KILIÇ ÇAYLI & Partners

EKİM 2021 SAYI: 22

Veri Hukuku Özel Sayısı

Kişisel Verileri Koruma Kurulu'nun Yeni Yayınlanan Karar Özetleri

- Bir Perakende Giyim Firmasının Kişisel Veri İhlali Bildirimi Hakkında Kişisel Verileri Koruma Kurumu'nun 20.01.2020 Tarihli ve 2020/50 Sayılı Kararı
- Bilgisayar Oyunları Alanında Faaliyet Gösteren Veri Sorumlusunun Veri İhlali Bildirimi Hakkında Kişisel Verileri Koruma Kurumu'nun 05.05.2020 Tarihli ve 2020/345 Sayılı Kararı
- Bir Bankanın Veri İhlali Bildirimi Hakkında Kişisel Verileri Koruma Kurumu'nun 07.05.2020 Tarihli ve 2020/359 Sayılı Kararı
- Bir Sigorta Şirketinin Veri İhlali Bildirimi Hakkında Kişisel Verileri Koruma Kurumu'nun 09/07/2020 Tarihli ve 2020/532 Sayılı Kararı

Whatsapp Uygulaması Hakkında Yürütülen Resen İncelemeye İlişkin KVKK Kamuoyu Duyurusu

Kişisel Verilerin Korunması Kurumu'nca yayımlanan "Yapay Zekâ Alanında Kişisel Verilerin Korunmasına İlişkin Tavsiyeler"

Kişisel Verilerin Korunması Kurumu'nca yayımlanan "Biyometrik Verilerin İşlenmesinde Dikkat Edilmesi Gereken Hususlara İlişkin Rehber"

Covid-19 PCR Test Sonucu ve Aşı Bilgisi Uygulamalarına İlişkin KVKK Kamuoyu Duyurusu

İmtiyaz Sahibi	Editör	Yazarlar	İletişim
Av. Duygu Kılıç Çaylı *Kılıç Çaylı & Partners* *Hukuk Ofisi adına*	*Kıvılcım Çaylı*	*Av. Belemir Gencal Doğanöz* *Av. Melis Pülten* *Stj. Av. Deniz Karaduman* *Stj. Av. Kaan Uğursal*	*Mutlukent Mah. Arda Sk. No:9* *Beysukent 06800 Çankaya* *Ankara/TURKİYE*

www.kiliccayli.com
info@kiliccayli.com

Kişisel Verileri Koruma Kurulu'nun 09.08.2021 Tarihli Yeni Yayınlanan Karar Özetleri Yayını

Bir Perakende Giyim Firmasının Kişisel Veri İhlali Bildirimi Hakkında Kişisel Verileri Koruma Kurumu'nun 20.01.2020 Tarihli ve 2020/50 Sayılı Kararı

İhlal bazı müşterilerin yeni bir hesap açarken kişisel verilerinin yanlışlıkla bir URL üzerinden veri sorumlusunun iç sistemlerine ve çalıştığı bazı üçüncü taraf satıcılara aktarılması şeklinde gerçekleşmiştir.

Durum, veri sorumlusunun olağan bir denetimi esnasında tespit edilmiştir. Veri sorumlusu Kuruma, iki uygulama analizi sağlayıcısından (analytics provider) verilerin hâlihazırda otomatik olarak silinmiş olduğuna dair teyit aldığını bildirmişse de ilk bulgulardan sonra konunun daha detaylı araştırılması için gerçekleştirilen soruşturma kapsamında başka yedi adet URL tarafından da sehven veri toplandığı ve bunların veri sorumlusunun etiket yönetim sistemine (tag management system) yönlendirildiği tespit edilmiştir.

Şirketin Kuruma yaptığı 10.06.2019 tarihli ilk bildirimde, ihlalden etkilenen kişisel verilerin, zorunlu alan olan e-posta adresi, doğum tarihi, açık metin şeklinde şifre verilerinin olduğu, ancak zorunlu alan olmayan ad soyadı verilerinin de etkilenmiş olabileceği veri sorumlusu tarafından belirtilmiştir.

Kurum tarafından, 01.08.2018 ve 21.10.2018 tarihlerinde gerçekleşen veri ihlallerinin tespitinin yaklaşık bir yıl sonra 02.07.2019 yapılmasının nedeni; Şirketin log kaydı/takip alarm sistemlerinin bulunmaması, etkin bir şekilde kullanılmaması ve Şirket tarafından gerekli kontrollerin yapılmaması olarak değerlendirilmiştir.

Ayrıca URL üzerinden kişisel verilerin üçüncü taraf satıcı/sağlayıcılar tarafından görülmesinin web sayfası tasarım aşamasında iken yapılan testlerin yetersiz olduğunun veya gerekli testlerin yapılmadığının göstergesi olduğu tespit edilmiştir.

Bu kapsamda **Web sayfası tasarım aşamasında iken yapılan testlerin yetersiz olması, gerçekleşen işlemlere dair takip/alarm sistemlerinin bulunmamasından kaynaklı ihlal tespitinin geç yapılmış olması sebebiyle**, 6698 sayılı Kişisel Verilerin Korunması Kanununun 12/1 maddesi çerçevesinde veri güvenliğini sağlamaya yönelik gerekli teknik ve idari tedbirleri almayan veri sorumlusu hakkında Kanunun 18. maddesinin 1/b bendi uyarınca 50.000 TL idari para cezası uygulanmasına karar verilmiştir.

