Ağustos 2021

KVKK KURUL KARARLARI

BERKER BERKER

Yayım Tarihi : 02/08/2021
Karar Tarihi : 18/06/2019
Karar No : 2019/170
Konu Özeti : Bir perakende giyim firmasının kişisel veri ihlali bildirimi

Veri sorumlusunun Kurumumuza intikal eden veri ihlal bildiriminde;

- İhlalin bazı müşterilerin yeni bir hesap açarken kişisel verilerinin yanlışlıkla bir URL üzerinden veri sorumlusunun iç sistemlerine ve çalıştığı bazı üçüncü taraf satıcı/sağlayıcılara aktarılması şeklinde gerçekleştiği ve bu durumun veri sorumlusunun olağan bir denetimi esnasında tespit edildiği,

- Kurumumuza veri ihlaline ilişkin bildirim yapıldığında, veri sorumlusunun iki uygulama analizi sağlayıcısından (analytics provider) verilerin hâlihazırda otomatik olarak silinmiş olduğuna dair teyit aldığı,

- İlk 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) yönlendirildiğinin öğrenildiği (Türkiye'deki ilgili kişilerin bu yedi adet URL'den iki tanesinde gerçekleşen hatadan etkilendiği),

- İhlalden etkilenen ilgili kişi sayısının 44 olduğu,

- İhlalden etkilenen kişi kategorilerinin aboneler/üyeler, müşteriler/potansiyel müşteriler olduğu,

- Şirketin Kurumumuzu muhatap 10.06.2019 tarihli ilk yazısında, ihlalden etkilenen kişisel verilerin, zorunlu alan olan e-posta adresi, doğum tarihi, açık metin şeklinde şifre verilerinin olduğu, ancak zorunlu alan olmayan ad soyad verilerinin de etkilenmiş olabileceği,

- İlgili kişilere 23.07.2019 tarihinde e-posta yoluyla bildirim yapıldığı

ifadelerine yer verilmiştir.

Söz konusu bildirimin incelenmesi neticesinde Kişisel Verileri Koruma Kurulunun 18/06/2019 tarih ve 2019/170 sayılı Kararı ile;

- 01.08.2018 ve 21.10.2018 tarihlerinde gerçekleşen veri ihlallerinin tespitinin yaklaşık bir yıl sonra 02.07.2019 tarihinde yapılmış olmasının, gerçekleştirilen işlemlere dair Şirketin log kaydı/takip alarm sistemlerinin bulunmadığının ya da etkin bir şekilde kullanılmadığının ve Şirket tarafından gerekli kontrollerin yapılmadığının göstergesi olduğu,

- 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

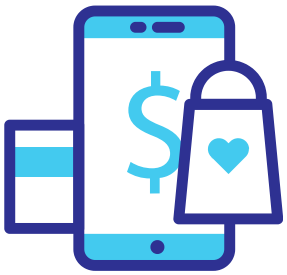
kanaatine varıldığından Web sayfası tasarım aşamasında iken yapılan testlerin yetersiz olması, gerçekleşen işlemlere dair takip/alarm sistemlerinin bulunmamasından kaynaklı ihlal tespitinin geç yapılmış olması sebebiyle, 6698 sayılı Kişisel Verilerin Korunması Kanununun (Kanun) 12 nci maddesinin (1) 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 **50.000 TL idari para cezası uygulanmasına,**

- İhlalin 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 değerlendirildiğinden bu hususta Kanun kapsamında yapılacak bir işlem bulunmadığına

karar verilmiştir.

Yayım Tarihi : 02/08/2021
Karar Tarihi : 11/02/2020
Karar No : 2020/113
Konu Özeti : **Elektronik satış hizmeti sağlayan bir şirketin veri ihlali bildirimi**



Veri sorumlusunun Kurumumuza intikal eden veri ihlal bildiriminde;

- Veri sorumlusu Şirketin e-ticaret sektöründe faaliyet göstermekte olduğu,
- Veri sorumlusunun internet sitesinden ve mobil uygulaması üzerinden ticari faaliyet amacı olmayan satıcılara ikinci el ürünlerini satmaları için bir aracı hizmet sağlayıcısı olarak teknik alt yapı sunduğu,
- Şirkete, internet sitesinin hacklendiği iddiasının iletildiği,
- Veri sorumlusunun personeli tarafından zaman zaman halka açık bağlantıların paylaşıldığı kafe ortamlarından çalışıldığı, ağ dinlemesinin de bu sırada gerçekleşmiş olabileceği,
- Azami 257.000 kişinin etkilenme ihtimalinin bulunduğu ancak veri sorumlusu tarafından 25 kişi dışında kimsenin veri ihlalinden etkilenmiş olduğuna dair kayıt tespit edilmediği,
- İhlalden etkilenen ilgili kişi kategorilerinin kullanıcılar olduğu,
- İhlalden etkilendiği belirtilen kişisel verilerin ad, soyadı, e-posta adresi, kriptolanmış kullanıcı hesabı şifreleri olduğu, 973.147 üyeye kadar olan kullanıcılardan 172.490 adedinin sisteme Facebook profili üzerinden kayıt olduğu için e-posta adreslerinin sistemde bulunmadığı, ancak veri ihlalinin gerçekleştirildiği e-posta adresi ile Şirket arasında yapılan konuşmalarda; tüm veri tabanları, kaynak kodlar, dosya ve müşteri verilerinin ele geçirildiğinin iddia edildiği,
- İhlalden özel nitelikli kişisel verilerin etkilenmediği,
- Kayıtlı kullanıcılara bildirimde bulunulduğu

ifadelerine yer verilmiştir.

Söz konusu bildirimin incelenmesi neticesinde Kişisel Verileri Koruma Kurulunun 11/02/2020 tarih ve 2020/113 sayılı sayılı Kararı ile;

Veri ihlalinden önce veri sorumlusuna ait internet ağı dışında halka açık bağlantıların paylaşıldığı kafe ortamlarından sisteme herhangi bir kısıt bulunmaksızın erişildiği, sızma testlerinin ihlalden sonra yapıldığı, ihlal öncesi sistemlerinde kritik bilgilere erişime neden olabilecek SQL Injection, Cross Site Scripting gibi zafiyetlerin bulunduğu, mobil uygulama içerisine tanımlanmış SSL Sertifikası olmamasından dolayı uygulama trafiğinin rahatlıkla dinlenebildiği, politikaların ve müdahale planlarının ihlal gerçekleştikten sonra oluşturulduğu, veri ihlali gerçekleşmeden önce kurumsal eğitim ve farkındalık faaliyetlerinin düzenlenmediği ve veri ihlalinin ancak veri ihlalini gerçekleştiren kişinin veri sorumlusu ile iletişime geçmesi neticesinde tespit edilebildiği dikkate alınarak 6698 sayılı Kişisel Verilerin Korunması Kanununun (Kanun) 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 **200.000 TL idari para cezası uygulanmasına karar verilmiştir**.

Yayım Tarihi : 02/08/2021
Karar Tarihi : 03/03/2020
Karar No : 2020/201
Konu Özeti : Bir bankanın veri ihlal bildirimi

Veri sorumlusunun Kurumumuza intikal eden veri ihlali bildiriminde;

- İhlalin, şirket müşterilerinin finansman taksit ödemesi tahsilatlarının gerçekleştiğine ilişkin ilgili müşterilere gönderilmesi gereken 905 kişiye ait bildirimin (e-posta ve kısa mesaj) işlem dışı ve Banka sisteminde kayıtlı diğer müşterilere gönderilmesi şeklinde gerçekleştiği,

- İhlalin gerçekleşme şekli ve yöntemi hakkında;

    - Sehven gönderildiği belirtilen bildirimlerin, Şirketin mail ve SMS gönderimleri için kullandığı bir "iç sistem uygulaması" ile yapıldığı,

    - "İç sistem uygulamasında" bir yazılım değişikliğine gidildiği,

    - Ancak geliştirme hatası sebebiyle müştereklik ilişkisi dışındaki ilişki tiplerine sahip müşterilere de sehven bildirim yapıldığı,

    - Teknik anlamda, kullanılması gereken fonksiyon ve metodun doğru kullanıldığı ancak parametrelerde yeterli kontrol konulmadığının anlaşıldığı,

    - "İç sistem uygulaması" üzerinden yapılan geliştirmeyle faydası amaçlanan işlemin gerçekleştiği fakat tüm senaryoların öngörülemediği için amaçlanandan daha fazla müşteriye bildirim yapılmasına sebep olduğu

