bir düzenleme olarak karşımıza çıkmaktadır. GDPR 99 maddeden oluşurken KVKK 33 maddeden oluşmaktadır.

Kişisel verilerin korunmasında veri ihlalinde ele geçirilen verilerin hepsi önemli olmakla birlikte, bazı verilerin önemine vurgu yapılmak için özel nitelikli kişisel veriler olarak ayrıca sayılmıştır. Özel nitelikli kişisel veriler, hem GDPR hem de KVKK'da belirtilmiştir. Özel nitelikli kişisel veriler, KVKK'da "ırkı, etnik kökeni, siyasi düşüncesi, felsefi inancı, dini, mezhebi veya diğer inançları, kılık ve kıyafeti, dernek, vakıf ya da sendika üyeliği, sağlığı, cinsel hayatı, ceza mahkûmiyeti ve güvenlik tedbirleriyle ilgili verileri ile biyometrik ve genetik veriler"[262] olarak sayılmıştır. GDPR'da ise "Irk veya etnik köken, siyasi görüşler, dini veya felsefi inançlar ya da sendika üyeliğini açığa çıkaran kişisel veriler, genetik veriler ile biyometrik veriler, sağlık verileri, cinsel yaşam, cinsel eğilime ilişkin veriler"[263] özel nitelikli kişisel veri olarak düzenlenmiştir.

KVKK'da GDPR'dan farklı olarak mezhep ve kılık kıyafet gibi dış görünüş bilgileri de özel nitelikli kişisel veri sayılmıştır. Bu iki veri türü GDPR'da

[260] KVKK 1. madde
[261] Daha ayrıntılı bilgi için bakınız. T.C. Anayasası 20. madde 3. fıkra.
[262] KVKK 6. madde
[263] GDPR 9. madde.

düzenlenmemiştir. Ancak mezhep ile ilgili kişisel veriler ayrıca GDPR'da belirtilmemiş olsa da GDPR'daki dini veya felsefi inanç başlığı altında düşünülebilir. KVKK'nın Türkiye'de uygulanan bir kanun olduğu düşünüldüğünde bu gibi veri türlerinin de kişi için önemli olduğundan özel nitelikli veri olarak kabul edilmesi mantıklıdır. Örneğin mezhep açısından kişisel verileri usule aykırı şekilde ele geçirilip yayınlanan bir şahsın ayrımcılık gibi olumsuz uygulamalara maruz kalma ihtimali bulunmaktadır. Bu zararın gerçekleşme ihtimalinin azaltılması için "mezhep" ve "kılık kıyafet" kanunda ayrıca sayılmıştır.

GDPR ile KVKK'nın farklı bir noktası ise GDPR'da çocuklarla ilgili bazı maddelere yer verilirken KVKK'da ayrıca çocuklarla ilgili bir düzenleme bulunmamaktadır. GDPR'da veri ihlalinde çocukların bilgilerinin ehemmiyetine ayrıyeten dikkat çekilmiştir.

AB'de kişisel verilerin korunmasının önemine dikkat çekilmesi amacıyla bir kişisel veri koruma günü ilan edilmiştir. AB'de bu gün "*Data Protection Day"* olarak anılmaktadır. 28 Ocak'ta kutlanmaktadır. 28 Ocak olarak kutlanmasının sebebi ise ilk yasal olarak kişisel bilgilerin korunmasına yönelik sözleşme olan 108 sayılı sözleşmenin yıl dönümü olmasıdır. AB üye devletleri ve kuruluşları tarafından kutlanmaktadır.[264] Aynı gün, *"Data Privacy Day"* yani "Veri Gizliliği Günü" olarak da bilinmektedir. Türkiye'deki durumda ise, 2018 yılında Milli Eğitim Bakanlığı tarafından 7 Nisan Kişisel Verileri Koruma Günü ilan edilmiştir. Eğitim kurumlarındaki öğrenci kulüplerine dahil olarak da Kişisel Verileri Koruma Kulübü eklenmesi yönünde

[264] Daha ayrıntılı bilgi için bakınız. European Data Protection Supervisor https://www.edps.europa.eu/data-protection/our-work/publications/events/european-data-protection-day-0_en#:~:text=Protection%20Day%202025!-,28%20January%202025,protection%20of%20their%20personal%20data. Erişim Tarihi 12.03.2025.

karar kılınmıştır.[265] 7 Nisan gününün seçilmesinin nedeni ise 7 Nisan 2016 tarihinin KVKK'nın Resmi Gazete'de yayımlanma tarihi olmasıdır.

GDPR, önceden bahsedilen uygulama alanının geniş olması ve sadece AB üye devletleri değil, diğer ülkelerdeki kişisel veri işleme işlemlerinde de uygulanabilmesi sebebiyle Türkiye'de de etkili olmuştur. KVKK'nın da yürürlüğe girmesi ile bu alan giderek daha ciddiye alınır hale gelmiştir. KVKK'da GDPR ile paralel ilerleyen kısımlar da bulunmaktadır. Kişisel verileri işlemeden önce rıza alınması, veri güvenliği için yükümlülüklerin yerine getirilmesi, veri öznesinin veya veri sahibinin kendi kişisel verilerine ulaşması veya kişisel verilerinin yok edilmesini istemesi gibi hükümler KVKK'da da vardır.[266]

Türkiye'deki kişisel veriler alanındaki resmi kurum ise "Kişisel Verileri Koruma Kurumu"dur. Misyonlarını kendileri Anayasa'ya uygun şekilde özel hayatın gizliliği ve temel hak ve özgürlüklere uyarak kişisel verileri korumak, toplumu bilinçlendirmek ve veri kaynaklı uluslararası finansal alanda özel veya kamu kişilerinin yarışabilmesini sağlayabilecek bir ortam yaratmak olarak açıklamışlardır.[267] Kurucu hukuki belgeleri KVKK'dır. Bu kurucu belge, kişisel veri ihlaline ilişkin bir sonraki başlıkta belirtilecek düzenlemeleri içermektedir. Kişisel Verileri Koruma Kurumu, Avrupa Veri Koruma Kurulu'na koruma gayesi odaklı olmasıyla benzemektedir.

Bu bilgiler ışığında, GDPR ile KVKK'nın karşılaştırılması kısaca bir özet şeklinde aşağıdaki tabloda açıklanacaktır.

---

[265] Kişisel Verileri Koruma Kurumu https://www.kvkk.gov.tr/Icerik/5278/Milli-Egitim-Bakanligi-7-Nisan-Gununun-Kisisel-Verileri-Koruma-Gunu-Olarak-Kutlanmasi-Kararlastirilmistir#:~:text=Tarihi%3A%2002.09.2018-,Milli%20E%C4%9Fitim%20Bakanl%C4%B1%C4%9F%C4%B1%207%20Nisan%20G%C3%BCn%C3%BCn%C3%BCn%20%22Ki%C5%9Fisel,Koruma%20G%C3%BCn%C3%BC%22%20Olarak%20Kutlanmas%C4%B1n%C4%B1%20Kararla%C5%9Ft%C4%B1rd%C4%B1 Erişim Tarihi 12.03.2025.

[266] Daha ayrıntılı bilgi için bakınız. Doxagon Blog https://www.doxagon.com/blog/gdpr-kvkk/#:~:text=GDPR%2C%20AB'de%20ya%C5%9Fayan%20bireylerin,dan%20daha%20kapsaml%C4%B1%20bir%20yasad%C4%B1r. Erişim Tarihi 10.03.2025.

[267] Kişisel Verileri Koruma Kurumu https://www.kvkk.gov.tr/Icerik/2074/Misyon---Vizyon Erişim Tarihi 11.03.2025.

Tablo 1: GDPR ile KVKK'nın Özet Olarak Karşılaştırılması.