Buna karşılık ihlalin veri sorumlusu tarafından 29.05.2019 tarihinde tespit edildiği, 06.06.2019 tarihinde Kurula bildirimin yapıldığı görülmekle birlikte yurtdışında mukim veri sorumlusu tarafından tespit tarihinden sonra söz konusu ihlalden Türkiye'deki ilgili kişilerin de etkilenip etkilenmediğine yönelik araştırma yapıldığı dikkate alındığında bu sürenin makul olduğu değerlendirilmiş ve işlem yapılmamasına karar verilmiştir.

Değerlendirme: Anılan kararda, Web sayfası tasarım aşamasında iken yapılan testlerin yetersiz olması, gerçekleşen işlemlere dair takip/alarm sistemlerinin bulunmamasından kaynaklı ihlal tespitinin geç yapılmış olması Kurum tarafından idari para cezasının gerekçesi olarak gösterilmiştir. Gerekli teknik ve idari tedbirlerin alınmadığını belirten kurum, aslında bu şekilde **Kişisel Veri Güvenliği Rehberine de atıfta bulunmuştur. Rehberin 28 ve 29. Sayfalarında 'Teknik Tedbirler Özet Tablosu' ve 'İdari Tedbirler Özet Tablosu'nda veri sorumluları tarafından alınabilecek tedbirler düzenlenmiştir.**

Kurum tarafından dayanılan idari para cezasının gerekçeleri de tablolarda yer almaktadır. Bu açıdan, şirket çalışma alanları, toplanan kişisel verilerin nitelikleri, Kurum tarafından yayınlanan rehberler ve kararlar doğrultusunda kişisel verilerin korunmasına ilişkin tüm idari ve teknik tedbirlerin alınması önem arz etmektedir.

Bilgisayar Oyunları Alanında Faaliyet Gösteren Veri Sorumlusunun Veri İhlali Bildirimi Hakkında Kişisel Verileri Koruma Kurumu'nun 05.05.2020 Tarihli ve 2020/345 Sayılı Kararı

Yapılan rutin güvenlik denetimi sırasında **eski bir veri sorumlusu çalışanı** (web geliştiricisi) tarafından içerisinde kaynak kod ile veri dosyaları içeren bir klasörün yetkisiz olarak github.com internet sitesine yüklendiği tespit edilmiştir. Konu hakkında inceleme başlatılmış ve yapılan incelemede klasör içerisinde yer alan birçok dosyada veri sorumlusu kullanıcılarının bir alt kümesinin kimliğini belirli kılabilecek bilgilerin bulunabileceği tespit edilmiş olsa da bu verilerin büyük bir kısmının veri sorumlusu hizmetlerinden menedilmiş sahte(bot) hesaplara ait olduğunun görülmüştür.

İncelemenin detaylandırılmasından sonra 12 Ocak 2019 tarihinde verilerin hem sahte(bot) hesaplara hem de Türkiye'de mukim kullanıcılara ait gerçek hesapların birleşiminden oluştuğu kesinleşmiştir.

Yapılan çalışmalar sonucunda bilindiği kadarıyla söz konusu verilerin GitHub'dan kaldırıldığı veya kamu erişimine kapalı hale getirildiği, ihlalden etkilenen kişisel verilerin kimlik (doğum tarihi), iletişim (e-posta adresi), lokasyon (internet hizmet sağlayıcı ve kullanıcı kayıt tarihi ve saati) gibi bilgilerin olduğu belirlenmiştir.

Veri ihlalinin, veri sorumlusu ve eski bir çalışanı ile iş ilişkisinin sonlanmasının akabinde, bu kişinin yetkisiz bir biçimde kişinin işinin ürünü olan kaynak kodu ve veri dosyalarını içeren klasörü github.com'a (GitHub) yüklemesi ile gerçekleştiği tespit edilmiştir. **Eski çalışanın kaynak kodları da github.com internet sitesine yüklemiş olmasının bir güvenlik açığı olduğu değerlendirilmiştir**. Bu kaynak kodların yetkisiz üçüncü kişiler tarafından analiz edilerek başka güvenlik açıklıklarına sebebiyet verebileceği dikkate alındığında kişisel veri güvenliği noktasında veri sorumlusu tarafından gerekli teknik ve idari tedbirlerin yeterince alınmamış olduğunun ve Kişisel Verileri Koruma Kurumunca yayınlanan Kişisel Veri Güvenliği Rehberinin(Teknik ve

İdari Tedbirler) 2.2. numaralı "**Çalışanların Eğitilmesi ve Farkındalık Çalışmaları**" uygun davranmadığının göstergesi olduğu tespit edilmiştir. İhlalin gerçekleşme tarihinin 19.04.2017, tespit tarihinin 09.01.2019, Kuruma bildirim tarihinin ise 28.02.2019 tarihi olduğu, aradan 2 yıla yakın süre geçtikten sonra 09.01.2019 tarihinde ihlalin tespit edilmesinin güvenlik kontrollerinin düzenli olarak yapılmadığının, dolayısıyla kişisel veri güvenliği takibi açısından veri sorumlusunun almış olduğu teknik ve idari tedbirlerin yetersiz kaldığının göstergesi olduğu tespit edilmiştir.

6698 sayılı Kişisel Verilerin Korunması Kanununun 12'nci maddesinin (1) numaralı fıkrası kapsamında veri güvenliğini sağlamaya yönelik gerekli teknik ve idari tedbirleri almayan veri sorumlusu hakkında Kanunun 18 inci maddesinin (1) numaralı fıkrasının (b) bendi uyarınca 100.000 TL, 19.04.2017'de gerçekleşen veri ihlalinin 09.01.2019 tarihinde tespit edildiği, Kuruma 28.02.2019 tarihinde bildirim yapıldığı hususları dikkate alındığında, veri sorumlusunun Kanunun 12/5 maddesinde yer verilen "en kısa sürede" bildirimde bulunma yükümlülüğüne aykırılık teşkil etmesi nedeniyle Kanunun 18/1/b bendi uyarınca veri sorumlusu hakkında 30.000 TL olmak üzere toplam 130.000 TL idari para cezası uygulanmasına karar verilmiştir.