- İlgili kişilere SMS ve e-posta kanalıyla bilgilendirmenin yapıldığı,

- İhlalden etkilenen kişi sayısının 905; kayıt sayısının 1831 olduğu,

- Etkilenen kişi kategorilerinin müşteriler olduğu,

- İhlalden etkilenen kişisel verilerin kimlik (isim-soy isim), müşteri işlem (cari hesap numarası, finansman hesap numarası, işlem tarihi) ve finans bilgileri (finansman taksit numarası, finansman taksit tutarı, finansman taksit tarihi) olduğu,

ifadelerine yer verilmiştir.
Söz konusu bildirimin incelenmesi neticesinde Kişisel Verileri Koruma Kurulunun 03/03/2020 tarih ve 2020/201 sayılı Kararı ile;

- İhlalin, şirket müşterilerinin finansman taksit ödemesi tahsilatlarının gerçekleştiğine ilişkin, ilgili müşterilere gönderilmesi gereken 905 kişiye ait bildirimin (e-posta ve kısa mesaj) işlem dışı ve Banka sisteminde kayıtlı, diğer müşterilere gönderilmesi şeklinde gerçekleştiği, bunun sonucunda ihlalden ilgili kişilerin; kimlik (isim-soy isim), müşteri işlem (cari hesap numarası, finansman hesap numarası, işlem tarihi) ve finans bilgileri (finansman taksit numarası, finansman taksit tutarı, finansman taksit tarihi) gibi kişisel verilerinin etkilendiği,

- Sehven gönderildiği bildirilen bildirimlerin, veri sorumlusu mail ve SMS gönderimleri için kullandığı bir iç sistem uygulaması ile yapıldığı, ihlale konu olayda teknik anlamda, "kullanılması gereken fonksiyon ve metodun doğru kullanılmasına rağmen parametrelerde yeterli kontrol konulmadığının anlaşıldığı, ilgili geliştirmeyle faydası amaçlanan işlemin gerçekleştiği fakat tüm senaryoların öngörülemediği için amaçlanandan daha fazla müşteriye bildirim yapılmasına sebep olduğu", bu teknik tedbir eksikliğinin de ihlale yol açtığı, bahsi geçen "Notification" uygulama sisteminin hata sonucu veya kasıtlı olarak bozulup bozulmadığını kontrol etmek için yerleştirilen kontrol mekanizmasının yeterli düzeyde olmadığı, bu tip hataların test aşamasında tespit edilerek değişikliklerin yayına alınmadan evvel düzeltilmesi gerektiği

dikkate alındığında, Kanunun 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 **75.000 TL idari para cezasının uygulanmasına,**

- İhlalin 05.07.2019 ile 08.07.2019 arasında gerçekleştiği, 08.07.2019 tarihinde tespit edildiği ve ihlal bildiriminin Kuruma 11.07.2019 tarihinde intikal ettiği, bu kapsamda bildirimin 72 saat içinde gönderildiği, ayrıca veri sorumlusu tarafından ilgili kişilere bildirim yapılmış olduğu

dikkate alındığında, veri sorumlusu hakkında Kanunun 12 nci maddesinin (5) numaralı fıkrası uyarınca yapılacak bir işlem olmadığına

karar verilmiştir.

Yayım Tarihi : 02/08/2021
Karar Tarihi : 07/05/2020
Karar No : 2020/357
Konu Özeti : Bir sigorta şirketinin veri ihlal bildirimi hakkında karar

Veri sorumlusunun Kurumumuza intikal eden veri ihlal bildiriminde;

- Veri sorumlusunun Çağrı Merkezi Birimi tarafından Teftiş Kuruluna; Çağrı Merkezi Satış Temsilcisi olarak dış kaynak sözleşmesi çerçevesinde çalışmakta olan bir çalışanın veri sorumlusunun ana sigortacılık (Cool:Gen) ekranları vasıtasıyla müşterilerin poliçe bilgilerini, portföy takibi için kullandığı yönündeki tereddütlerin iletilmesi üzerine, Teftiş Kurulu Başkanlığınca inceleme yapılmasına karar verilmiş olduğu, bu çalışma çerçevesinde elde edilen bulgular neticesinde ihlalin gerçekleştiğinin anlaşıldığı,

- Veri sorumlusunun yapmış olduğu Teftiş Kurulu incelemesi neticesinde; sistemlerinde tutulmakta olan isim-soyisim, iletişim, plaka bilgilerinin yer aldığı listeyi taşeron çalışanın kendisine atanan kurum e-posta adresinden şahsi e-posta adresine 22.10.2019 ve 24.10.2019 tarihlerinde göndermesi sonucu veri ihlali gerçekleştiğinin tespit edildiği,

- İhlalden etkilenen kişi ve kayıt sayısının 91 olduğu,

- İhlalden etkilenen kişisel veri kategorilerinin müşterilere ait kimlik, iletişim ve risk yönetimi bilgisi (poliçe süreçleri kapsamında elde edilen plaka bilgisi) olduğu,

- Veri sorumlusu nezdinde kullanılan veri sızıntısı önleme uygulamasının, belirli anahtar kelimeleri yakalamak üzere kurgulandığı ancak veri sızıntısına konu olan ihlal, bu anahtar kelimeleri içermediğinden herhangi bir uyarının oluşmadığı,

- Veri ihlal bildiriminin yapıldığı tarih itibariyle ihlal ile ilgili olan çalışanların tamamının kişisel veri koruma eğitimi almadığı, ancak çalışan/taşeron çalışan sayısının fazla olması ve şirketin iş faaliyetlerindeki yoğunluk nedeniyle ve ilgili eğitimler kapsamında azami faydayı sağlayabilmek adına eğitimlerin tek bir seferde tüm çalışanlara bir arada değil de farklı gruplar halinde verilecek şekilde planlandığı, bu nedenle, ilgili sürecin veri sorumlusu çalışanlarının %92'si için tamamlanmış olduğu ve geriye kalan %8 için devam etmekte olduğu

ifadelerine yer verilmiştir.

Söz konusu bildirimin incelenmesi neticesinde Kişisel Verileri Koruma Kurulunun 07/05/2020 tarih ve 2020/357 sayılı Kararı ile;

- Veri sorumlusunun sisteminde tutulmakta olan 91 müşteriye ait isim-soyisim, iletişim, plaka bilgilerinin yer aldığı listeyi taşeron çalışanın kendisine atanan kurum e-posta adresinden şahsi e-posta adresine 22.10.2019 ve 24.10.2019 tarihlerinde göndermesi sonucu veri ihlali gerçekleştiği,

- İhlal kapsamında etkilenen kişisel verilerin veri sızıntısı önleme uygulamasında yakalanmak üzere kurgulanmadığı ve bu sebeple ihlale konu olan e-posta iletiminin anahtar kelimeleri içermediğinden herhangi bir uyarının oluşmadığı, ihlal konusu olan kişisel verilerin veri sızıntısı önleme uygulamasında tanımlanabilir kişisel veriler olduğu dikkate alındığında bu durumun kişisel veri güvenliğine ilişkin doğru ve tutarlı bir prosedürün, veri sorumlusunun çalışma ve işleyişine uygun şekilde entegre edilmediğinin göstergesi olduğu,

- Teftiş Kuruluna; veri sorumlusunun ana sigortacılık ekranlarını kullanarak müşterilerin poliçe bilgilerini portföy takibi için kullanıldığı yönündeki tereddütlerin iletilmesi üzerine yapılan inceleme ile veri ihlalinin, gerçekleşmesinden yaklaşık iki ay sonra ancak tespit edilebildiği ve söz konusu tereddütlerin Teftiş Kuruluna bildirilmemesi durumunda veya tereddütlerin oluşmaması durumunda veri ihlalinin tespit edilemeyeceğinin anlaşıldığı dikkate alındığında alınacak tedbirlerin önceden belirlendiği iyi bir olay yönetiminin kurgulanmadığı ve bu nedenle veri sorumlusunun, Kurumumuzun yayınlamış olduğu “Kişisel Veri Güvenliği Rehberi”nde de belirtildiği üzere bilişim ağlarında sızma veya olmaması gereken bir hareket olup olmadığının takip edilmesi noktasında alınan teknik tedbirler açısından yetersiz kaldığı,

- Veri ihlali öncesinde veri ihlali ile ilgili çalışanların tamamının kişisel veri koruma eğitimi almadığı ve ihlali gerçekleştiren çalışan için de bu eğitiminin atanmış olduğu ancak almadığı dikkate alındığında bu durumun veri sorumlusu Şirketin kişisel veri güvenliğinin sağlanması bakımından yeterli idari tedbirleri almadığının göstergesi olduğu

değerlendirmelerinden hareketle 6698 sayılı Kişisel Verilerin Korunması Kanununun 12 nci maddesinin (1) numaralı fıkrası çerçevesinde veri güvenliğini sağlamaya yönelik gerekli teknik tedbirleri almayan veri sorumlusu hakkında Kanunun 18 nci maddesinin (1) numaralı fıkrasının (b) bendi uyarınca **90.000 TL idari para cezası uygulanmasına,**

- Kurulun 24.01.2019 tarih ve 2019/10 sayılı Kararı ile belirlenen veri ihlalinin öğrenilmesinden itibaren başlayan 72 saatlik süre içerisinde veri sorumlusunun Kurumumuza bildirimde bulunduğu, öte yandan ilgili kişilere gerekli bildirimlerin yapıldığı ve söz konusu bildirim örneklerinin Kurumumuza gönderildiği

dikkate alındığında veri sorumlusu hakkında Kanunun 12 nci maddesinin (5) numaralı fıkrası yapılacak bir işlem bulunmadığına

karar verilmiştir.