GDPR	KVKK
Küresel uygulanma alanına sahiptir. (AB'dekilerin verileri işleniyorsa.)	Türkiye öncelikli uygulanma alanıdır.
Veri öznelerin hakları daha kapsamlıdır.	Veri özneleri hakları daha sınırlıdır.
Veri koruma görevlisinin zorunlu olduğu haller bulunmaktadır.	Veri koruma görevlisi zorunlu değildir.
Veri ihlali bildirimi 72 saat içinde yapılmalıdır.	Veri ihlali bildirimi hızlı yapılmalıdır.
En yüksek idari para cezası sınırı 20 Milyon € veya küresel cironun %4'ü'dür.	En yüksek idari para ceza sınırı 1 Milyon Türk lirasıdır.
Özel nitelikli kişisel veriler sayılmıştır.	Özel nitelikli kişisel veriler sayılmıştır ancak bunlara ek olarak mezhep ve kılık kıyafet de eklenmiştir.
Çocuklara ilişkin düzenlemeler bulunmaktadır.	Çocuklara ilişkin ayrıca düzenlemeler yoktur.

6.2.2. Türk Hukukunda Veri İhlali Bildirimi

KVKK'da kişisel veri ihlali bildirimi veri güvenliği maddesi altında düzenlenmiştir. KVKK'nın 12. maddesi uyarınca işlenen veriler kanuna aykırı ele geçirildiği halde veri sorumlusu bu durumu ilgilisine veya Kurul'a bildirmelidir ve gerekirse internet sitesinde veya başka bir şekilde bunu duyurmalıdır.[268] Burada veri sorumlusuna en kısa sürede bildirme yükümlülüğü verilmiştir. Veri sorumlusu ve veri

[268] KVKK 12. madde 5.fıkra

işleyen edindikleri kişisel verileri görevlerine devam ettikleri sürece ve görevleri bittikten sonra da kimseyle paylaşmama yükümlülüğü altındadırlar.[269] Edindikleri bilgiler önemli kişisel veriler olduğundan ilgili işleme faaliyetleri bittikten sonra da bu sorumluluk devam etmektedir. Hak kaybı, olumsuzluklar yaşanmaması için bu düzenleme yerinde olmuştur. Örneğin Türkiye'de gerçekleşen bir veri ihlali, AB vatandaşlarının verilerinin işlenmesinde gerçekleştiyse bu veri ihlalinde GDPR hükümlerine göre aksiyon alınması gerekmektedir. AB'ye bildirilir ve öncesinde değinildiği üzere GDPR uygulanır.

GDPR'daki kişisel veri ihlali üzerine verilecek idari para cezaları uygulaması, KVKK'da da karşımıza çıkmaktadır. "Suçlar ve Kabahatler" başlığı altında düzenlenen para cezaları sebebine göre değişerek 5.000 Türk lirasından başlayarak 1.000.000 Türk lirasına kadar çıkabilmektedir.[270] Kişisel veri ihlali bildiriminden KVKK'de "veri güvenliğine ilişkin yükümlülükler" başlığı altında bahsedilmekteydi. Veri güvenliğine ilişkin idari para cezası ise 15.000 Türk lirasından 1.000.000 Türk Lirası'na kadar belirlenmiştir.[271] Kişisel veri güvenliği ile ilgili yükümlülüklere uymayanlara uygulanmaktadır. Türkiye'deki ilgili konuya ilişkin durum bu şekildedir.

Belirtmek gerekir ki GDPR, KVKK'dan çok daha detaylı ve geniş kapsamlı bir düzenlemedir. GDPR, kişisel verilerin korunması alanındaki düzenlemeler içinde oldukça sıkı kurallara sahip bir düzenleme olarak görülmektedir. Örneğin GDPR para cezaları, KVKK'ya kıyasla, miktarlarına yukarıda değinildiği üzere çok daha yüksek meblağlar olabilmektedir. Ayrıca GDPR'da hükümlere göre verilen idari para cezası en yüksek sınır hangisi ise o sınırdan verilmektedir.

Uygulamada bu durum KVKK'ya göre GDPR'ın daha caydırıcı bir yaklaşım göstermesine sebep olmaktadır. GDPR'ın daha sıkı kurallara sahip olmasında, AB'de

[269] KVKK 12. madde 4. fıkra
[270] KVKK 12. madde.
[271] KVKK 18. madde, (b) fıkrası.

bu alanda önceden bahsedilen eski düzenlemelerin zaman içinde değişip gelişerek GDPR'ı ortaya çıkarmasının payı vardır. Eski bir geçmişe sahip olan GDPR'ın daha detaylı düşünülmüş olmasının sebebi budur. Türkiye'de ise 2010 yılından sonra yeni yeni bu alanda adımlar atılmaya başlanmıştır. Türkiye'nin bu alandaki güncel durumu, AB'nin yaşadığı süreç gibi bir gelişme sürecinde olması olarak yorumlanabilir. KVKK'nın da hızla gelişen teknolojinin getirdiği gerekliliklere göre zaman içinde uyum sağlayacak şekilde düzenlemeler içereceği söylenebilmektedir.

Türkiye'de, AB'de bulunmayan, büyük bir veri deposu olarak görülebilecek e-Devlet sistemi bulunmaktadır. e-Devlet sisteminde, Türkiye'de yaşayan nüfusa kayıtlı olan tüm vatandaşların isim, telefon, adres, borç, dava, okul, iş, medeni durumu, adına açılan icra takipleri, iş başvurusu yaptığı kadro bilgileri, sağlık bilgileri, hastane kayıtları, ilaç reçeteleri veya raporları gibi geniş bir yelpazedeki bilgileri bulunmaktadır. Bu bilgilerin yanlış ellere geçmesi felaketvari sonuçlara yol açabilir. Bu bilgileri ele geçiren kötü niyetli şahıslar kendi kullanımı için olmasa bile istekli alıcılarına bu bilgileri ücreti karşılığında satıp kazanç elde etme yoluna girebilirler.

Durumu somutlaştırmak üzere tamamen varsayımsal bir örnekten bahsedelim; kadın sığınma evlerinde kalan ve eski eşinden şiddet görme ihtimali ile saklanan bir kadın olduğunu düşünelim. Bu veri ihlali gerçekleşmiş olsaydı ve bu verileri pazarlayan kötü niyetli şahıslar bulunsaydı, söz konusu eski eş, kadının saklandığı yerin adresine ulaşıp onun can güvenliğini tehlikeye atacak eylemlerde bulunabilirdi. Görülmektedir ki bir veri ihlali her zaman sadece bir veri ihlali olmamaktadır. Domino taşları gibi birbirini takip eden olaylar silsilesine dönüşüp olumsuz sonuçlara yol açma ihtimali bulunmaktadır. İlgili devlet kurumları, bu ihtimalleri göz önünde bulundurarak düzenlemeler yapmalı ve önlemler almalıdır.

Kişisel Verileri Koruma Kurumu, GDPR'a uyum sürecine dikkat vermektedir ve katkıda bulunmaktadır. GDPR, bir temel kılavuz olarak görülmektedir. Kişisel Verileri Koruma Kurumu'nun "Kişisel Veri İhlali Bildirim Usul Ve Esaslarına İlişkin Kişisel Verileri Koruma Kurulunun 24.01.2019 Tarih Ve 2019/10 Sayılı Kararına İlişkin Duyuru"su bu duruma örnek teşkil etmektedir. Kişisel Verileri Koruma Kanunu'nun 12. maddesinde veri ihlali bildirimine ilişkin veri sorumlusunun "en kısa sürede" ilgili bildirimi Kurul'a bildireceğinden bahsedilmişti. "En kısa sürede" ifadesinin artık GDPR'daki 72 saat olarak yorumlanması gerektiği ve aynı GDPR'daki gibi 72 saati geçmesi durumunda gecikme nedenlerinden de bahsedilmesi gerektiği belirtilmiştir.[272] Görüldüğü üzere Kişisel Verilerin Korunması Kanun maddelerinin yorumlanmasında GDPR hükümleri öncülük eder durumdadır.