Değerlendirme: Kişisel Veri Güvenliği Rehberi'nin (Teknik ve İdari Tedbirler) 2.2. numaralı "*Çalışanların Eğitilmesi ve Farkındalık Çalışmaları*" başlığı altında yer alan maddesine atıf yaparak ceza gerekçesi açıklanmıştır. Buna göre: "*Çalışanların, kişisel verilerin hukuka aykırı olarak açıklanmaması ve paylaşılmaması gibi konular hakkında eğitim almaları, çalışanlara yönelik farkındalık çalışmaları yapılması ve güvenlik risklerinin belirlenebildiği bir ortam oluşturulması kişisel veri güvenliğinin sağlanması bakımından çok önemlidir.* ***Veri sorumlusu nezdinde çalışan herkesin hangi konumda çalıştığına bakılmaksızın kişisel veri güvenliğine ilişkin rol ve sorumlulukları, görev tanımlarında belirlenmeli ve çalışanların bu konudaki rol ve sorumluluğunun farkında olması sağlanmalıdır.*** *Ayrıca kişisel veri içeren ortamlara erişim hakkı verilirken veya bu konuda kurum kültürü oluşturulurken "Yasaklanmadıkça Her Şey Serbesttir" prensibi değil,* ***"İzin Verilmedikçe Her Şey Yasaktır"*** *prensibine uygun hareket edilmesine dikkat edilmelidir."*

Kanun uygulaması açısından yol gösterici ve bağlayıcı niteliktedir. Bu kapsamda Kurum tarafından Ocak 2018 tarihinde yayımlanan Teknik ve İdari Tedbirler başlıklı Rehberi incelediğimizde özellikle veri sorumlusu tarafından veri güvenliğine ilişkin alınması gereken idari tedbirler başlığı altında çalışanların eğitilmesi gerektiği ve farkındalık çalışmalarının oldukça önemli olduğu görülmektedir.

Bir Bankanın Veri İhlali Bildirimi Hakkında Kişisel Verileri Koruma Kurumu'nun 07.05.2020 Tarihli ve 2020/359 Sayılı Kararı

İhlalin; Kredi Kayıt Bürosu (''KKB'') ekranında, Veri Sorumlusu Banka'nın eski çalışanının işin gereğinden fazla adette sorgulama yapılması ile gerçekleştiği tespit edilmiştir. Çalışanın ifadesine göre; T.C. kimlik numaraları Banka dışından 3. şahıs tarafından iletilip kişilerin kredi skorlarının öğrenilmek istenildiği, ihlalin yıllık periyotlarla hazırlanan kontroller neticesinde veri ihlalini gerçekleştiren çalışanın işin gereğinden fazla adette sorgulama yaptığının fark edilmesi üzerine Teftiş Raporu hazırlanmıştır. Çalışanın KKB sorgulamalarını ilgili kişilerin gıyabında gerçekleştirdiği, KKB sorgulamalarını gerçekleştirdiği esnada cep telefonu ile ilgilendiği ve KKB sorgulamalarını yaptıktan hemen sonra bir kâğıda not aldığı, bazı tarihlerde bu kâğıdın fotoğrafını çektiği ve/veya cep telefonu ile yazıştığının tespit edilmesiyle ihlal gün yüzüne çıkmıştır. İhlalin Temmuz 2018 ile Mayıs 2019 tarihleri arasında gerçekleşmiş ve ihlalden veri sorumlusunun müşterisi olan ve müşterisi olmayan toplam 5695 kişinin etkilenmiştir. İhlalden etkilenen kişisel veriler:

- Şahısların bankalardan kullanmış oldukları tüm kredili ürünlere ilişkin geçmişleri,
- Ödeme performansları, borç rakamları,
- Adres, telefon vb.

olduğu veri sorumlusu tarafından ifade edilmiştir.

Çalışan tarafından, 5889 adet T.C. kimlik numarası sorgulanmış ve 2851'inin Banka müşterisi olmadığı tespit edilmiştir. Veri ihlalinin Temmuz 2018 ile Mayıs 2019 arasında gerçekleştiği, ihlalin anlaşılmasını sağlayan KKB sorgulama sayısının tespit edilmesine yönelik **kontrolün yıllık periyotlarla yapılıyor olması nedeniyle ihlalin 1 yıla yakın süre boyunca devam ettiği** ve ancak 18 Temmuz 2019 tarihinde tespit edilebildiği hususlarının, "Kişisel Veri Güvenliği Rehberi'nin (Teknik ve İdari Tedbirler-Rehber) "Kişisel Veri Güvenliğinin Takibi" başlığına aykırı olduğu Kurum tarafından değerlendirilmiştir. Veri sorumlusu tarafından kişisel verilerin korunmasına ilişkin kişisel veri güvenliği takibinin uygun zaman aralıklarıyla yapılmaması, veri sorumlusu tarafından ihlal öncesi yapılması gereken; kullanıcı bazında log kayıtlarında yetki sınırlaması, ekranların gereksiz rollere kapatılması, kişisel verilerin korunması ile ilgili uyarı metnine yer verilmesi gibi kullanıcı yetki ve rollerine yönelik kontrollerin ve düzenlemelerin ihlal sonrasında gerçekleştirilmiş olmasını Rehber'in **"Kişisel Veri İçeren Ortamların Güvenliğinin sağlanması"** başlığına aykırı olarak bulmuştur. **İlgili teknik ve idari tedbirlerin ihlal öncesinde yeterince alınmaması da ihmal olarak değerlendirilmiştir**. Veri ihlalinden önce sorgulanabilecek kişi sayısının sınırlandırılmamış olduğu ve ancak ihlalin gerçekleşmesinden sonra 250 üzerinde sorgulama yapan kullanıcıların kamera kayıtları incelenerek veri ihlali oluşturacak bir durum olup olmadığının kontrol edildiği hususunun, Rehber'in "Mevcut Risk ve Tehditlerin Belirlenmesi" başlığına aykırı olduğu Kurum değerlendirilmiştir. Veri sorumlusuna ait çalışanlar için veri güvenliği ve Kişisel Verilerin