Yayım Tarihi : 02/08/2021
Karar Tarihi : 09/07/2020
Karar No : 2020/530
Konu Özeti : Bir bankanın kişisel veri ihlali bildirimi

Veri sorumlusunun Kurumumuza intikal eden veri ihlal bildiriminde;

- Bankanın denetim ekiplerinin aldıkları bir ihbar üzerine yaptığı inceleme sonucunda bir Banka personelinin, 23 adet Banka müşterisinin Türkiye Bankalar Birliği Risk Merkezi (KBB) skorlarını veya TCKN bilgisini 01.01.2019 ile 05.12.2019 tarihleri arasında Whatsapp uygulaması aracılığıyla bir tanıdığı (3. kişi) ile paylaştığının tespit edildiği,

- Personelin 23 Banka müşterisine ait paylaşımlardan menfaat temin ettiğine dair somut bir tespite ulaşılmadığı,

- 19 kişinin KKB, 4 kişinin TCKN, 1 kişinin doğum tarihi, 2 kişinin hesaplarına ilişkin bilgi, 1 kişinin kredi başvurusuna ilişkin bilgi, 23 kişinin isim, soyadı bilgileri olmak üzere toplamda 23 kişiye ait kişisel verilerin ihlalden etkilendiği, özel nitelikli kişisel verilerin etkilenmediği,

- İhlalden etkilenen ilgili kişi gruplarının müşteriler olduğu,

- İhlal ile ilgili olan personelin son bir yıl içerisinde kişisel veri koruma eğitimi aldığı

ifadelerine yer verilmiştir.

Söz konusu bildirimin incelenmesi neticesinde Kişisel Verileri Koruma Kurulunun 09/07/2020 tarih ve 2020/530 sayılı Kararı ile;

- İhlalden 19 kişinin KKB, 4 kişinin TCKN, 1 kişinin doğum tarihi, 2 kişinin hesaplarına ilişkin bilgi, 1 kişinin kredi başvurusuna ilişkin bilgi, 23 kişinin isim, soy isim bilgileri olmak üzere toplamda 23 kişiye ait kişisel verilerin etkilenmiş olduğunun belirtildiği; ancak ihlale sebebiyet veren personelin 01.01.2019-05.12.2019 tarihleri arasında 1.052 kişi için 10.529 adet KKB sorgulaması gerçekleştirdiği,

- Kişi sayısı göz önüne alındığında Kurumumuza gönderilen ekran görüntülerinde yer alan 23 kişiden daha fazla kişinin etkilenmiş olabileceği, söz konusu sorgulama miktarı ile aynı bölgede yer alan diğer personeller içerisinde kişinin 1. sırada olduğu, personelin bu husus ile ilgili makul bir açıklamasının olmadığı, veri sorumlusu tarafından da personelin müşterilere ilişkin bilgileri Banka dışına sızdırmış olabileceği yönünde şüphe oluştuğu,

- İhlal öncesinde veri sorumlusu tarafından personelin KKB sorgularının sınırlandırılmadığı,

- İhlale sebebiyet veren kişinin bölge ortalamasından oldukça yüksek miktarda sorgulama yapması hususunun incelenmemesi ve durumun ihlalin başlangıç tarihinden yaklaşık 1 yıl sonra ihbar sonucu öğrenildiği göz önüne alındığında yeterince denetim ve gözetim yapılmadığı,

- Veri sorumlusunca gerçekleştirilen "Kişisel Verilerin Korunması Kanunu Eğitimi"nin yeterli olmadığı

kanaatine varıldığından Kanunun 12 nci maddesinin (1) numaralı fıkrası hükmü çerçevesinde veri güvenliğini sağlamaya yönelik gerekli teknik ve idari tedbirleri almayan veri sorumlusu hakkında kabahatin haksızlık içeriği, veri sorumlusunun kusuru ve ekonomik durumu da göz önünde bulundurularak Kanunun 18 inci maddesinin (1) numaralı fıkrasının (b) bendi uyarınca **200.000 TL idari para cezasının uygulanmasına** karar verilmiştir.

Yayım Tarihi : 02/08/2021
Karar Tarihi : 22/07/2020
Karar No : 2020/567
Konu Özeti : Bir oyuncak şirketinin veri ihlal bildirimi

Veri sorumlusunun Kurumumuza intikal eden veri ihlal bildiriminde;

- Kötü niyetli kullanıcılar tarafından, başka internet sitelerinden elde edilen kullanıcı adı ve şifrelerin, veri sorumlusunun internet sitesinde yer alan "Üye Girişi" sekmesinde denenerek 29 adet müşterinin hesabına yetkisiz erişim gerçekleşmesi suretiyle meydana geldiği,

- İhlalden etkilenen kişisel verilerin 29 müşteriye ait ad, soyad, e-posta adresi, telefon numarası, kayıtlı adres, müşteri işlem kategorisinde daha önce satın alınan ürün bilgilerinin olduğu,

- Markaya ilişkin kurulmuş olan uyarılar doğrultusunda herhangi bir sitede markanın kullanılması halinde, Şirketin Bilgi İşlem Departmanına bir bildirim düştüğü ve bu bildirim ile adı geçen siteye yönlendirme yapılmakta olduğu,

- Şirkete ulaşan bir bildirim doğrultusunda bir internet sitesinde, veri sorumlusunun markasına ait 29 adet hesap ile ilgili bir içerikle karşılaşıldığı,

- Söz konusu içeriğe erişimin, ancak ilgili siteye üye olunduğu takdirde sağlanabildiği,

- Söz konusu internet sitesi yöneticilerine bir ihtar gönderilerek internet sitesinde yer alan ihlale konu sayfanın kaldırılmasının sağlandığı

ifadelerine yer verilmiştir.

Söz konusu bildirimin incelenmesi neticesinde Kişisel Verileri Koruma Kurulunun 22/07/2020 tarih ve 2020/567 sayılı Kararı ile;

- Kişisel hesaplara erişim hususunda veri güvenliğinin sağlanması amacıyla kullanıcı kimliklerinin doğrulanması gerekmekte olup veri sorumlusunun veri ihlali öncesinde alması gereken güvenlik önlemlerinden olan iki faktörlü kimlik doğrulama yöntemini (SMS/Captcha) veri ihlali sonrasında yayına almayı planladığı dikkate alındığında veri sorumlusunun veri güvenliğini sağlamaya yönelik gerekli teknik tedbirleri almadığı,

- İhlalden etkilenen ilgili kişilerin hesaplarının şifreleri incelendiğinde müşteriler tarafından kullanılan şifrelerin sadece rakamlardan ya da sadece harf dizilerinden oluşabildiği, müşterilere hesap açılırken müşterilerin güçlü şifre oluşturması için zorlanmadığı,

- Veri sorumlusu nezdinde gerçekleşen ihlal sırasında web uygulama güvenlik duvarının (WAF) yetkisiz erişim işlemini saldırı ya da normal kullanıcı girişi olup olmadığını tespit edene kadar saldırganların belli bir miktarda hesaba yetkisiz erişim sağlayabildiği dikkate alındığında veri sorumlusunun uygulama güvenliğini sağlayamadığı

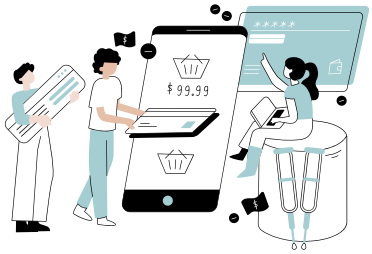
hususları dikkate alındığında 6698 sayılı Kişisel Verilerin Korunması Kanununun (Kanun) 12 nci maddesinin (1) numaralı fıkrası çerçevesinde veri güvenliğini sağlamaya yönelik gerekli teknik tedbirleri almayan veri sorumlusu hakkında Kanunun 18 nci maddesinin (1) numaralı fıkrasının (b) bendi uyarınca **75.000 TL idari para cezası uygulanmasına,**

- Kurulun 24/01/2019 tarih ve 2019/10 sayılı Kararı ile belirlenen veri ihlalinin öğrenilmesinden itibaren başlayan 72 saatlik süre içerisinde veri sorumlusunun bildirimde bulunmadığı; ancak yaşanan 1 günlük bir gecikmenin pandemi süreci nedeniyle makul olduğuna ve bu çerçevede veri sorumlusu hakkında yapılacak bir işlem bulunmadığına,

- İlgili kişilere yapılan bildirimin 18/09/2019 tarih ve 2019/271 sayılı Kurul Kararının gerekliliklerini tam anlamıyla karşılamadığı dikkate alındığında, veri sorumlusunun Kişisel Verileri Koruma Kurulunun 18/09/2019 tarih ve 2019/271 sayılı Kararına uygun bir şekilde ilgili kişilere ihlale ilişkin bildirim yapması hususunda talimatlandırılmasına

karar verilmiştir.