Görüldüğü üzere birbirine yakın coğrafyalar olan AB ve Türkiye, kişisel veriler alanında da birbirinden etkilenmişlerdir. Türkiye, kişisel veriler alanında AB'ye göre henüz yolun başında bir pozisyondadır. Bunun nedeni ise yukarıda bahsedildiği üzere Türkiye'deki kanun düzenlemelerinin AB'ye göre çok daha sonra yapılmış olmasıdır. GDPR örnek alınarak gerektiğinde Kişisel Verileri Koruma Kanunu'nda yeni düzenlemeler yapılabileceği aşikârdır. Uyum sağlayarak yapılan düzenlemeler, kanunun gerçek hayata uygulanmasında da yardımcı olacaktır. Türkiye'deki kişisel verilerin korunması alanı yüzü geleceğe dönük bir alan olarak yoluna devam edecektir. Bunun sebebi ise zamanla gelişen teknolojinin kişisel verilerin korunması hukuku alanında yeni düzenlemeler yapılmasını gerektirecek olmasıdır.

[272] 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 11.03.2025.

SONUÇ

Bu çalışmada "Veri ihlali nedir?" sorusu temel konu seçilmiştir ve kişisel veri ihlali bildirimleri incelenmiştir. Kişisel veri ihlali bildirimi, daha önce örneklendirilen veri ihlali ve sonrasında gelişen olaylarda elzem rol oynaması sebebiyle odak noktası olmuştur. Kişisel veri ihlali bildirimi, içinde bulunduğu düzenleme olan GDPR'ın ve GDPR'ın ilkelerinin ve kavramlarının açıklanmasıyla, onun önemli örnekleriyle, uygulanma alanıyla işlenmeye başlamıştır. Daha sonra kişisel veri ihlali bildiriminin tanımı, denetim makamına ve veri sahibine yapılması, yaptırımları, veri ihlali bildiriminin önemi, ilgili yargı kararları, KVKK'daki yeri ele alınmıştır.

Kişisel verilerin korunması, bir alan olarak yenidir. Bu alan hukuk, bilişim teknolojileri, ticaret gibi farklı alanlarla etkileşim içindedir. Birbirinden farklı olan bu alanların kişisel verilerin korunması ile ilgili hale gelmesi, kişisel verilerin korunması alanının giderek kapsamının genişlediğini göstermektedir. Kişisel verilerin korunması hukuku, diğer hukuk alanlarına göre (örneğin ceza hukuku gibi) daha yeni bir oluşumdur. Kişisel verilerin korunması alanı, sadece hukuk alanını değil, kişisel verileri dijital ortamda verilerin güvenliğini sağlayacak bilgisayar programlarının var olmasını sağlayan bilişim alanını da yakından ilgilendirmektedir. Veri güvenliğinin sağlanması için bu programların varlığı gereklidir. İşlenecek verilerin niteliklerine göre gerekli önlemlerin alınması gereklidir.

Kişisel veri kavramını bu kadar önemli hale getiren nokta, var olan verinin bir şahsa ait olmasıdır. Herkes tarafından bilinen bir verinin aynı değeri taşıdığı söylenemez çünkü zaten herkesin o veriye erişimi bulunmaktadır. Toplum genelinde bilinen veri haline gelmiş bulunmaktadır. Kişisel verinin tek başına değerli olması dışında bu veri bir gerçek kişiyle ilişkilendirebildiği durumlarda veri daha da değerli hale gelmektedir. Bu anlayışın en derinine, kökenine inildiğinde birey kavramının

önemiyle karşılaşılmaktadır. Bir bireyi birey yapan nedir? O bireyin bir insan olması ona gerekli değerin atfedilmesini sağlamaktadır. Bir birey salt insan olduğu için bile temel bir saygıyı hak etmektedir. İnsan haklarına saygılı hukuk anlayışına sahip devletlerde bireyin varlığına, onun varoluşunun hukuk sistemine yansıması olan birey kavramına itimat edilmektedir. Bireye duyulan saygıdan dolayı birey ile ilgili olan, bireyin bir parçası veya uzantısı olan şeylere de saygı duyulup önem verilmektedir. Bireye ait bilgiler ise günümüzde kişisel veri kavramı ile karşılık bulmaktadır. Bu sebeptendir ki veriyi değerli hale getiren unsurun verinin bireye ait olması şeklinde karşımıza çıktığı görülmektedir. Kişisel veriye de bu nedenle önem verilip saygı duyulmaktadır çünkü kişisel veri insana aittir. Örneğin bir makinenin özelliklerine ait bilgiler kişisel veri olarak sayılamamaktadır. İnsana ait özellikler içinse aynı şey söylenememektedir. İnsana saygı duyulmaktadır. Kişisel veriye de insana ait olması sebebiyle saygı duyulmaktadır. Bu anlayış, insana ve insandan gelene duyulan saygı ve verilen değer olarak açıklanabilmektedir.

Bu anlayış doğrultusunda, durmadan gelişen teknoloji sayesinde kişisel veri kavramının önemi giderek artmıştır ve bu konuda düzenlemeler yapılmaya başlanmıştır. Önceden bahsedildiği üzere, AB'de kişisel veri alanında ilk çalışmaların 80'li yıllarda yapıldığı görülmektedir. 80'li yıllardan günümüze kişisel verilere ilişkin hukuki düzenlemeler değişerek en son GDPR'daki halini almıştır. Türkiye'de ise 2010 yılında ilk defa T.C. Anayasası'na bir maddenin fıkrasında düzenlenen kişisel verilerin, takvimler 2016 yılını gösterdiğinde kendi alanına ait bir kanuna yani KVKK'ya sahip olduğu görülmektedir. Ayrıca bu kanunla ilişkili olarak Kişisel Verileri Koruma Kurumu adlı resmi bir kuruluşun da açıldığı görülmektedir.

Kişisel verinin öneminin dünya genelinde artık daha açık ve net anlaşılması öngörülen bir durumdur. Bu verilerin işlenmesinde ise önce koruyabilecek yeterli güvenliğe sahip olunması gerekmektedir. Bir veri ihlali yaşanmasını beklemek yerine

veri işleme faaliyetine başlanmadan önce veri güvenliğini sağlayacak gerekli sisteme sahip olunup olunmadığı kontrol edilmelidir. Böyle bir güvenlik sistemi bulunmuyor ise de kurulması gerekmektedir. GDPR, veri güvenliği sağlanmasını ve veri ihlallerini oldukça ciddiye almaktadır. Veri ihlallerine verilen ehemmiyetin bu hükümler ile somutlaştığı görülmektedir. GDPR merkezinde şekillenen bu çalışma, veri ihlal bildirimleri odaklı hazırlanmıştır.

Veri ihlal bildirimlerinin, olası bir ihlal durumunda ihlalin neden olacağı zararı en aza indirebilecek işleve sahip olabileceği göz önünde bulundurulmaktadır. Veri ihlal bildirimi yapılırken veri öznesine veya veri sahibine yapılan bilgilendirmeler ve hatta uyarılar ile ihlalin etkisi kontrol altında tutulabilmektedir ancak bu tüm veri ihlalleri için geçerli olamamaktadır. Örneğin büyük veri deposu haline gelen ve bulunduğu ülkedeki her vatandaşla ilgili kritik bilgilere sahip bir platform olduğunu düşünelim. Bu platformdaki kişisel veriler vatandaşların hayatlarının tüm kayıtlarını içermektedir. Bu büyüklükteki bir veri deposunun veri ihlaline uygulaması halinde gerekli veri ihlal bildirimi olabilecek en kısa sürede yapılıp ihlalin önemine ilişkin bilgilendirmeler yapılsa bile sonuçlarını hafifletmenin mümkün olmayabileceği ihtimali de her zaman göz önünde bulundurulmalıdır.