Korunması Kanunu konusunda **belli aralıklarla eğitim ve farkındalık çalışmalarının yapıldığı**, çalışanların %86'sının konuyla ilgili bilgilendirme eğitimini tamamladığı, kalan kişilere ise eğitimin tekrar iletildiği ifade edildiği **ancak bu hususta tevsik edici belge gönderilmediği** hususlarının, Kişisel Verilerin Korunması Kanununun 2016 yılında kabul edilen, Rehber'in 2018 yılının ocak ayında yayımlanmış olduğu *"Çalışanların Eğitilmesi ve Farkındalık Çalışmaları"* tedbirine aykırı nitelikte olduğu ve halen çalışanlara eğitim verilmesinin sağlanmadığı belirtilerek Kanun'un 12'nci maddesinin (1) numaralı fıkrası çerçevesinde veri güvenliğini sağlamaya yönelik gerekli teknik ve idari tedbirleri almayan veri sorumlusu hakkında Kanunun 18'nci maddesinin (1) numaralı fıkrasının (b) bendi uyarınca 400.000 TL ceza uygulanmıştır.

Yine 18.07.2019 tarihinde tespit edilmiş olan ihlal 31.07.2019 tarihinde Kurula bildirilmiştir. Geç bildirim sebebi olarak şirket tarafından, Teftiş Raporunda yer alan bilgilerin hangilerinin paylaşıldığının net olmadığının ifade edilmesi, eldeki delillerin yetersizliği, olayın mahiyetinden emin olunmaması, müşteri şikâyeti olmaması, dışarıdan gelen T.C. Kimlik numaralarına istinaden bu durumun ortaya çıkması gibi sebeplerle, bildirim gerekip gerekmediğinin kurum içinde değerlendirilmesi ve tüm ilgili ünitelerden görüş alınmasından kaynaklandığı sebepleri ileri sürülmüştür. Kurum ise belirtilen sebeplerin geç bildirim için **geçerli bir mazeret olmadığına karar vermiştir.** Veri ihlalinden etkilenen 5695 kişi arasında **sadece Bankada iletişim bilgileri bulunanlara veri ihlal bildiriminde bulunulması ise ilgili kişilerin tamamına bildirimde bulunmak adına makul çabanın sarf edilmemesi olarak değerlendirilmiştir**.

Bu kapsamda ise Kanun'un 12/5 numaralı fıkrasında yer verilen "**en kısa sürede" (Kurul'a bildirim için 72 saat)** bildirimde bulunma yükümlülüğüne aykırı davranan veri sorumlusu hakkında Kanunun 1871/b maddesi uyarınca 50.000 TL olmak üzere toplam 450.000 TL idari para cezası uygulanmasına karar verilmiştir.

Değerlendirme: Karar ile Kişisel Veri Güvenliği Rehberi içerisinde yer alan tedbirlerden 3 başlığa atıfta bulunulmuştur.

1- *'Kişisel Veri Güvenliğinin Takibi'*: *"Veri sorumlularının sistemleri çoğunlukla hem içeriden hem de dışarıdan gelen saldırılar ve siber suçlara veya kötü amaçlı yazılımlara maruz kalmakta olup çeşitli belirtilere rağmen bu durum uzun süre fark edilememekte ve müdahale için geç kalınabilmektedir. Bu durumun önüne geçebilmek için; a) Bilişim ağlarında hangi yazılım ve servislerin çalıştığının kontrol edilmesi, b) Bilişim ağlarında sızma veya olmaması gereken bir hareket olup olmadığının belirlenmesi, c) Tüm kullanıcıların işlem hareketleri kaydının düzenli olarak tutulması (log kayıtları gibi), ç) Güvenlik sorunlarının mümkün olduğunca hızlı bir şekilde raporlanması, d) Çalışanların sistem ve servislerdeki güvenlik zafiyetlerini ya da bunları kullanan tehditleri bildirmesi için resmi bir raporlama prosedürü oluşturulması, gerekmektedir."*

KKB sorgulama sayısının tespit edilmesine yönelik kontrolün yıllık periyotlarla yapılıyor olması bu kapsamda ihmal olarak değerlendirilmiştir. Görüldüğü üzere, kişisel verilerin ihlali halinde Kurum, durumun uzun süre fark edilememesi ve gerekli kontrollerin uzun periyotlarda yapılması hallerini şirketin ceza-

landırılma gerekçeleri arasında saymıştır. Bu nedenle, özellikle çalışan sistemlerinin periyodik ve sık kontrolleri, şirketler bakımından kişisel verilerin korunması anlamında büyük önem arz etmektedir.