Yayım Tarihi : 02/08/2021
Karar Tarihi : 17/09/2020
Karar No : 2020/715
Konu Özeti : Bir e-ticaret şirketinin veri ihlal bildirimi



Veri sorumlusunun Kurumumuza intikal eden veri ihlal bildiriminde;

- İhlalin, kaynağı ve zamanı tahmin edilemeyen şekilde internet üzerinde ifşa olmuş kullanıcı e-posta adresleri ve şifrelerinin, veri sorumlusunun internet sitesinin giriş ekranında, robot bir uygulama vasıtasıyla denenmesi şeklinde gerçekleştiği,

- İhlalin, veri sorumlusunun bilgi güvenliği ekibi tarafından, olayın gerçekleştiği gecenin sabahı, mesai başlangıcında yapılan rutin kontroller sırasında tespit edildiği, müteakiben vaka hakkında detaylı araştırma başlatıldığı,

- İhlalden etkilenen kişi ve kayıt sayısının 832 olduğu,

- İhlalle ilişkili 832 hesabın kullanıcısına e-posta aracılığıyla bildirimde bulunulduğu, bildirimlerin, olaya ilişkin inceleme ve tespitler tamamlandıktan sonra derhal yapıldığı,

- İhlale konu olan platformun işleyişi kapsamında, giriş yapmak isteyen kullanıcıların e-posta ve şifrelerini girerek ilk olarak ana ekrana, bu ana ekranı geçtikten sonra da üyelik hesaplarının bulunduğu ekranlara ulaşabildiği

ifadelerine yer verilmiştir.

Söz konusu bildirimin incelenmesi neticesinde Kişisel Verileri Koruma Kurulunun 17/09/2020 tarih ve 2020/715 sayılı Kararı ile;

- Veri sorumlusu tarafından her ne kadar bahsi geçen e-posta adreslerinin ve şifrelerinin internet sitesi üzerinden ele geçirilmediği ve ihlalden etkilenen herhangi bir kimlik, iletişim veya müşteri işlem bilgisinin bulunmadığı belirtilse de ilgili kişilerin hesaplarına yetkisiz kişilerce erişimde bulunulduğu, kişisel verilerin gizliliğinin bozulduğu ve söz konusu durumun da veri ihlali oluşturduğu,

- Veri sorumlusunun aynı IP adresinden başarısız oturum açma girişim sayısının veri ihlalinden sonra sınırlandırıldığı, bahsi geçen sınırlandırma tedbirini önceden almış olması halinde internet ortamında sıkça rastlanan saldırı neticesinde ihlalin gerçekleşmesinin önlenebileceği ya da ihlalin etkisinin azaltılabileceği, bunun da veri sorumlusunun veri ihlali öncesinde veri güvenliğini sağlamaya yönelik alması gereken teknik tedbirleri yeterli ve gerekli düzeyde almadığının göstergesi olduğu,

- İhlalden 832 kişiye ait e-posta adresi ve şifre bilgilerinin etkilenmiş olduğunun beyan edildiği,

- Veri sorumlusu tarafından kullanıcıların belirli zaman aralıklarında şifrelerini değiştirmelerinin sağlanmadığı,

- “Web uygulaması güvenlik duvarı” [WAF (Web Application Firewall)] üzerinde aynı IP ile başarılı oturum açma işleminin engellenmesi kural tanımının veri ihlali gerçekleşmeden önce alınması gerekirken veri ihlalinin gerçekleşmesinden sonra alındığı,

- İhlale konu olayda ilgili kişiler önemli bir zarara uğramamış olsa da bahsi geçen internet sitesinin kullanım düzeyi ve içerisinde yer alan kişisel veriler düşünüldüğünde veri sorumlusunun ilgili tedbirleri almamasının ihlal sonucunda potansiyel tehdit açısından ciddi bir risk taşıdığı

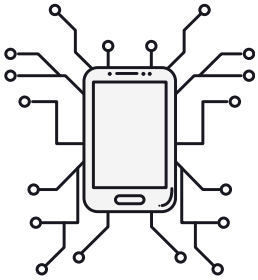
değerlendirmelerinden hareketle; 6698 sayılı Kişisel Verilerin Korunması Kanununun (Kanun) 12 nci maddesinin (1) numaralı fıkrası çerçevesinde veri güvenliğini sağlamaya yönelik gerekli teknik ve idari tedbirleri almayan veri sorumlusu hakkında kabahatin haksızlık içeriği, veri sorumlusunun kusuru ve ekonomik durumu da göz önünde bulundurularak Kanunun 18 nci maddesinin (1) numaralı fıkrasının (b) bendi uyarınca **165.000 TL idari para cezası uygulanmasına,**

- İhlalin 17.12.2019 tarihinde gerçekleştiği, 17.12.2019 tarihinde tespit edildiği ve 20.12.2019 tarihinde Kurumumuza bildirildiği dikkate alındığında Kanunun 12 inci maddesinin (5) numaralı fıkrası kapsamında Kurulun 24/01/2019 tarih ve 2019/10 sayılı Kararı ile belirlenen veri ihlalinin öğrenilmesinden itibaren başlayan 72 saatlik süre içerisinde veri sorumlusunun bildirimde bulunduğu, öte yandan veri sorumlusu tarafından ilgili kişilere bildirim yapıldığı

dikkate alındığında, veri sorumlusu hakkında Kanunun 12 nci maddesinin (5) numaralı fıkrası kapsamında yapılacak bir işlem bulunmadığına

karar verilmiştir.

Yayım Tarihi : 02/08/2021
Karar Tarihi : 22/10/2020
Karar No : 2020/816
Konu Özeti : Bir teknoloji şirketinin veri ihlal bildirimi



Veri sorumlusunun Kurumumuza intikal eden veri ihlal bildiriminde;

- İhlalin, mağazada yapılan bir alışveriş sonrasında adına e-fatura düzenlenen müşterinin sistemde kayıtlı e-posta adresine ilgili faturanın gönderilmesi neticesinde bu faturanın aynı ad ve soyada sahip farklı bir müşteriye ulaşması neticesinde gerçekleştiği,

- CRM sistemi üzerinde adına fatura düzenlenen müşterinin telefon numarasının aynı ad ve soyada sahip iki farklı müşteri adına oluşturulduğu ve kayıtlarda her ikisinde de yer aldığı,

- Bu durumun kişilerin GSM-1 ve GSM-2 olarak oluşturulan kayıtları arasına aynı telefon numarasının bir müşteri için GSM-1, diğer müşteri için GSM-2 olarak kaydedilmiş olması nedeniyle fatura gönderiminde hatalı e-posta adresine ulaşılması nedeniyle meydana geldiği,

- 15.10.2020 tarihinde kişisel verileri ihlal edilen müşteri ile aynı ad ve soyada sahip müşterinin müşteri hizmetlerini arayarak kendisine iletilmiş olan e-mailde yer alan faturanın kendisine ait olmadığı bilgisini vermesi üzerine sistem üzerinden kontroller gerçekleştirilerek ihlalin tespit edildiği,

- Kayıtlarda meydana gelen karışıklığın mağazadaki kayıt aşamasında hatalı bilgi girişinden mi yoksa CRM sistemindeki veri tekilleştirme özelliğinden mi kaynaklandığına ilişkin araştırmaların sürdüğü,

- İhlalin hemen ardından müşteri kayıtlarının sistem üzerinden düzeltildiği, hatalı faturanın diğer müşteriden geri alınmasının sağlandığı ve doğru bilgilerle doğru kişiye fatura düzenlendiği,

- İhlalden etkilenen kişisel verilerin; müşterinin adı soyadı, T.C. Kimlik Numarası, cep telefonu numarası ve fatura bilgileri olduğu,

- İhlal edilen kişisel verilerin olumsuz etki doğurması yüksek olmayan kişisel veriler olduğu ve aynı zamanda ihlalin etkisinin azaltılması amacıyla ilgili kişiye bildirim yapılması ve sehven gönderilen e-postanın silinmesi gibi gerekli işlemlerin gerçekleştirildiği,

- İhlalin 15.10.2020 tarihinde gerçekleştiği ve 16.10.2020 tarihinde tespit edildiği,

- İhlalden etkilenen kişi sayısının 1; kayıt sayısının 4 olduğu,

- İlgili kişiye telefon görüşmesi ile bildirim yapıldığı

ifadelerine yer verilmiştir.