Veri ihlali olumsuz sonuçlara yol açabilecek bir durum olarak görülmektedir. Bunun sebebinin ise verilerin içeriğinin kötü niyetli ellerde veri öznelerine veya veri sahiplerine karşı bir silah niteliğinde kullanılabilecek bilgiler içermesi olduğu söylenebilmektedir. Bu tabirle anlatılmak istenen ilk başta çok da önemli olmayan bir veri ihlalinin tekrarladıkça veya ilerledikçe önemli sonuçlara yol açabileceğidir. Veri ihlalleri tehlike arz etmektedir çünkü bulunan, depolanan, işlenen veri öznelerine veya veri sahiplerine ait veriler, sadece isim, adres, telefon gibi veriler değil ayrıca o veri öznesinin veya veri sahibinin ilgi alanları, siyasi görüşü, toplumsal meselelere bakışı, alışveriş alışkanlıkları gibi verilerdir. Bu verilerin bu kadar önem taşımasının sebebi ise

ilgili verilerin artık veri sahibi veya veri öznesi kişinin düşünce yapısını özetler hale gelmiş olmalarıdır. Hatta tekrarlı şekilde taraflı reklamlarla veya taraflı gönderiler ile kişinin seçimlerde kullanacağı oya bile etki edilebilmektedir. Toplumsal bir olaya karşı kişinin takınacağı tavır tahmin edilebilir veya yönlendirilebilir duruma gelmiştir. Bunu amaçlayan kişiler tarafından abartılı bir tabirle bir zihin kontrol aracı gibi kullanılma ihtimali doğmaktadır.

Çalışmada açıklandığı üzere veri ihlalleri ciddi olumsuzluklara sebep olabilmektedir. Bu nedenle veri ihlal bildirimi, kişisel verilerin korunmasının önemli bir unsurudur. Veri ihlalinin getirdiği en büyük tehlikelerden birisinin, çalışmanın Kişisel Veri İhlaline ve GDPR'a İlişkin Güncel Tartışmalar başlığında bahsedilen seçim örneğinde de görüldüğü üzere toplumların kaderinin değiştirilebilme ve ihlalden sorumlu olan kişinin istediği şekilde yönlendirilebilme tehlikesi veya ihtimali olduğu görülmektedir.

Bu duruma başka bir örnek ise sosyal medyada kadın erkek ayrımı yapılarak yorumlanabilme ihtimali olan bir gönderide kullanıcının bilgilerine göre farklı görüşlerdeki yorumların gösterilmesidir. Cinsiyet bilgilerine göre kadınlara kadınları savunan yorumları, erkeklere erkekleri savunan yorumları öne çıkarıp göstermektedir. Bireylere kendi görüşüyle aynı yorumları gösterip farklı görüşte olan yorumları öne çıkarmayarak toplumdaki bireyler kutuplaşmaya sürüklenmektedir. Tabiri caizse kişinin kendi at gözlüğünün dışını görememesi sonucu "farklı" olana tahammülün azalması ve şiddet türlerinin açığa çıkması ihtimalinin artması ile karşı karşıya kalınmaktadır. Bu işleyişin ise gelecekte daha büyük toplumsal problemlere yol açabileceği öngörülmektedir.

Bu incelenen konular sonucunda kişisel veri ihlali bildiriminin zaman ve içerik açısından geliştirilebileceğine ulaşılmıştır. GDPR'da veri ihlali bildiriminin yapılması için verilen sürelerin, veri ihlalinin büyük olması durumunda 72 saat sınırının daha kısa

süreye çekilmesinin pozitif etki yaratacağı ortaya çıkmıştır. İçerik açısından ise veri ihlali bildiriminin içerdiği bilgilerin daha açıklayıcı olması için artırılması ancak kısa ve öz biçimde açıklanması gerektiği kanısına varılmıştır.

Öneri ve geleceğe yönelik tahmin olarak, yukarıda bahsedilen örnekten ilerlersek, Türkiye'de e-Devlet gibi bir platform varken herkesin neredeyse tüm bilgilerinin kayıtlı olduğu bu verilerin kıymetinin ve ihlal bildirimlerinin ehemmiyetinin açık ve bariz ortada olduğu görülmektedir. Türkiye açısından fiziksel bir tehdit olmamasına rağmen adeta bir milli güvenlik, siber güvenlik meselesidir. İşte bu sebeple bile veri ihlal bildirimi zamanında yapılmalıdır. Varılan sonuca göre, önceden değinilen 72 saat kuralı örneğinde düşünürsek, veri ihlali yaşandığının bildirimi daha erken ulaştırılabiliyorsa, bildirimin daha erken yapılmasının yararlı olacağı görülmektedir. Etkili bildirim yapmak önemlidir çünkü veri ihlali bildiriminde, yaşanan ihlal hakkında gerekli bilgilerin verilerek ihlalin mahiyeti anlaşılmaktadır. Böyle etkili bildirimlerde veri öznesi veya veri sahibi kendi çapında daha dikkatli davranmaktadır. Sonuç olarak veri ihlalinin getirebileceği negatif çıktılara karşı veri öznesi ya da veri sahibi habersiz kalmamaktadır başka bir deyişle gözü açık olmaktadır.

Tüm bu durumlar göz önünde bulundurulduğunda, bireylerin hukuka ve kanun koyuculara olan güvenlerine istinaden her alanda olduğu gibi veri ihlallerinin bildirimlerinde de bireylerin kimliklerinin manipüle edilmesine ihtimal vermeyecek ve vatandaşların gizliliklerine saygı gösteren düzenlemelerin yapılmasının, herkes için doğru olacağı görülmektedir. Bireylerin kişisel verileri değerlidir ve veri ihlallerine karşı korunmalıdır. Bu durum hem Türkiye'de hem de AB'de yaşayan bireyler için geçerlidir.

KAYNAKÇA

KİTAPLAR

1) Bakırel, N. B., **Veri Sorumlusu Ve Veri İşleyen Arasındaki Sorumluluk Paylaşımı Avrupa Birliği Genel Veri Koruma Tüzüğü Ve Kişisel Verilerin Korunması Kanunu Çerçevesinde Değerlendirilmesi,** Seçkin, 2021.
2) Balaban, M.F., **Elektronik Haberleşme Sektöründe İşlenen Kişisel Verilerin Korunması,** Adalet, 2023.
3) Çağlayan R., Koca, M., Saka, R., **Avrupa Birliği Hukuku, İdare Hukuku Ve Ceza Hukuku Açısından Kişisel Verilerin İmhası**, 2022.
4) Çelikel, S., **Kişisel Verilerin Korunması Hukuku Kapsamında Veri Sorumlusu Ve Veri Sorumlusunun Yükümlülükleri,** Seçkin, 2022.
5) Erdoğmuş, E., **6698 Sayılı Kişisel Verilerin Korunması Kanunu Kapsamında Açık Rıza,** Seçkin, 2022.
6) Giakoumopoulos, C., Buttarelli G., O'Flaherty, M., **Handbook on European Data Protection Law**, Publications Office of the European Union, Luxembourg, 2018.
7) Göçmen Uyarer, S., **Kişisel Verilerin Korunması Kanunu Ve Türk Ceza Kanunu Kapsamında Kişisel Verilerin Korunması,** Seçkin, 2020.
8) Günay, B., **Kişiliğin Korunması Kapsamında Kişisel Verilerin Hukuka Aykırı Kullanılması Nedeniyle Hukuki Sorumluluk,** Seçkin, 2023.
9) Korkmaz, İ., **Kişisel Verilerin Ceza Hukuku Kapsamında Korunması**, Seçkin, 2019.
10) Taşçı Aydemir, E**., Kişisel Verilerin Kaydedilmesi Suçu,** Seçkin, 2022.
11) Tepe, E., **Kişisel Verilerin Korunması,** Adalet, 2021.
12) Voigt, P., von dem Bussche, A., **The EU General Data Protection Regulation (GDPR),** Springer, 2017.
13) Yılmaz, T., **Avrupa Birliğinde Kişisel Verilerin Korunması Hukuku,** Adalet, 2022.