2- 'Kişisel Veri İçeren Ortamların Güvenliğinin sağlanması': "*Kişisel veriler elektronik ortamda ise, kişisel veri güvenliği ihlalini önlemek için ağ bileşenleri arasında erişim sınırlandırılabilir veya bileşenlerin ayrılması sağlanabilir. Örneğin kullanılmakta olan ağın sadece bu amaçla ayrılmış olan belirli bir bölümüyle sınırlandırılarak bu alanda kişisel verilerin işleniyor olması halinde, mevcut kaynaklar tüm ağ için değil de sadece bu sınırlı alanın güvenliğini sağlamak amacıyla ayrılabilecektir.*"

Kişisel verilerin ihlalinin önüne geçmek amacıyla yapılması gereken, yetki sınırlaması, ekranların gereksiz rollere kapatılması, kişisel verilerin korunması ile ilgili uyarı metnine yer verilmesi gibi kullanıcı yetki ve rollerine yönelik tedbirlerin ihlal sonrasında gerçekleştirilmiş olması bu kapsamda değerlendirilmiştir. İhlal bildirimi halinde yapılan Kurum incelemesinde Kurum'un önemle üzerinde durduğu başka bir husus, önlem alınmasıdır. Kurum birçok kararında gerekli önlemlerin ihlal öncesi alınması gerekliliğini vurgulamıştır. Bu durum da Kurum için kişisel verilerin korunmasında teknik ve idari tedbirlerin önceden alınması ve bu tedbirlerin takibinin sağlanmasının önemini gözler önüne sermektedir.

3- "Mevcut Risk ve Tehditlerin Belirlenmesi": "*Kişisel verilerin güvenliğinin sağlanması için öncelikle veri sorumlusu tarafından işlenen tüm kişisel verilerin neler olduğunun, bu verilerin korunmasına ilişkin ortaya çıkabilecek risklerin gerçekleşme olasılığının ve gerçekleşmesi durumunda yol açacağı kayıpların doğru bir şekilde belirlenerek buna uygun tedbirlerin alınması gerekmektedir. Bu riskler belirlenirken;*

- Kişisel verilerin özel nitelikli kişisel veri olup olmadığı,

- Mahiyeti gereği hangi derecede gizlilik seviyesi gerektirdiği,

- Güvenlik ihlali halinde ilgili kişi bakımından ortaya çıkabilecek zararın niteliği ve niceliği dikkate alınmalıdır. Bu risklerin tanımlanması ve önceliğinin belirlenmesinden sonra; söz konusu risklerin azaltılması ya da ortadan kaldırılmasına yönelik kontrol ve çözüm alternatifleri; maliyet, uygulanabilirlik ve yararlılık ilkeleri doğrultusunda değerlendirilmeli, gerekli teknik ve idari tedbirler planlanarak uygulamaya konulmalıdır."

İhlalin önüne geçilememesinin, sorgulamada sınırlama (kota) bulunmamasından kaynaklandığı belirtilmiştir.

Şirketlerin bu kapsamda risk analizine önem vermesi ve ihlalin meydana gelmesi halinde uğranılacak olası zararların tespit edilmesi sağlanarak, bu yönde önlemlerin önceden alınması için çalışmalar yapması önem arz etmektedir. Örneğin şirketlerin kendi çalışma alanlarına, işlenen kişisel verilerin niteliğine de uygun olarak olası risklerin ve sonuçlarının düzenlendiği bir tablo yapması ve risklere ilişkin önlemleri belirleyerek bu doğrultuda; kişisel verilerin korunmasına ilişkin tüm idari ve teknik tedbirleri zamanında alması faydalı olabilir.

Bir Sigorta Şirketinin Veri İhlali Bildirimi Hakkında Kişisel Verileri Koruma Kurumu'nun 09/07/2020 Tarihli ve 2020/532 Sayılı Kararı

Veri sorumlusunun bilgi sistem destek hizmeti aldığı hizmet sağlayıcısında meydana gelen sistemsel bir hata sonucu Otomatik Katılım Sistemi (OKS) kapsamında kendisine bağlı 61 şirketin müşterisi olan 367 ilgili kişinin kişisel verilerini içeren akıbet dosyalarını söz konusu hata sebebiyle yanlış alıcılara gönderilmiştir. Veri ihlalinden veri sorumlusunun müşterisi olan 61 şirketin toplam 367 çalışanın etkilendiği belirtilmiştir. Destek hizmeti sağlayıcısından iletilen bilgiye göre; **hataya sebebiyet veren uygulama 2010 yılında geliştirilmiş olup geliştirmede eski bir programdan yararlanıldığı**, yapılan geliştirme 2011 yılında devreye alındığı için, 2010 yılı ve öncesinde bu hata oluşmadığı tespit edilmiştir. Alt yapının ilk kez kurulmasından beri mevcut olan bir hatanın olduğu ve bu hatanın ilk kez içerisinde bulunduğumuz yıl bilgisinin son rakamının 0 (sıfır) olması sebebiyle gerçekleşebildiği değerlendirilmiştir. (Örneğin bu alt yapı, 2010 yılından önce geliştirilseydi ilk kez 2010 yılında karşılaşılacaktı ancak 2010 yılından sonra geliştirildiği için ilk problem 2020'de yaşanmıştır.), İhlalden 367 gerçek kişiye ait kimlik (TCKN, ad soyadı, doğum tarihi, SGK numarası), iletişim (telefon numarası, e-posta adresi), özlük (işe başlama tarihi) ve finans (IBAN numarası, katkı payı tutarı) verilerinin etkilenmiş ve ihlalden etkilenen kişilere ihlal sonrası şirket tarafından e-posta ile bildirim yapılmıştır.

Veri ihlaline sebep olan sistemsel hatanın 2011 yılından itibaren kullanılmaya başlanan uygulama yazılımından kaynaklanması sebebiyle ihlal, Kurum tarafından yayınlanan Kişisel Veri Güvenliği Rehberi (Teknik ve İdari Tedbirler)'nde 3.5.Bilgi Teknolojileri Sistemleri Tedariki, Geliştirme ve Bakımı başlığına aykırılık olarak değerlendirilmiştir.