Söz konusu bildirimin incelenmesi neticesinde Kişisel Verileri Koruma Kurulunun 22/10/2020 tarih ve 2020/816 sayılı Kararı ile;

- İhlalden 1 kişiye ait kişisel verilerin etkilendiği,
- İlgili kişiye telefon yoluyla bildirim yapıldığı,
- İhlale konu kişisel verilerin ilgili kişi üzerinde olumsuz etki doğurma olasılığının düşük olduğu,
- İhlale konu e-postanın silinmesinin sağlandığı,
- Veri sorumlusunun ihlale kısa zamanda müdahale ettiği

hususları dikkate alındığında, bu aşamada veri sorumlusu hakkında 6698 sayılı Kişisel Verilerin Korunması Kanununun 12 nci maddesi kapsamında **yapılacak bir işlem olmadığına karar verilmiştir.**

Yayım Tarihi : 02/08/2021
Karar Tarihi : 08/12/2020
Karar No : 2020/935
Konu Özeti : **Bir sigorta şirketinin kişisel veri ihlali bildirimi**

Veri sorumlusunun Kurumumuza intikal eden veri ihlal bildiriminde;

- Sağlık yenileme talebinde bulunan bir müşteriye, Müşteri İletişim Merkezi (Çağrı Merkezi) tarafından sehven başka bir müşterinin poliçe muafiyet bildirimi bilgisinin iletildiği,
- Dolayısıyla gerçek kişiye ait sağlık verisinin, konunun tarafı olmayan başka bir müşteri ile paylaşıldığı,
- Veri Kaybı Önleme Sistemi (DLP) düzenli kontrolleri sırasında, sistemi kontrol eden görevli tarafından veri ihlalinin tespit edildiği ve ilgili birimlere aksiyon alınması için iletildiği,
- Veri ihlalinden kimlik, iletişim ve sağlık kategorilerindeki kişisel verilerin etkilendiği,
- Sehven iletilen poliçe muafiyet bildiriminde, ilgili kişinin sağlık poliçesi kapsamında olmayan rahatsızlıklarının belirtildiği,
- Bu rahatsızlıkların poliçe muafiyetinin, ilgili kişinin bu rahatsızlıklara sahip olması veya sahip olduğu şüphesi olması sebebiyle yazıldığından, ilgili kişinin sağlık verisinin işlendiği,
- Veri ihlalinden veri sorumlusu müşterisi olan 1 kişinin etkilendiği,
- Veri sorumlusunun Müşteri İletişim Merkezi çalışanlarının müşteriyle direkt temasta olduklarından dolayı düzenli eğitimlere tabi olduğu

ifadelerine yer verilmiştir.

Söz konusu bildirimin incelenmesi neticesinde Kişisel Verileri Koruma Kurulunun 08/12/2020 tarih ve 2020/935 sayılı sayılı Kararı ile;

- İhlalden 1 kişinin etkilendiği,
- İhlalden etkilenen kişisel verilerin kimlik, iletişim ve sağlık bilgileri olduğu,
- Veri sorumlusunun “en kısa sürede” (24.01.2019 tarih ve 2019/10 sayılı Kurul kararında belirtilen 72 saatlik süre içerisinde) Kurumumuza veri ihlalini bildirme yükümlülüğünü yerine getirdiği,
- İlgili kişilere ihlale ilişkin 03.12.2020 tarihinde bildirim yapılacağının belirtildiği

hususları dikkate alındığında veri sorumlusu hakkında 6698 sayılı Kişisel Verilerin Korunması Kanununun 12 inci maddesi kapsamında bu aşamada yapılacak bir işlem bulunmadığına, öte yandan veri sorumlusu tarafından ilgili kişiye bildirim yapılması ve söz konusu bildirimin yapıldığı ile bahse konu verilerin sehven gönderilen müşteri nezdinde silindiğine dair tevsik edici belgelerin **Kurumuza iletilmesi hususunda talimatlandırılmasına karar verilmiştir.**

Yayım Tarihi : 02/08/2021
Karar Tarihi : 15/12/2020
Karar No : 2020/957
Konu Özeti : Bir ilaç şirketinin veri ihlal bildirimi

Veri sorumlusunun Kurumumuza intikal eden veri ihlal bildiriminde;

- İhlalin güvenlik seviyesini artırmak amacıyla yeni bir sunucuya geçiş sürecinde sunucu parametreleri optimize edilmediği için aylık maaş bordrosu bildirimlerinin e-posta yoluyla bildirilmesinde sistemsel bir hata meydana gelmesi ile oluştuğu,

- Sistem tarafından otomatik olarak oluşturulan ve güncel maaş bordrolarını içeren e-postalarda meydana gelen hata nedeniyle, 337 çalışanın bordrosunun yanlış çalışanlara gönderildiği,

- İhlalin yanlış bordro giden bir çalışanın e-posta yoluyla İnsan Kaynakları Departmanına bilgi vermesi sonucu anlaşıldığı,

- İhlalin 27.11.2020 tarihinde gerçekleştiği ve aynı gün tespit edildiği,

- Teknik eşleştirme hatası nedeniyle çalışanın aylık bordrosuna, başka bir çalışan tarafından erişilebilmesinin mümkün olduğu,

- Bordroların, çalışanın o ayki maaş bilgisi ve ad- soyad, banka hesap numarası ve T.C. kimlik numarası gibi kişisel veriler içerdiği,

- İhlalden etkilenen kişi sayısının 337; kayıt sayısının 1348 olduğu

ifadelerine yer verilmiştir.

Söz konusu bildirimin incelenmesi neticesinde Kişisel Verileri Koruma Kurulunun 15/12/2020 tarih ve 2020/957 sayılı Kararı ile;

- İhlalin, gerçekleşmesinden 13 dakika sonra tespit edildiği, gerçekleşmesinden 2 saat sonra ise sonlandırıldığı,

- İhlalin, güvenlik seviyesini arttırmak amacıyla yeni bir sunucuya geçiş sürecinde oluştuğu,

- İhlal veri sorumlusunun çalışanlarının bordro bilgilerinin diğer çalışanlara gönderilmesi şeklinde gerçekleştiğinden olumsuz etki doğurma olasılığının düşük olduğu,

- İhlale sebep olan e-postaların silinmiş olduğu ve e-postaların gönderildiği kişilere gerekli uyarının yapıldığı,

- İhlale sebep olan konuda ihlal sonrası gerekli teknik ve idari tedbirlerin alındığı

dikkate alındığında Kanunun 12 inci maddesinin (1) numaralı fıkrası kapsamında veri sorumlusu hakkında bu aşamada yapılacak bir işlem olmadığına,

- İhlalin tespit tarihinden sonra 72 saat içinde Kurula bildirilmemiş olduğu dikkate alındığında, Kanunun 12 nci maddesinin (5) numaralı fıkrası uyarınca işlenen verilerin kanuni olmayan yollarla başkaları tarafından elde edilmesi halinde en kısa sürede ilgilisine ve Kurula, Kişisel Verileri Koruma Kurulunun 18.09.2019 tarih ve 2019/271 sayılı Kararına uygun olarak bildirimde bulunması hususunda daha dikkatli olunması, ayrıca ilgili kişilere bildirim yapıldığına ve e-postanın gönderildiği kişilere e-postanın silinmesi yönünde uyarının yapıldığına ilişkin tevsik edici belgelerin **Kurumumuza gönderilmesi hususlarında veri sorumlusunun talimatlandırılmasına**

karar verilmiştir.