MAKALELER

1) Alsenoy, B.V., **Reconciling The (Extra)Territorial Reach Of The GDPR With Public International Law**, Gert Vermeulen- Eva Lieve (Ed.), Data Protection And Privacy Under Pressure Transatlantic Tensions, EU Surveillance, And Big Data, 2017, s. 77-100. https://kuleuven.limo.libis.be/discovery/fulldisplay?docid=lirias1711958&context=SearchWebhook&vid=32KUL_KUL:Lirias&search_scope=lirias_profile&adaptor=SearchWebhook&tab=LIRIAS&query=any,contains,LIRIAS1711958&offset=0&lang=en , Erişim Tarihi 20.03.24.
2) Alunge, R., **Breach of security vs personal data breach: effect on eu data subject notification requirements**. International Data Privacy Law, 11(2), 2021, s.163-181.
3) Azzi, A., **The challenges faced by the extraterritorial scope of the general data protection regulation**, Journal of Intellectual Property, Information Technology and Electronic Commerce Law, 9(2), 2018, s. 126-137.
4) Bârsan, M.-M., **A Partial Overview of the Data Subjects' Control over Their Personal Data under the General Data Protection Regulation,** Bulletin of the Transilvania University of Brasov, Series VII: Social Sciences & Law, 11 (60)(2), 2018, s.129–134.
5) Bendiek, A., Römer, M., **Externalizing Europe: the global effects of European data protection. Digital Policy, Regulation and Governance,** 21(1), 2019, s. 32-43.
6) Boban, M., **GDPR and Data Protection Impact Assessment (DPIA),** Economic and Social Development, International Scientific Conference on Economic and Social Development, 61, 2020, s. 215-223.
7) Clifford, D., Ausloos, J., **Data protection and the role of fairness**, Yearbook of European Law, 37, 2018, s. 130-187.
8) Çimen Bulut, İ., **Avrupa Birliği Genel Veri Koruma Tüzüğü Kapsamında Getirilen Yeni Teknik ve Yaptırım Mekanizmaları**, Anadolu Üniversitesi Sosyal Bilimler Dergisi, Cilt 20, Sayı 2, 2020, s. 127-142. https://dergipark.org.tr/en/pub/ausbd/article/758041 , Erişim Tarihi 09.12.23.
9) Dal, U., **Avrupa Birliği Genel Veri Koruma Tüzüğü'nün ülke dışı uygulama yetkisi ve bu yetkinin uluslararası hukukta meşruiyeti**, Kişisel

Verileri Koruma Dergisi, Cilt 1, Sayı 1, 2019, s. 21-33. https://dergipark.org.tr/en/pub/kvkd/issue/45759/553880 Erişim Tarihi 12.12.23.

10) De Hert P., Czerniawski M., **Expanding the European data protection scope beyond territory: Article 3 of the General Data Protection Regulation in its wider context**, International Data Privacy Law, Cilt 6, Sayı 3, 2016, s. 230–243.

11) Dilsiz, V., **Dijital Dünyada Kişisel Veri Kavramı ve KVKK/GDPR Kapsamında Bir Değerlendirme**, 2021. s.5

12) Drechsler, L.,**Individual Rights in International Personal Data Transfers Under the General Data Protection Regulation. Review of European Administrative Law,** Cilt 16, Sayı 1, 2023, s. 35–56. https://doi.org/10.7590/187479823X16800083010347

13) Dülger, M. V., **Avrupa Birliği Genel Veri Koruma Tüzüğü Bağlamında Kişisel Verilerin Korunması**, Yaşar Hukuk Dergisi, Cilt 1, Sayı 2, 2019, s. 71-174. https://dergipark.org.tr/en/pub/yhd/issue/52537/807628, Erişim Tarihi 07.12.23.

14) Dülger, M. V., **Kişisel Verileri Koruma Kurulunun "Kurula Şikâyette Bulunma Süresi" ile "Veri İhlali Bildirimi"ne İlişkin Kamuoyu Duyuruları Hakkında Değerlendirme,** 2021.

15) Dülger, M. V**., Veri İhlali Bildiriminde Bulunması Gereken Unsurlar ve Bildirim Esas ve Usulleri: KVK Kurulu'nun 18 Eylül 2019 Tarihli, 2019/271 Sayılı ve 24 Ocak 2019 Tarihli, 2019/10 Sayılı Kararlarının Değerlendirilmesi,** 2021.

16) Green, D., **Strategic Indeterminacy and Online Privacy Policies: (Un)informed Consent and the General Data Protection Regulation**, Int J Semiot Law 38, 2025, s.701–729. https://doi.org/10.1007/s11196-024-10132-4

17) Guida, S., **The European Data Protection Board's Position on the Processing of Personal Data In The Context Of Covid-19**, European Data Protection Law Review (EDPL), 6(2), 2020, s. 262-264.

18) Hahn, I., **Purpose limitation in the time of data power: is there way forward?**, European Data Protection Law Review (EDPL), 7(1), 2021, s. 31-44.

19) Hajduk, P., **The Powers of the Supervisory Body in the Gdpr as a Basis for Shaping the Practices of Personal Data Processing**, Review of European & Comparative Law, 45(2), 2021, s.57–75. https://doi.org/10.31743/recl.10733

20) Kuner, C., **Territorial Scope and Data Transfer Rules in the GDPR: Realising the EU's Ambition of Borderless Data Protection,** Legal Studies Research Paper Series University of Cambridge Faculty of Law, Paper No. 20/2021, April 2021, s.16. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3827850 Erişim Tarihi 19.08.2024.

21) Kuner, C., Bygrave, L., Docksey, C., Drechsler, L., **The EU general data protection regulation: a commentary**, 2020, Update of Selected Articles (May 4, 2021), s.238.

22) Mansfield-Devine, S., **Meeting the needs of GDPR with encryption. Computer Fraud & Security**, 2017(9), s.18. https://www.sciencedirect.com/science/article/abs/pii/S1361372317301008 Erişim Tarihi 06.03.2025.

23) Mehta, B., Sau, S., Patel, D., Rai, A., Das, B., Takidar, S. K., **Transparency through the lens of data protection and privacy: A clinical research organisation medical writing perspective**, Medical Writing, Cilt 33, Sayı 4, 2024, s. 64–67. https://doi.org/10.56012/vmom7031

24) Mustert, L., Santos, C., **The European Data Protection Board-a (non) consensual and (un) accountable role?**, 2024, s.33.

25) Neuman, K. L., Kavanagh, P., Balbirnie, D., White, M., **Schrems II: European Data Protection Board Data Transfers Guidance**, Intellectual Property & Technology Law Journal, 33(3), 2021, s. 18–22.

26) Oğuz, S., **Kişisel Verilerin Korunması Hukukunun Genel İlkeleri,** Bilgi Ekonomisi Ve Yönetimi Dergisi, Cilt 13, Sayı 2, 2018, s.121-138. https://dergipark.org.tr/en/pub/beyder/issue/41709/425303 Erişim Tarihi 12.12.23

27) Övündür, F., **Dijital Tek Pazar Stratejisinin Hukuki Bağlamında Kişisel Veri Güvenliğinin Sağlanması**, İstanbul Ticaret Üniversitesi Sosyal Bilimler Dergisi, Sayı 38, 2020, s.118-131. https://dergipark.org.tr/en/pub/iticusbe/issue/57051/780007 Erişim Tarihi 04.04.2025.

28) Rossi, A., **How the Snowden revelations saved the EU general data protection regulation**, The International Spectator, 53(4), 2018, s. 95-111.

29) Russo, A., Lax, G., Dromard, B., **A System to Access Online Services with Minimal Personal Information Disclosure**, Inf Syst Front 24, 2022, s. 1563–1575. https://doi.org/10.1007/s10796-021-10150-8

30) Ryngaert C, Taylor M., **The GDPR as Global Data Protection Regulation?** American Journal of International Law Unbound, Cambridge University Press, Cilt 114, 2020, s.5-9. https://www.cambridge.org/core/journals/american-journal-of-international-law/article/gdpr-as-global-data-protection-regulation/CB416FF11457C21B02C0D1DA7BE8E688 Erişim Tarihi 26.08.2024.