Kanunun 12'nci maddesinin (1) numaralı fıkrası çerçevesinde veri güvenliğini sağlamaya yönelik gerekli teknik ve idari tedbirleri almayan veri sorumlusu hakkında Kanunun 18/1/b maddesi uyarınca 30.000 TL idari para cezasının uygulanmasına karar verilmiştir.

Değerlendirme: Karar ile atıf yapılan 3.5.Bilgi Teknolojileri Sistemleri Tedariği, Geliştirme ve Bakımı maddesinde yer alan: "*Veri sorumlusu tarafından yeni sistemlerin tedariki, geliştirilmesi veya mevcut sistemlerin iyileştirilmesi ile ilgili ihtiyaçlar belirlenirken güvenlik gereksinimleri göz önüne alınmalıdır. Uygulama sistemlerinin girdilerinin doğru ve uygun olduğuna dair kontroller yapılmalı, doğru girilmiş bilginin işlem sırasında oluşan hata sonucunda veya kasıtlı olarak bozulup bozulmadığını kontrol etmek için uygulamalara kontrol mekanizmaları yerleştirilmelidir.*" ifadesi gereği veri ihlaline sebep olan yazılımdaki sistemsel hatanın, veri güvenliğinin sağlanması amacıyla tespit edilebilmesi, hataların tespiti için gerekli donanımların veya programların kullanılması, sistemin sürekli olarak takip edilmesi, düzenli olarak, bakım, onarım ve iyileştirilmesinin yapılması gereklidir.

Whatsapp Uygulaması Hakkında Yürütülen Resen İncelemeye İlişkin Kamuoyu Duyurusu Kişisel Verilerin Korunması Kurulu İnternet Sitesinde 03.09.2021 Tarihinde Yayınlanmıştır.

WhatsApp, 2021 yılı başında Hizmet Koşullarının ve Gizlilik İlkesinin kullanıcıların kişisel verilerinin işlenmesine ve yurtdışında bulunan üçüncü taraflara aktarılmasına açık rıza verecek şekilde güncelledi. Gelen güncelleme sebebiyle açık rıza vermeyen kullanıcıların ise uygulamayı kullanamayacağına ve hesaplarının silineceğine dair Whatsapp tarafından bilgilendirme yapıldı. **WhatsApp tarafından kişisel verilerin işlenmesinin sözleşmenin bir parçası haline getirilmesi ve ilgili kişilere seçme imkânı sunulmaksızın hizmet şartı olarak** onay alınması üzerine Kişisel Verileri Koruma Kurulu; yurtdışına veri aktarımı, hizmetin açık rıza şartına bağlanması ve genel ilkelere uygunluk hususları başta olmak üzere, WhatsApp hakkında resen inceleme başlattı.

Kişisel Verileri Koruma Kurulu 3 Eylül 2021 tarihinde sitesinde yaptığı duyuruyla Whatsapp hakkında başlatılan soruşturmada 1.950.000 Türk lirası idari para cezasına hükmettiğini kamuoyuyla paylaştı. WhatsApp'ın Hizmet Koşulları ve Gizlilik İlkesi metinlerinin güncellenmesi dolayısıyla re'sen açılmış olan soruşturmada Kurul, 3 Eylül 2021 tarihli 2021/891 sayılı kararı ile WhatsApp'ın kişisel verilerin hukuka aykırı işlenmesini önlemek için yeterli teknik ve idari tedbirleri almadığı dolayısıyla WhatsApp'ın veri güvenliğine ilişkin yükümlülüklerini yerine getirmediğine karar verdi.

- Kullanıcılardan kişisel verilerinin işlenmesine ve yurtdışında yerleşik üçüncü taraflara aktarılmasına seçimlik hak sunulmaksızın tek bir açık rıza alınması, sözleşmeye aktarıma ilişkin hüküm koymak suretiyle işleme ve aktarım faaliyetlerinin, tek metinde birbirinden ayrılmaz bir biçimde ilgili kişiye sunulduğu dikkate alındığında, açık rızanın "özgür iradeyle açıklanması" unsurunun zedelendiği,
- Hizmet Koşulları ve Gizlilik İlkesinde yer alan "aktarım"a ilişkin ifadelerin müzakereye kapalı nitelikte sunularak ilgili kişilerin sözleşmeye bir bütün olarak onay vermeye zorlandığı, bu suretle açık rızanın saf dışı bırakılmaya çalışıldığı, uygulamanın kullanılmasının aktarım şartına bağlandığı, veri sorumlusunun bu uygulamasının Kanunun 4'üncü maddesinde yer alan "Hukuka ve dürüstlük kurallarına uygun olma" ilkesine aykırılık teşkil ettiği,
- İşlenen tüm kişisel verilerin aktarımına ilişkin açık rıza istenildiği, ancak bu verilerin işlendikleri amaçla orantılı ve sınırlı bilgiler olmadığı Kanunun 4'üncü maddesinde yer alan "belirli, açık ve meşru amaçlar için işlenme" ve "işlendikleri amaçla bağlantılı, sınırlı ve ölçülü olma" ilkelerine aykırı hareket edildiği,
- WhatsApp tarafından kişisel verilerin işlenmesinin sözleşmenin bir parçası haline getirilmek suretiyle ilgili kişilerden sözleşmeye onay vermelerinin istenildiği ve sonra-

sında "Bir sözleşmenin kurulması veya ifasıyla doğrudan doğruya ilgili olması kaydıyla, sözleşmenin taraflarına ait kişisel verilerin işlenmesinin gerekli olması" ibaresiyle görünen işlem sözleşmeye onay verme olsa da asıl yapılan işlemin kişisel verilerin işlenmesine açık rıza alınması niteliğinde olduğu, bu bakımdan sözleşmenin içerisine derç edilerek hizmetin bir koşulu olarak dayatılması suretiyle alınan açık rızanın, "özgür iradeyle açıklanması" unsurunun zedelendiği,