Yayım Tarihi : 02/08/2021
Karar Tarihi : 20/05/2020
Karar No : 2021/511-512-513
Konu Özeti : **Avukatların icra takip dosyalarındaki kişisel verilere vekâletname olmaksızın hukuka aykırı olarak erişim sağlaması ve Adalet Bakanlığı tarafından icra tevzi bürolarında görevli personel eliyle alacaklı vekili avukatlara borçluların alacaklı olduğu icra takip dosyalarında bulunan kişisel verilerin hukuka aykırı olarak aktarılması.**

Adalet Bakanlığı ve bir avukat hakkında Kuruma intikal ettirilen ihbarlarda özetle; alacaklı vekili avukatların, icra tevzi bürolarına başvuruda bulunup borçluların alacaklı olduğu icra takip dosyalarının bilgilerini haksız bir şekilde elde ettiği, ayrıca avukatların bu sayede, icra dairesinde diledikleri dosyaları da inceleyebildiği, her ne kadar avukatın dosyanın bir örneğini alması vekâlet sunmasına bağlı olsa da kişisel verilere yetkisiz kişilerin erişiminin engellenmesinin veri sorumlularına verilen görevlerden biri olduğu ve avukatlar ya da görevlendirdikleri kişiler tarafından, icra tevzi bürosu yetkilileri ve memurları aracılığıyla; borçluların alacaklı olduğu icra takip dosyalarında bulunan kişisel verilerin hukuka aykırı olarak ele geçirilmesi ile avukatların icra dairelerindeki diledikleri dosyaları vekâletname olmaksızın incelemelerinin 6698 sayılı Kişisel Verilerin Korunması Kanununa aykırılık teşkil ettiği belirtilerek; bu kapsamda icra tevzi bürosu çalışanları tarafından yapılan aktarımların ve avukatlar tarafından vekâletname olmaksızın icra takip dosyalarındaki kişisel verilere erişimin 6698 sayılı Kanuna aykırı olduğunun tespit edilmesi, bu durumun düzeltilmesi için Adalet Bakanlığı nezdinde ivedilikle girişimlerde bulunulması ve gerekli idari yaptırımların uygulanması talep edilmiştir. Yapılan ihbarlara binaen Kişisel Verileri Koruma Kurulu tarafından resen inceleme başlatılmasına karar verilmiştir.

Başlatılan inceleme çerçevesinde veri sorumlusu Adalet Bakanlığından konuya ilişkin bilgi ve belge talep edilmiş olup, alınan cevabi yazıda özetle;

- İlgili mevzuat ve içtihat çerçevesinde, alacağını tahsil etmek isteyen alacaklı veya vekilinin takibin kesinleşmesini müteakip borçlunun alacaklı olduğu dosyalar da dâhil olmak üzere borçlunun her türlü mal varlığını, hak ve alacağını sorgulama hakkının 2004 sayılı İcra ve İflas Kanunundan kaynaklandığının anlaşıldığı;

- Ayrıca avukatın veya stajyerlerinin dava takip dosyalarını vekâletname olmaksızın inceleme isteğinin ilgililerce yerine getirilmesinin 1136 sayılı Avukatlık Kanununda düzenlendiği; bu kapsamda avukatların ve stajyerlerinin alacağın tahsilini teminen borçlunun alacaklı olduğu dosyaları sorgulama ve kendilerine tanınan dosya inceleme hakkını icra dairelerinde tespit amacıyla bu işle görevlendirilen icra tevzi büroları vasıtası ile yapmasının uygun olacağının, icra dairesinde görevli personelin de vekâletname ibraz etmeksizin dosya incelemek isteyen avukat ve stajyerlerine bu isteklerini yerine getirmelerinin fotokopi ve benzeri yollarla örnek almamaları kaydı ile zorunlu olduğunun değerlendirildiği;

- Bu itibarla avukat veya stajyerlerinin müvekkillerinin alacağına kavuşmasını sağlamak için borçluların alacaklı olduğu dosyaları tespit etmesi ve tespit ettiği dosyaları incelemesi hususunun kanunlarda açıkça öngörülmesi ve yukarıda izah edilen nedenlerle 6698 sayılı Kanuna aykırılık kapsamında bulunmayacağının değerlendirildiği

ifade edilmiştir.

Yine, başlatılan inceleme çerçevesinde veri sorumlusu avukattan savunması istenilmiş olup, alınan cevabi yazıda özetle; *Avukatlık Kanununun 46 ncı maddesinin 2 inci fıkrasında yer alan "Avukat veya stajyer, vekaletname olmaksızın dava ve takip dosyalarını inceleyebilir. Bu inceleme isteğinin ilgililerce yerine getirilmesi zorunludur."* hükmü sınırları kapsamında borçlunun alacaklı olduğu dosyaların tespit edildiği, bu dosyalara borçlunun alacaklı olduğu icra dosyalarından talepte bulunmak ve ilgili icra müdüründen karar aldırmak suretiyle haciz işlemi yapıldığı; bunun göreviyle ilgili bir iş olduğu; bu işlemlerin yapılmaması halinde işini gereği gibi yapmadığı için müvekkiline karşı sorumluluğun dahi gündeme geleceği ve bu kapsamda tüm işlemlerin yasalar çerçevesinde yürütüldüğü ifade edilmiştir.

İhbar başvuruları ile veri sorumlularından alınan bilgi ve belgelerin ilgili mevzuat çerçevesinde incelenmesi neticesinde Kurulun 20/05/2021 tarihli ve 2021/511-512-513 sayılı Kararları ile

- 2004 sayılı İcra ve İflas Kanununun *"Taşınır ve taşınmaz malların haczi"* başlıklı 85 inci maddesinin birinci fıkrasının *"Borçlunun kendi yedinde veya üçüncü şahısta olan taşınır mallariyle taşınmazlarından ve alacak ve haklarından alacaklının ana, faiz ve masraflar da dahil olmak üzere bütün alacaklarına yetecek miktarı haczolunur. "* hükmünü amir olduğu; hükümde haciz yoluyla takip kapsamında borçlunun taşınır ve taşınmaz malları ile alacak ve haklarına haciz konulabileceğinin öngörüldüğü ve bu kapsamda, borçlunun alacaklı olduğu icra dosyalarına konu alacaklara da haciz konulmasının mümkün olduğu;

- Diğer taraftan, 1136 sayılı Avukatlık Kanununun 46 ncı maddesinin,

"İşlerin stajiyer veya sekreterle takibi, dava dosyalarının incelenmesi ve dosyadan örnek alma:

Madde 46 – (Değişik : 2/5/2001 - 4667/32 md.)

Avukat, işlerini kendi sorumluluğu altındaki stajyeri veya yanında çalışan sekreteri eliyle de takip ettirebilir, fotokopi veya benzeri yollarla örnek aldırabilir. Avukatın onanmasını istemediği örnekler harca tabi değildir.

Avukat veya stajyer, vekaletname olmaksızın dava ve takip dosyalarını inceleyebilir. Bu inceleme isteğinin ilgililerce yerine getirilmesi zorunludur. Vekaletname ibraz etmeyen avukata dosyadaki kağıt veya belgelerin örneği veya fotokopisi verilmez." hükmünü,

2 nci maddesinin üçüncü fıkrasının ise,

“Avukatlığın amacı:

Madde 2 – (Değişik birinci fıkra : 2/5/2001 - 4667/2 md.) …

(Değişik üçüncü fıkra: 2/5/2001 - 4667/2 md.) Yargı organları, emniyet makamları, diğer kamu kurum ve kuruluşları ile kamu iktisadi teşebbüsleri, özel ve kamuya ait bankalar, noterler, sigorta şirketleri ve vakıflar avukatlara görevlerinin yerine getirilmesinde yardımcı olmak zorundadır. Kanunlarındaki özel hükümler saklı kalmak kaydıyla, bu kurumlar avukatın gerek duyduğu bilgi ve belgeleri incelemesine sunmakla yükümlüdür. Bu belgelerden örnek alınması vekaletname ibrazına bağlıdır. Derdest davalarda müzekkereler duruşma günü beklenmeksizin mahkemeden alınabilir.” hükmünü amir olduğu;

- *Anılan hükümlerden avukatların vekâletname sunmasına gerek olmaksızın icra takip dosyalarını inceleyebileceğinin ve ilgili makamların da avukatlara bu konuda gerekli imkanları sağlamakla yükümlü kılındığının anlaşıldığı;*

- *Bununla birlikte, 2004 sayılı İcra ve İflas Kanununun 8/a maddesinin altıncı fıkrası ile 22.07.2020 tarihli ve 7251 sayılı Kanunla değişik 78 nci maddesinin birinci fıkrasının;*

“Elektronik işlemler:

Madde 8/a – (Ek: 2/7/2012-6352/3 md.)