31) Saygın, D., Yılmaz, Y. E., **C-131/12- Google İspanya v. AEPD Davası ve 2014/19685 Numaralı C.K. Anayasa Mahkemesi Bireysel Başvurusu Kapsamında Avrupa Birliği Hukukunda Unutulma Hakkı ve Türk Hukuk Sistemine Yansıması**, Anadolu Üniversitesi Sosyal Bilimler Dergisi, 23(3), 2023, s. 685-700. https://doi.org/10.18037/ausbd.1257429 Erişim Tarihi 07.03.2025

32) Schmitz-Berndt, S., **Edpb adopts updated guidelines on personal data breach notification under gdpr: the end of the one-stop-shop reporting mechanism for non-eu establishments**, European Data Protection Law Review (EDPL), 8(4), 2022, s.517-520.

33) Seçkin, A. Z., **Türk Kişisel Verileri Koruma Mevzuatının Avrupa Birliği Genel Veri Koruma Tüzüğü İle Uyumlaştırılması Sürecinde Doğabilecek Sorunlar Ve Bu Sorunlara Yönelik Çözüm Önerileri,** Yeditepe Üniversitesi Akademik Açık Arşiv. https://openaccess.yeditepe.edu.tr/yayinaea/Ayca%20Zanbaklar%20Se%C3%A7kin_Preprint_653903412ac2e.pdf Erişim Tarihi 12.12.23.

34) Selek, O., **Genel Veri Koruma Tüzüğü Işığında Kişisel Verilerin İşlenmesinde Rıza Açıklaması**, Dokuz Eylül Üniversitesi Hukuk Fakültesi Dergisi Cilt 21, Sayı 2, 2019, s. 911-951. https://dergipark.org.tr/tr/pub/deuhfd/issue/51788/646330 , Erişim Tarihi 07.12.23.

35) Sevindi N. S., Ordu., M. E., **AB ve Türk Hukukunda Veri İhlalinin Tespiti ve Bildirim Süresinin Karşılaştırmalı Değerlendirmesi**, Kişisel

Verileri Koruma Dergisi, Cilt 5, Sayı 1, 2023, s.12-22. Erişim Tarihi 07.12.23.

36) Soysal, T., **Unutulma Hakkının Avrupa Birliği'nin Genel Veri Koruma Tüzüğü Çerçevesinde İncelenmesi**, Uyuşmazlık Mahkemesi Dergisi, Sayı 13, 2019, s. 339-422. https://dergipark.org.tr/tr/pub/mdergi/issue/45986/581902, Erişim Tarihi 07.12.23.

37) Spindler, G., Schmechel, P., **Personal data and encryption in the european general data protection regulation. Journal of Intellectual Property, Information Technology and Electronic Commerce Law**, 2016, 7(2), s. 163. https://heinonline.org/HOL/Page?collection=journals&handle=hein.journals/jipitec7&id=174&men_tab=srchresults Erişim Tarihi 06.03.2025.

38) Tikkinen-Piri, C., Rohunen, A., Markkula, J., **EU General Data Protection Regulation: Changes and implications for personal data collecting companies. Computer Law & Security Review**, 34(1), 2018, s.134-153. https://www.sciencedirect.com/science/article/pii/S0267364917301966 Erişim Tarihi 17.03.2025.

39) Uncular, S**., The right to removal in the time of post-google Spain: myth or reality under general data protection regulation?**, International Review of Law, Computers & Technology, 33(3), 2019, s. 309–329. https://doi.org/10.1080/13600869.2018.1533752

40) Ural Uslan, Y., Değirmenci, S., **Avrupa Birliği Genel Veri Koruma Tüzüğü Işığında Türkiye'de Kişisel Verileri Koruma Kurumu**, Optimum Ekonomi Ve Yönetim Bilimleri Dergisi, Cilt 10, Sayı 1, 2023, s. 23-38. https://dergipark.org.tr/en/pub/optimum/issue/74376/1106817 , Erişim Tarihi 07.12.23.

41) Utzerath, J., Dennis, R., **Numbers and statistics: data and cyber breaches under the General Data Protection Regulation**, Int. Cybersecur. Law Rev. 2, 2021, s. 339-348. https://doi.org/10.1365/s43439-021-00041-8

42) Vedder, A., Naudts, L., **Accountability for the use of algorithms in a big data environment**, International Review of Law, Computers & Technology, 31(2), 2017, s. 206–224. https://doi.org/10.1080/13600869.2017.1298547

43) Ward, A., **The Oldest Trick in the Facebook: Would the General Data Protection Regulation Have Stopped the Cambridge Analytica Scandal?**, Trinity College Law Review, 25, 2022, s. 221-242.

44) Whitworth, M., **Data at Rest Encryption and Key Management in GDPR, IDC Analyze the Future**, 2018, s. 6. Erişim tarihi 06.03.2025.

45) Yordanov, A., **Nature and ideal steps of the data protection impact assessment under the general data protection regulation**, European Data Protection Law Review (EDPL), 3(4), 2017, s. 486-495.

46) Yücedağ, N., **Kişisel verilerin korunması kanunu kapsamında genel ilkeler,** Kişisel Verileri Koruma Dergisi, Cilt 1, Sayı 1, 2019, s. 47-63. https://dergipark.org.tr/en/pub/kvkd/issue/45759/566993 , Erişim Tarihi 12.12.23.

İNTERNET KAYNAKÇA

1) Article 29 Working Party (2017), Guidelines on Personal data breach notification under Regulation 2016/679, WP250, 3 October 2017. https://www.edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-personal-data-breach-notification-under_en Erişim Tarihi 05.01.2025.

2) Avrupa İnsan Hakları Sözleşmesi, 8. madde ve 34. madde. https://echr.coe.int/documents/convention_eng.pdf Erişim Tarihi 04.06.2025.

3) Avrupa Birliği'nin İşleyişi Hakkında Antlaşma, T.C. Dışişleri Bakanlığı Avrupa Birliği Başkanlığı Çevirisi https://www.ab.gov.tr/files/pub/antlasmalar.pdf Erişim Tarihi 29.12.2023.

4) Avrupa Birliği Temel Haklar Şartı (Türkçe Çevirisi) http://www.ceidizleme.org/ekutuphaneresim/dosya/687_1.pdf Erişim Tarihi 03.01.2024.

5) Avrupa Genel Veri Koruma Tüzüğü, T.C. Dışişleri Bakanlığı Avrupa Birliği Başkanlığı Çevirisi (General Data Protection Regulation) https://www.ab.gov.tr/siteimages/resimler/N%C4%B0HA%C4%B0%20H%C3%87DB%20GDPR%206_11_2023(5).pdf Erişim Tarihi 14.11.2023.

6) Avrupa Veri Koruma Denetçisi https://edps.europa.eu/data-protection/data-protection/legislation/history-general-data-protection regulation_en#:~:text=In%202016%2C%20the%20EU%20adopted,as%20law%20across%20the%20EU. Erişim Tarihi 14.11.2023.

7) Avrupa Veri Koruma Denetçisi https://edps.europa.eu/about-edps_en Erişim Tarihi 27.11.2023.

8) Avrupa Veri Koruma Kurulu https://www.edpb.europa.eu/about-edpb/who-we-are/legacy-art-29-working-party_en Erişim Tarihi 22.04.2024.

9) Avrupa Veri Koruma Kurulu https://www.edpb.europa.eu/our-work-tools/support-cooperation-and-enforcement/gdpr-cooperation-and-enforcement_en Erişim Tarihi 23.04.2024.