- Veri sorumlusunun Türkiye'de bulunan ilgili kişilerden elde ettiği kişisel veriler üzerinde, bu verileri elde ettikten sonra yapmış olduğu kaydetme, depolama, değiştirme, aktarma gibi her türlü işleme faaliyetinin, sunucuları Türkiye'de bulunmadığı sürece kişisel verilerin yurt dışına aktarımı anlamına geldiği, dolayısıyla söz konusu aktarımın, Kanunun "Kişisel verilerin yurt dışına aktarılması" başlıklı 9 uncu maddesine uygun olarak yapılmasının zorunluluk arz ettiği ancak veri sorumlusu tarafından aktarım faaliyetleri için hiçbir şekilde açık rızaya başvurulmadığının beyan edildiği, bununla birlikte veri sorumlusunca Kurulumuza bir taahhütname başvurusunda da bulunulmadığı dikkate alındığında, veri sorumlusu tarafından Kanunun 9 uncu maddesine uygun hareket edilmediği,
- Veri sorumlusu tarafından, profilleme amacıyla çerezler aracılığıyla yapılacak kişisel veri işleme faaliyetine ilişkin olarak ilgili kişilerden açık rıza alınmadığı, bu kapsamda yürütülen kişisel veri işleme faaliyetinin de hukuka uygun olmadığı,

tespitleri yapılmıştır.

Nihayetinde Kurul, yukarıda ifade ettiğimiz gerekçeler neticesinde WhatsApp'ın kişisel verilerin hukuka aykırı işlenmesini önlemek için gerekli her türlü teknik ve idari tedbiri almadığını, bu durumun da 18. maddede yer alan veri güvenliğine ilişkin yükümlülüklerin yerine getirilmesine aykırı olduğunu ifade ederek, Whatsapp hakkında 1.950.000 Türk lirası idari para cezasına hükmetmiştir. Bunun yanı sıra Whatsapp; Hizmet Koşulları ve Gizlilik İlkesi metinlerini üç ay içerisinde Kanuna uygun hale getirmekle ve kanuna uygun bir aydınlatma metni hazırlamakla yükümlü kılındı.

Bu ceza WhatsApp'ın veri sorumlusu olarak aldığı tek ceza değil.

İrlanda Veri Koruma Komisyonu (DPC) tarafından 2018 yılında WhatsApp hakkında soruşturma başlatılmıştı. DPC, WhatsApp'ın veri saklama politikasının Avrupa Birliği'nin şeffaflık ilkesine uygun olup olmadığına yönelik araştırmasını tamamladı. İnceleme Whatsapp kullanıcı bilgilerinin Facebook ile paylaşılması dahil, veri politikasının şeffaflığına ilişkin başlatılmıştı. AB Genel Veri Koruma Tüzüğü (GDPR) gereğince; WhatsApp'ın Avrupa Birliği'nin veri gizliliği yasalarını ihlal ettiği ve Facebook'un diğer şirketleriyle kişisel verileri paylaştığı tespit edildi. Soruşturma sonucunda DPC, WhatsApp'a 225 milyon Euro para cezası keserek; faaliyetlerini AB veri kurallarıyla uygun hale getirmesini de istedi.

"Yapay Zekâ Alanında Kişisel Verilerin Korunmasına İlişkin Tavsiyeler" 15.09.2021 Tarihinde, Kişisel Verilerin Korunması Kurumu Resmi İnternet Sitesinde Yayınlanmıştır.

Yapay zekâ alanındaki geliştiriciler, üreticiler, servis sağlayıcılar ve karar alıcıları kapsayan bu dokümanda yapay zekâ uygulamalarında kişisel verilerin korunmasına dair tavsiyeler bulunmaktadır.

"Biyometrik Verilerin İşlenmesinde Dikkat Edilmesi Gereken Hususlara İlişkin Rehber" 16.09.2021 Tarihinde, Kişisel Verilerin Korunması Kurumu Resmi İnternet Sitesinde Yayınlanmıştır.

İlgili rehberde Kişisel Verilerin Korunması Kanunu'nun 6.maddesi ile Avrupa Birliği Genel Veri Koruma Tüzüğünün (GVKT) 4.maddesi ışığında kişisel verilerin biyometrik veri niteliğine haiz olabilmesi için;

- Kişinin fizyolojik, fiziksel veya davranışsal özellikleri gibi ayırt edici özellikleri veri işleme sonucunda ortaya çıkarılmalı,
- Ortaya çıkarılan özellikler kişinin kimliğini tanımlamaya yarayan ya da kişinin kimliğini doğrulayan kişisel veriler olmalıdır.
- "Biyometrik Veri İşleme İlkeleri" başlıklı kısımda, veri sorumlusunun, Kanunun 4.maddesindeki genel ilkeler ve 6.maddesinde düzenlenen şartlara uygun bir şekilde ancak belirli ilkeler doğrultusunda biyometrik verileri işleyebileceğinden bahsedilmiştir.