…
(Ek fıkra:6/12/2018-7155/10 md.) Alacaklı, Ulusal Yargı Ağı Bilişim Sistemi üzerinden bu sisteme entegre bilişim sistemleri vasıtasıyla dosya safahat bilgileri ile borçlunun mal, hak veya alacağını elli kuruş karşılığında sorgulayabilir. Bu miktar her yıl, bir önceki yıla ilişkin olarak 4/1/1961 tarihli ve 213 sayılı Vergi Usul Kanununun mükerrer 298 inci maddesi hükümleri uyarınca tespit ve ilan edilen yeniden değerleme oranında artırılır. Adalet Bakanlığı yeniden değerleme oranında artırılan ücreti beş katına kadar artırmaya ve azaltmaya ayrıca gün ve dosya esaslı olmak üzere belirli sayıdaki sorgulamayı ücretten istisna tutmaya yetkilidir. Genel yönetim kapsamındaki kamu idarelerinden bu ücret alınmayacağı gibi alacaklının bir gün içinde aynı dosya üzerinden beş kez yapacağı sorgudan da ücret alınmaz. Bu kapsamda alınacak ücret Adalet Bakanlığının belirleyeceği usule göre tahsil edilir ve takip gideri olarak borçluya yüklenemez.

…
II. HACİZ

Haciz:

1 – Talep Müddeti,

Madde 78 – (Değişik: 3/7/1940-3890/1 md.)

(Değişik birinci fıkra:22/7/2020-7251/49 md.) Ödeme emrindeki müddet geçtikten ve borçlu itiraz etmiş ise itirazı kaldırıldıktan sonra mal beyanını beklemeksizin alacaklı, haciz konmasını isteyebilir. Ancak, alacaklı dilerse haciz talebinde bulunmaksızın Ulusal Yargı Ağı Bilişim Sistemi üzerinden, bu sisteme entegre bilişim sistemleri vasıtasıyla borçlunun mal, hak veya alacağını sorgulayabilir. Sorgulama sonunda Ulusal Yargı Ağı Bilişim Sistemi, varsa borçlunun mal, hak veya alacağının mahiyeti ve detayı hakkında bilgi verir ve bu durumda sistem üzerinden de haciz talep edilebilir. Bu takdirde icra dairesi, tespit edilen mal, hak veya alacağı elektronik ortamda haczeder. Sorgulama sonunda edinilen bilgiler hukuka aykırı olarak paylaşılamaz. Sorgulama ve haciz işlemlerinin yürütülebilmesi için kamu kurum veya kuruluşları ile 19/10/2005 tarihli ve 5411 sayılı Bankacılık Kanununun 3 üncü maddesinde tanımlanan kredi kuruluşları ve finansal kuruluşlar, Ulusal Yargı Ağı Bilişim Sistemi ile kendi sistemleri arasında entegrasyonu sağlar. Sorgulamanın tür, kapsam ve sınırı ile diğer hususlar Adalet Bakanlığınca yürürlüğe konulan yönetmelikle belirlenir.””

şeklinde olduğu;

- Söz konusu hükümler uyarınca alacaklı vekili avukatların, Ulusal Yargı Ağı Bilişim Sistemi üzerinden borçlunun alacaklı olduğu icra dosyaları dahil olmak üzere mal, hak veya alacağı hakkında sorgulama yapabileceği;

değerlendirmelerinden hareketle;

- *2004 sayılı İcra ve İflas Kanununun 85 inci maddesi çerçevesinde borçlunun kendi veya üçüncü kişi nezdindeki alacaklarına haciz konulabileceği, 2004 sayılı Kanunun 8/a ve 78 nci maddeleri uyarınca Ulusal Yargı Ağı Bilişim Sistemi vasıtasıyla alacaklı tarafından borçluların mal, hak veya alacaklarının sorgulanabileceği, avukatların müvekkillerinin alacağını tahsil etmek amacıyla 1136 sayılı Avukatlık Kanununun 46 ncı maddesi uyarınca dava ve icra takibi dosyalarını vekâletname sunmaksızın inceleyebileceği ve bu kapsamda 6698 sayılı Kanunun 5 inci maddesinin ikinci fıkrasının (a) bendinde düzenlenmiş işlemenin “kanunlarda açıkça öngörülmesi” şartına dayanılarak alacaklı vekili avukatlar tarafından borçlunun alacaklı olduğu icra dosyalarına ilişkin olarak kişisel veri işleme faaliyeti yürütebileceğinden avukatların vekâletname olmaksızın icra takip dosyalarındaki kişisel verilere hukuka aykırı olarak erişim sağladığı iddiası bakımından 6698 sayılı Kanun kapsamında yapılacak bir işlem bulunmadığına,*

- *1136 sayılı Avukatlık Kanununun 2 nci maddesinde ilgili makamların avukatların görevlerini yapmak üzere ihtiyaç duyduğu bilgi ve belgeleri avukatların incelemesine sunmakla yükümlü olduğunun düzenleme altına alındığı ve bu kapsamda 6698 sayılı Kanunun 8 inci maddesinin üçüncü fıkrasında düzenlenmiş “Kişisel verilerin aktarılmasına ilişkin diğer kanunlarda yer alan hükümler saklıdır.” düzenlemesi uyarınca Adalet Bakanlığı tarafından icra tevzi bürosunda görevli personel eliyle borçlunun alacaklı olduğu icra dosyaları hakkında bilgi ve belge sağlama amacıyla avukatlara görevlerini yerine getirebilmeleri için kişisel veri aktarımı yapılabileceğinden Adalet Bakanlığı tarafından alacaklı vekili avukatlara borçluların alacaklı olduğu icra takip dosyalarında bulunan kişisel verilerin hukuka aykırı olarak aktarılması iddiası bakımından 6698 sayılı Kanun* ***kapsamında yapılacak bir işlem bulunmadığına***

karar verilmiştir.

Yayım Tarihi : 09/08/2021
Karar Tarihi : 20/01/2020
Karar No : 2020/50
Konu Özeti : **Bir perakende giyim firmasının kişisel veri ihlali bildirimi**

Veri sorumlusunun Kurumumuza intikal eden veri ihlal bildiriminde;

- İhlalin bazı müşterilerin yeni bir hesap açarken kişisel verilerinin yanlışlıkla bir URL üzerinden veri sorumlusunun iç sistemlerine ve çalıştığı bazı üçüncü taraf satıcı/sağlayıcılara aktarılması şeklinde gerçekleştiği ve bu durumun veri sorumlusunun olağan bir denetimi esnasında tespit edildiği,

- Kurumumuza veri ihlaline ilişkin bildirim yapıldığında, veri sorumlusunun iki uygulama analizi sağlayıcısından (analytics provider) verilerin hâlihazırda otomatik olarak silinmiş olduğuna dair teyit aldığı,

- İlk 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) yönlendirildiğinin öğrenildiği (Türkiye'deki ilgili kişilerin bu yedi adet URL'den iki tanesinde gerçekleşen hatadan etkilendiği),

- İhlalden etkilenen ilgili kişi sayısının 44 olduğu,

- İhlalden etkilenen kişi kategorilerinin aboneler/üyeler, müşteriler/potansiyel müşteriler olduğu,

- Şirketin Kurumumuzu muhatap 10.06.2019 tarihli ilk yazısında, ihlalden etkilenen kişisel verilerin, zorunlu alan olan e-posta adresi, doğum tarihi, açık metin şeklinde şifre verilerinin olduğu, ancak zorunlu alan olmayan ad soyad verilerinin de etkilenmiş olabileceği,

- İlgili kişilere 23.07.2019 tarihinde e-posta yoluyla bildirim yapıldığı

ifadelerine yer verilmiştir.

Veri ihlal bildiriminin Kurumumuzun yetki ve görev alanı çerçevesinde incelenmesi neticesinde; Kişisel Verileri Koruma Kurulunun 20/01/2020 tarih ve 2020/50 sayılı Kararı ile;

- 01.08.2018 ve 21.10.2018 tarihlerinde gerçekleşen veri ihlallerinin tespitinin yaklaşık bir yıl sonra 02.07.2019 tarihinde yapılmış olmasının, gerçekleştirilen işlemlere dair Şirketin log kaydı/takip alarm sistemlerinin bulunmadığının ya da etkin bir şekilde kullanılmadığının ve Şirket tarafından gerekli kontrollerin yapılmadığının göstergesi olduğu,

- 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

kanaatine varıldığından 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 (Kanun) 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 50.000 TL idari para cezası uygulanmasına,

- İhlalin 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 değerlendirildiğinden bu hususta **Kanun kapsamında yapılacak bir işlem bulunmadığına**

karar verilmiştir.