10) Case C-673/17 (Court of Justice), Bundesverband der Verbraucherzentralen und Verbraucherverbände — Verbraucherzentrale Bundesverband eV v Planet49 GmbH [2019], ECLI:EU:C:2019:801. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:62017CJ0673

11) Case C-311/18 (Court of Justice), Data Protection Commissioner v Facebook Ireland Ltd and Maximillian Schrems [2020], ECLI:EU:C:2020:559. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:62018CJ0311

12) Case C-247/23 (Court of Justice), Deldits v Országos Idegenrendészeti Főigazgatóság [2025], ECLI:EU:C:2024:747 https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:62023CJ0247

13) Case C-152/22 (Court of Justice), Deutsche Telekom AG v Bundesrepublik Deutschland [2024], ECLI:EU:C:2024:226. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:62022CJ0152

14) Case C-77/21 (Court of Justice), Digi Távközlési és Szolgáltató Kft. v Nemzeti Adatvédelmi és Információszabadság Hatóság [2022], ECLI:EU:C:2022:817. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:62021CJ0077

15) Case C-645/19 (Court of Justice), Facebook Ireland Ltd and Others v Gegevensbeschermingsautoriteit [2021], ECLI:EU:C:2021:483. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:62019CJ0645

16) Case C-40/17 (Court of Justice), Fashion ID GmbH & Co. KG v Verbraucherzentrale NRW eV [2019], ECLI:EU:C:2019:629. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:62017CJ0040

17) Case C-487/21 (Court of Justice), FF v CRIF GmbH [2023], ECLI:EU:C:2023:369. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:62021CJ0487

18) Case C-307/22 (Court of Justice), FT v DW [2023], ECLI:EU:C:2023:11. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:62022CJ0307

19) Case C-131/12 (Court of Justice) Google Spain SL and Google Inc. v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González [2014] ECLI:EU:C:2014:317. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:62012CJ0131

20) Case C-25/17 (Court of Justice), Jehovan todistajat –uskonnollinen yhdyskunta v Tietosuojavaltuutetun toimisto [2018], ECLI:EU:C:2018:551. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:62017CJ0025

21) Case C-439/19 (Court of Justice), Latvijas Republikas Saeima [2021], ECLI:EU:C:2021:504. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:62019CJ0439

22) Case C-434/16 (Court of Justice), Peter Nowak v Data Protection Commissioner [2017], ECLI:EU:C:2017:994. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:62016CJ0434

23) Case C-154/21 (Court of Justice), RW v Österreichische Post AG [2023], ECLI:EU:C:2023:3. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:62021CJ0154

24) Case C-768/21 (Court of Justice) TR v Land Hessen [2024] ECLI:EU:C:2024:785. https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX:62021CJ0768

25) Case C-340/21 (Court of Justice), VB v Natsionalna agentsia za prihodite [2023], ECLI:EU:C:2023:11. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:62021CJ0340

26) Case C-191/15 (Court of Justice) Verein für Konsumenteninformation v Amazon EU Sàrl [2016] ECLI:EU:C:2016:612. https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX:62015CJ0191

27) Case C-230/14 (Court of Justice) Weltimmo s.r.o. v Nemzeti Adatvédelmi és Információszabadság Hatóság [2015] ECLI:EU:C:2015:639. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:62014CJ0230

28) Case C-210/16 (Court of Justice), Wirtschaftsakademie Schleswig-Holstein GmbH v. ULD [2018], ECLI:EU:C:2018:388. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:62016CJ0210

29) Case T-325/23 (General Court) Meta Platforms Ireland v EDPB [2023] 62023TN0325. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62023TN0325&qid=1744017281819

30) Case T-557/20 (General Court), Single Resolution Board (SRB) v European Data Protection Supervisor (EDPS) [2023], ECLI:EU:T:2023:66. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:62020TJ0557

31) Charter of Fundamental Rights of the European Union, OJ C 326, 26.10.2012, s. 391–407. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A12012P%2FTXT Erişim Tarihi 04.06.2025.

32) Clifford Chance Article https://www.cliffordchance.com/insights/resources/blogs/talking-tech/en/articles/2022/05/spanish-data-protection-agency-imposes-10-million-euro-fine-on-g.html Erişim Tarihi 07.03.2025.

33) CNPD decision regarding Amazon Europe Core S.À R.L. https://cnpd.public.lu/en/actualites/national/2025/03/amazon-decision.html Erişim Tarihi 07.04.2025.

34) Council of Europe. (1981). Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Convention 108). Strasbourg, 28.01.1981. European Treaty Series – No. 108. https://www.coe.int/en/web/data-protection/convention108 Erişim Tarihi 03.06.2025.

35) Council Decision (EU) 2019/682 of 9 April 2019 authorising Member States to sign, in the interest of the European Union, the Protocol amending the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data. Official Journal of the European Union, L 115, 02.05.2019, s. 7–9 https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32019D0682 Erişim Tarihi 03.06.2025.

36) Data Privacy Manager https://dataprivacymanager.net/5-biggest-gdpr-fines-so-far-2020/ Erişim Tarihi 07.03.2025.

37) Directive 95/46/EC of the European Parliament and of the Council of 24.10.1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, OJ L 281, 23.11.1995, s. 31–50. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:31995L0046 Erişim Tarihi 03.06.2025.

38) Directive (EU) 2016/680 of the European Parliament and of the Council of 27.04.2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, OJ L 119, 4.5.2016, s. 89–131. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32016L0680 Erişim Tarihi 03.06.2025.

39) Doxagon Blog https://www.doxagon.com/blog/gdpr-kvkk/#:~:text=GDPR%2C%20AB'de%20ya%C5%9Fayan%20bireylerin,dan%20daha%20kapsaml%C4%B1%20bir%20yasad%C4%B1r. Erişim Tarihi 10.03.2025.

40) European Data Protection Board. (2021). Guidelines 01/2021 on examples regarding data breach notification – Version 2.0. https://edpb.europa.eu/our-

work-tools/our-documents/guidelines/guidelines-012021-examples-regarding-data-breach_e Erişim Tarihi 03.06.2025.

41) European Data Protection Board, Guidelines 9/2022 on Personal Data Breach Notification under GDPR – Version 2.0, 28 March 2023, https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-092022-personal-data-breach-notification-under_en Erişim Tarihi 03.06.2025.

42) European Data Protection Supervisor https://www.edps.europa.eu/data-protection/our-work/publications/events/european-data-protection-day-0_en#:~:text=Protection%20Day%202025!-,28%20January%202025,protection%20of%20their%20personal%20data. Erişim Tarihi 12.03.2025.

43) GDPR Register https://www.gdprregister.eu/news/startup-uses-ai-for-gdpr-compliance/ Erişim Tarihi 03.01.2025.

44) GDPR Summary https://www.gdprsummary.com/gdpr-summary/ Erişim Tarihi 14.11.2023.

45) Inspired eLearning https://inspiredelearning.com/blog/a-brief-history-of-the-gdpr/#:~:text=GDPR%20was%20created%20to%20replace,data%20is%20the%20common%20currency. Erişim Tarihi 29.12.2023.

46) Ireland Data Protection Commission (DPC Inquiry Reference: IN-20-7-4) https://dataprotection.ie/en/news-media/press-releases/data-protection-commission-announces-decision-instagram-inquiry Erişim Tarihi 07.04.2025.

47) Ireland Data Protection Commission https://www.dataprotection.ie/en/news-media/press-releases/irish-data-protection-commission-fines-linkedin-ireland-eu310-million Erişim Tarihi 07.04.2025.

48) Katılım Sürecinde Müzakere Fasılları (AB Başkanlığı) https://www.ab.gov.tr/files/rehber/07_rehber.pdf Erişim Tarihi 03.01.2024.

49) 6698 sayılı Kişisel Verilerin Korunması Kanunu https://www.mevzuat.gov.tr/mevzuat?MevzuatNo=6698&MevzuatTur=1&MevzuatTertip=5

50) 6698 sayılı Kişisel Verilerin Korunması Kanunu Gerekçesi. https://www5.tbmm.gov.tr/sirasayi/donem26/yil01/ss117.pdf Erişim Tarihi 27.11.2023.

51) 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 11.03.2025.

52) Kişisel Verileri Koruma Kurumu https://www.kvkk.gov.tr/Icerik/2074/Misyon---Vizyon Erişim Tarihi 11.03.2025.

53) Kişisel Verileri Koruma Kurumu https://www.kvkk.gov.tr/Icerik/5278/Milli-Egitim-Bakanligi-7-Nisan-Gununun-Kisisel-Verileri-Koruma-Gunu-Olarak-Kutlanmasi-Kararlastirilmistir#:~:text=Tarihi%3A%2002.09.2018-,Milli%20E%C4%9Fitim%20Bakanl%C4%B1%C4%9F%C4%B1%207%20Nisan%20G%C3%BCn%C3%BCn%C3%BCn%20%22Ki%C5%9Fisel,Koruma%20G%C3%BCn%C3%BC%22%20Olarak%20Kutlanmas%C4%B1n%C4%B1%20Kararla%C5%9Ft%C4%B1rd%C4%B1 Erişim Tarihi 12.03.2025.