Bu ilkeler;

a) Temel hak ve özgürlüklerin özüne dokunmaması,
b) Başvurulan yöntemin işleme amacına ulaşılabilmesi bakımından elverişli olması, veri işleme faaliyetinin ulaşılmak istenen amaç için uygun olması,
c) Biyometrik veri işleme yönteminin ulaşılmak istenen amaç bakımından gerekli olması,
d) Veri işlemeyle ulaşılmak istenilen amaç ve aracın arasında orantı bulunması,
e) Gerektiği süre kadar tutulması, gereklilik ortadan kalktıktan sonra söz konusu verilerin gecikmeksizin imha edilmesi,
f) İşleme amacı doğrultusunda sınırlı olmak üzere; veri sorumlularının Kanunun 10.maddesine uygun bir biçimde aydınlatma yükümlülüğünü yerine getirmesi,
g) Açık rızanın gerekmesi halinde ilgili kişilerin açık rızalarının Ka-

nuna uygun şekilde alınmış olmasıdır.

Bu kapsamda;

- Veri sorumlusu tarafından bütün ilkelerin sağlandığı kayıt altına alınıp belgelendirilmelidir.
- Gerekmediği takdirde, biyometrik veri alınırken genetik veri (kan, tükürük vb.) alınmamalıdır.
- Biyometri türünün veya türlerinin seçiminde tercih edilen biyometrik veri türünün veya türlerinin diğerleri yerine neden seçildiğine dair gerekçeler ve belgeler sunulmalıdır.
- Kanunun 4.maddesinin 1.fıkrasının (d)bendinde yer alan ilgili mevzuatta öngörülen veya işlendikleri amaç için gerekli olan süre kadar muhafaza edilme ilkesi gereği, kişisel verilerin işlenmesinde azami süre belirlenmelidir.
- İlgili rehberin "Biyometrik Veri Güvenliği" başlıklı kısmında, Biyometrik veri işleyen veri sorumlularının; kanun, yönetmelik, tebliğ ve kurul kararlarında yer alan kişisel veri güvenliği ile ilgili hususlara dikkat etmelerinin zorunlu olduğu ifade edilmiştir.
- Veri sorumlusunun, verilerinin niteliği ve veri işlemenin ilgili kişi açısından oluşturulacağı muhtemel risklerle ilgili olarak, verilerin güvenliğini sağlamak amacıyla gerekli teknik ve idari tedbirleri almasının gerektiği ifade edilmiştir.

Covıd-19 PCR Test Sonucu ve Aşı Bilgisi Uygulamalarına İlişkin Kamuoyu Duyurusu Kişisel Verilerin Korunması Kurulu İnternet Sitesinde 28.09.2021 Tarihinde Yayınlanmıştır.

Duyuruda, 28.09.2021 tarihli ve 2021/980 sayılı kararında yer alan Covid-19 PCR test sonuç ve aşı bilgilerinin işlenmesine ilişkin değerlendirmeler paylaşılmıştır.

Kişilerin tahlil, görüntüleme, test, rapor, aşı durumu gibi sağlık durumlarına ilişkin bilgileri Kişisel Verilerin Korunması Kanunu'nun 6. maddesine göre kişisel sağlık verisi niteliğine sahip olup özel nitelikli kişisel veri kategorisinde bulunmaktadır. Bu sebeple, söz konusu bilgilerin Kanun'un 6. maddesinde yer verilen işleme şartlarına uygun olarak işlenmesi gerekmektedir. Ancak COVID-19 PCR test sonuçlarının işlenmesi konusu bu kapsam dışında değerlendirilmiştir.

Covid-19 salgınının dünya çapındaki gerek sağlık gerek sosyal hayat gerek ekonomi üzerindeki etkileri dikkate alındığında, bu salgınla mücadele kapsamında aşı durumu ve PCR test sonucu gibi Covid-19'a ilişkin kişisel sağlık verilerinin; kamu sağlığının, kamu güvenliğinin ve kamu düzeninin korunması amacıyla işlenmesi gerekliliği bulunduğu değerlendirilmiştir.

Salgın hastalık gibi kamu güvenliği ve kamu düzenini tehdit eden durumlarda bu tehdidi ortadan kaldırabilmek amacıyla salgın hastalığın bulaşıcılığının önüne geçilebilmesini teminen kanunla yetki verilmiş kamu kurum ve kuruluşlarınca yürütülen faaliyetler kapsamında kişisel verilerin işlenmesinin de Kanunun 28/1/ç maddesi kapsamında de-

ğerlendirilmesi gerektiği görüşü bildirilmiştir. Anılan madde gereğince "*Kişisel verilerin millî savunmayı, millî güvenliği, kamu güvenliğini, kamu düzenini veya ekonomik güvenliği sağlamaya yönelik olarak kanunla görev ve yetki verilmiş kamu kurum ve kuruluşları tarafından yürütülen önleyici, koruyucu ve istihbari faaliyetler kapsamında işlenmesi.*" halinde Kanun hükümleri uygulanmayacaktır.

Bu kapsamda Covid-19'un sebebiyet verdiği salgın hastalığın kamu güvenliği ve kamu düzenini tehdit etmesi sebebiyle hastalığın yayılımını engellemek amacıyla Covid-19 aşı bilgisi ve/veya negatif sonuçlu PCR test bilgisinin işlenmesinin kamu güvenliğini ve kamu düzenini koruma amacına yönelik olarak işlenebileceği değerlendirmesinde bulunmuştur.

İmtiyaz Sahibi	Editör	Yazarlar	İletişim
Av. Duygu Kılıç Çaylı *Kılıç Çaylı & Partners* *Hukuk Ofisi adına*	*Kıvılcım Çaylı*	*Av. Belemir Gencal Doğanöz* *Av. Melis Pülten* *Stj. Av. Deniz Karaduman* *Stj. Av. Kaan Uğursal*	*Mutlukent Mah. Arda Sk. No:9* *Beysukent 06800 Çankaya* *Ankara/TURKİYE*