54) KVKK Asistan https://www.kvkkasistan.com/Haberler/turkiye%E2%80%99de-kurulu-sirketlerin-gdpr-uyum-sorumlulugu/79 Erişim Tarihi 03.01.2024.

55) La Justice https://justice.public.lu/fr/actualites/2025/03/tribunal-administratif-jugement-amazon-amende-cnpd.html Erişim Tarihi 07.04.2025.

56) Organisation for Economic Co-operation and Development (OECD), Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data, 23.09.1980. https://www.oecd.org/sti/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm Erişim Tarihi 03.06.2025.

57) Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), OJ L 119, 4.5.2016, s. 1–88. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=OJ:L:2016:119:TOC Erişim Tarihi 03.06.2025.

58) Skillcast https://www.skillcast.com/blog/biggest-gdpr-fines-2024 Erişim Tarihi 03.01.2025.

59) T.C. Anayasası https://www.mevzuat.gov.tr/mevzuat?MevzuatNo=2709&MevzuatTur=1&MevzuatTertip=5 Erişim Tarihi 10.03.2025.

60) The Autoriteit Persoonsgegevens (The Dutch data protection authority) https://autoriteitpersoonsgegevens.nl/en/current/dutch-dpa-imposes-a-fine-of-290-million-euro-on-uber-because-of-transfers-of-drivers-data-to-the-us Erişim Tarihi 07.04.2025.

ÖZET

İnsanların hayatının vazgeçilmez bir parçası haline gelen internet, yine insanların hayatının her alanında büyük etkiler yaratmaktadır. Bu büyük etki yarattığı alanlardan birisi de hukuktur. Özellikle kişisel veriler alanında etkisi her geçen gün daha da ciddiye alınmaktadır. Modern çağda bir bireyin tüm kişisel bilgileri internet üzerinde veri olarak depolanmaktadır. Gerek devletler tarafından gerekse özel kurumlar tarafından birey hakkında her türlü çeşit bilgi depolanıp kullanılmaktadır. Bu kişisel veri kullanımının belli kurallara uygun yapılabilmesi ve bireylerin kişisel veri güvenliğinin sağlanabilmesi için Avrupa Birliği tarafından Genel Veri Koruma Tüzüğü oluşturulmuştur. Tezin konusu Avrupa Birliği "Genel Veri Koruma Tüzüğü'nde Veri İhlali Bildirimleri"dir. Tezin kapsam ve sınırlılık konusunda gelindiğinde ise, bu çalışmada başta Genel Veri Koruma Tüzüğü olmak üzere ilgili mevzuatı, Türkiye'deki 6698 sayılı Kişisel Verilerin Korunması Kanunu'na da değinecek şekilde ilerleyecektir. Ana noktası belirtildiği üzere Genel Veri Koruma Tüzüğü'nde veri ihlali bildirimleri olacaktır. Tezin ilk bölümünde, Avrupa Genel Veri Koruma Tüzüğü, veri ihlali bildirimi ile bağlantılı kavramlar, kurul, Tüzük'ün uygulanma alanı, ilkeler ve tartışmalar açıklandıktan sonra ilgili mevzuatın kişisel veri ihlali bildirimi ile ilgili özellikleri de konunun anlaşılabilmesi açısından incelenip araştırma konusuna yönelik çıkarımlarda bulunulacaktır. Sınırlandırma bu şekilde ilerleyecektir çünkü araştırma noktasının açıkça irdelenebilmesi için bu gereksinim oluşmaktadır. Tezin ikinci bölümünde ise kişisel veri ihlali bildirimi, kişisel veri ihlali bildirimi sonrası, veri sorumlusunun yükümlülükleri ve etkili bildirimin önemi, iyileştirilmesi, ilgili yargı kararları, Genel Veri Koruma Tüzüğü'nün sınır aşırı etkisi ve Türk hukukunda kişisel verilerin korunması ve veri ihlali bildirimi incelenecektir.

Genel amaç, veri ihlali bildirimlerinin ne olduğunu tam olarak kavramaktır. Alt amaç ise bu bildirimlerin nasıl yapıldığına, bildirim sonrası yaptırımların ne olduğuna, iyileştirmek için neler yapılabileceğine ve etkili bildirim yapmanın önemine cevap bulmaktır. Bir veri ihlali yaşandığında bildirim yapılması, sıradaki en önemli adımlardan biri haline gelmektedir. Genel Veri Tüzüğü'nün 33. maddesinde "Kişisel veri ihlalinin denetim makamlarına bildirilmesi" düzenlenmiştir. Ardından gelen 34. maddede ise "Kişisel veri ihlali hakkında veri öznesinin bilgilendirilmesi" düzenlenmiştir. Öncelikle ilgili denetim makamına bildirim yapılmasına önem verilmiştir. Bu noktada bazı kurallar da getirilmiştir. Bunlar uygulamaya yönelik kurallardır. Uygulamada ise bu kuralların ne kadar etkili olabildiği incelenecektir ve etkin bir yöntem veya Tüzüğün bu konuda uygulanmasını etkin hale getirecek, iyileştirecek bir değişiklik yapılabilir mi amacıyla da hareket edilecektir. Böylece, uygulamanın da etkili bir şekilde işlemesine katkıda bulunulacaktır.

Anahtar Kelimeler: Avrupa Birliği hukuku, Avrupa Birliği Genel Veri Koruma Tüzüğü, Kişisel verilerin korunması, Veri ihlali bildirimi, Kişisel veri ihlalinin denetim makamlarına bildirilmesi, kişisel veri ihlalinin veri öznesine (veri sahibine) bildirilmesi.

ABSTRACT

The internet, which has become an indispensable part of people's lives, has great effects on every aspect of people's lives. One of the areas where it has great effects is law. Its effect, especially in the field of personal data, is taken more seriously every day. In the modern age, all personal information of an individual is stored as data on the internet. All kinds of information about the individual is stored and used by both states and private institutions. In order for this personal data usage to be carried out in accordance with certain rules and to ensure the security of individuals' personal data, the General Data Protection Regulation was established by the European Union. The subject of the thesis is "Data Breach Notifications in the General Data Protection Regulation" of the European Union. When it comes to the scope and limitation of the thesis, this study will proceed by touching on the relevant legislation, especially the General Data Protection Regulation, and the Personal Data Protection Law No. 6698 in Türkiye. As the main point is stated, there will be data breach notifications in the General Data Protection Regulation. In the first part of the thesis, the European General Data Protection Regulation, concepts related to data breach notification, the board, the scope of application of the Regulation, principles and discussions will be explained, and then the features of the relevant legislation regarding personal data breach notification will be examined in order to understand the subject and conclusions will be made regarding the research subject. The limitation will proceed in this way because this requirement arises in order to clearly examine the research point. In the second part of the thesis, personal data breach notification, the obligations of the data controller after the personal data breach notification and the importance of effective notification, its improvement, relevant court decisions, the cross-border effect of the General Data Protection Regulation and the protection of personal data and data breach notification in

Turkish law will be examined. The general aim is to fully understand what data breach notifications are. The sub-goal is to find answers to how these notifications are made, what the sanctions are after the notification, what can be done to improve and the importance of effective notification. When a data breach occurs, notification becomes one of the most important steps in the future. Article 33 of the General Data Regulation regulates "Notification of personal data breach to supervisory authorities". The following article 34 regulates "Information of data subjects about personal data breach". First of all, importance is given to notifying the relevant supervisory authority. Some rules have also been introduced at this point. These are rules for implementation. In practice, it will be examined how effective these rules are and whether an effective method or a change can be made to make the implementation of the Regulation effective and improve it. Thus, it will contribute to the effective operation of the application.

Keywords: European Union law, European Union General Data Protection Regulation, Protection of personal data, Data breach notification, Notification of personal data breach to supervisory authorities, notification of personal data breach to data subject (data owner).