Yayım Tarihi : 09/08/2021
Karar Tarihi : 05/05/2020
Karar No : 2020/345
Konu Özeti : Bilgisayar oyunları alanında faaliyet gösteren veri sorumlusunun veri ihlali bildirimi hakkında

Veri sorumlusunun Kurumumuza intikal eden veri ihlali bildiriminde;

- 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 yüklendiğinin tespit edildiği ve konu hakkında inceleme başlatıldığı,

- 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 men edilmiş sahte(bot) hesaplara ait olduğunun görüldüğü,

- İncelemenin detaylandırılmasından sonra 12 Ocak 2019 tarihinde verilerin hem sahte(bot) hesaplara hem de Türkiye'de mukim kullanıcılara ait gerçek hesapların birleşiminden oluştuğunun kesinleştiği,

- Yapılan çalışmalar sonucunda bilindiği kadarıyla söz konusu verilerin github'dan kaldırıldığı veya kamu erişimine kapalı hale getirildiği,

- İhlalden etkilenen kişi sayısının 62 olduğu,

- İhlalden kullanıcılar, müşteriler ve potansiyel müşteriler ile çocukların etkilendiği, ihlalden etkilenenlerin tamamına yakınının yetişkin olmakla birlikte az sayıda çocuğun da içlerinde yer aldığı,

- İhlalden etkilenen kişisel verilerin kimlik(doğum tarihi), iletişim(e-posta adresi), lokasyon(internet hizmet sağlayıcı ve kullanıcı kayıt tarihi ve saati) gibi bilgilerin olduğu

ifadelerine yer verilmiştir.

Veri ihlal bildiriminin Kurumumuzun yetki ve görev alanı çerçevesinde incelenmesi neticesinde; Kişisel Verileri Koruma Kurulunun 05/05/2020 tarih ve 2020/345 sayılı Kararı ile;

- 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, eski çalışanın kaynak kodları da github.com internet sitesine yüklemiş olmasının bir güvenlik açığı olduğu, 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" başlığı altında "…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." şeklinde açıklanan hususlara uygun davranmadığının göstergesi olduğu,

- 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,

- Personele veri sorumlusunun çok sayıda politikasının imzalatıldığının veri sorumlusu tarafından beyan edilmiş olmasına rağmen söz konusu çalışanın kişisel verileri de içeren dosyaları kendi taşınabilir depolama aygıtına kopyalamasının politikaların etkin şekilde uygulanmadığı ve farkındalık konusunda yeterli etkiyi sağlamadığının göstergesi olduğu

hususları dikkate alındığında, 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 nci maddesinin (5) numaralı fıkrasında yer verilen "en kısa sürede" bildirimde bulunma yükümlülüğüne aykırılık teşkil etmesi nedeniyle Kanunun 18 nci maddesinin (1) numaralı fıkrasının (b) bendi uyarınca veri sorumlusu hakkında 30.000 TL

olmak üzere **toplam 130.000 TL idari para cezası uygulanmasına**

karar verilmiştir.

Yayım Tarihi : 09/08/2021
Karar Tarihi : 07/05/2020
Karar No : 2020/359
Konu Özeti : **Bir bankanın veri ihlali bildirimi hakkında**

Veri sorumlusunun Kurumumuza intikal eden veri ihlali bildiriminde;

- İhlalin; KKB ekranında, Veri Sorumlusu Banka'nın eski çalışanının işin gereğinden fazla adette sorgulama yapılması ile gerçekleştiği, çalışanın ifadesine göre; T.C. kimlik numaraları Banka dışından 3. şahıs tarafından iletilip kişilerin kredi skorlarının öğrenilmek istenildiği,

- İhlalin yıllık periyotlarla hazırlanan kontroller neticesinde veri ihlalini gerçekleştiren çalışanın işin gereğinden fazla adette sorgulama yaptığının fark edilmesi üzerine hazırlanan Teftiş Raporu ile; çalışanın KKB sorgulamalarını ilgili kişilerin gıyabında gerçekleştirdiği, KKB sorgulamalarını gerçekleştirdiği esnada cep telefonu ile ilgilendiği ve KKB sorgulamalarını yaptıktan hemen sonra bir kağıda not aldığı, bazı tarihlerde bu kağıdın fotoğrafını çektiği ve/veya cep telefonu ile yazıştığının tespit edilmesiyle anlaşıldığı,

- İhlalin Temmuz 2018 ile Mayıs 2019 tarihleri arasında gerçekleştiği,

- İhlalden veri sorumlusunun müşterisi olan ve müşterisi olmayan toplam 5695 kişinin etkilendiği,

- İhlalden etkilenen kişisel verilerin, şahısların bankalardan kullanmış oldukları tüm kredili ürünlere ilişkin geçmişleri, ödeme performansları ve borç rakamları, adres, telefon vb. olduğu

ifadelerine yer verilmiştir.

Veri ihlal bildiriminin Kurumumuzun yetki ve görev alanı çerçevesinde incelenmesi neticesinde; Kişisel Verileri Koruma Kurulunun 07/05/2020 tarih ve 2020/359 sayılı Kararı ile;

- 7305 adet KKB sorgulaması yapıldığı, bu sorgularda 5889 adet TC kimlik numarası sorguladığı, (mükerrer olanlar elendikten sonra 5695) bu TC kimlik numaralarının 3038'inin Banka müşterilerine ait olduğu, 2851'inin Banka müşterisi olmadığı,

- 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" başlığı altında yer alan "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 zaafiyetlerini ya da bunları kullanan tehditleri bildirmesi için resmi bir raporlama prosedürü oluşturulması, gerekmektedir."*, ifadelerine aykırı olarak veri sorumlusu tarafından kişisel verilerin korunmasına ilişkin kişisel veri güvenliği takibinin uygun zaman aralıklarıyla yapılmadığının göstergesi olduğu,

- 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 olmasının Rehber'in "Kişisel Veri İçeren Ortamların Güvenliğinin sağlanması" başlığı altında "*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."*, ifadelerine aykırı olarak ilgili teknik ve idari tedbirlerin ihlalin öncesinde yeterince alınmadığının göstergesi olduğu,

- 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" başlığı altında yer alan *"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.",* ifadelerine aykırı sorgulamada sınırlama (kota) bulunmamasından kaynaklandığı,

- 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 edildiği, Rehber'in 2018 yılının ocak ayında yayımlanmış olduğu ve "Çalışanların Eğitilmesi ve Farkındalık Çalışmaları" başlığının altında; "…

- *"…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.",* ifadelerine aykırı olarak gerçekleşen çalışanlara eğitim verilmesinin halen sağlanmadığı

hususları dikkate alındığında, 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,

- 18.07.2019 tarihinde tespit edilmiş olan ihlalin 31.07.2019 tarihinde Kurula bildirildiği, geç bildirim sebebi olarak belirtilen Teftiş Raporunda yer alan bilgilerin hangilerinin paylaşıldığının net olmadığının ifade edilmesi, eldeki delillerin yetersizliği, olayın mahiyetinden emin olunmaması, müşteri şikayeti 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 sebebinin, 24.01.2019 Tarih ve 2019/10 sayılı Kişisel Veri İhlali Bildirim Usul ve Esaslarına İlişkin Kurul Kararı'nda yer alan *"…Formda yer alan bilgilerin aynı anda sağlanmasının mümkün olmadığı hallerde, bu bilgilerin gecikmeye mahal verilmeksizin aşamalı olarak sağlanmasına…"* ifadeleri göz önünde bulundurulduğunda ilgili sebeplerin Kurula geç bildirimde bulunulması için geçerli bir mazeret niteliği taşımadığı,

- Veri ihlalinden etkilenen 5695 kişi arasında sadece Bankada iletişim bilgileri bulunanlara veri ihlal bildiriminde bulunulduğu, bu kapsamda ilgili kişilerin tamamına bildirimde bulunmak adına makul çaba sarf edilmediği ve Kurumumuz tarafından talep edilmesine rağmen ihlalin bildirildiği kişi sayısının ve bu kişilerin Banka müşterisi olup olmadığına hususlarına dair Kurumumuza bilgi verilmediği

hususları dikkate alındığında; Kanunun 12 nci maddesinin (5) numaralı fıkrasında yer verilen "en kısa sürede" (Kurul'a bildirim için 72 saat) bildirimde bulunma yükümlülüğüne aykırı davranan veri sorumlusu hakkında Kanunun 18 nci maddesinin (1) numaralı fıkrasının (b) bendi uyarınca 50.000 TL olmak üzere **toplam 450.000 TL idari para cezası uygulanmasına**

karar verilmiştir.

Yayım Tarihi : 09/08/2021
Karar Tarihi : 22/05/2020
Karar No : 2020/421
Konu Özeti : **Kişisel bakım sektöründe faaliyet yürüten bir veri sorumlusunun veri ihlali bildirimi hakkında**

Veri sorumlusunun Kurumumuza intikal eden veri ihlali bildiriminde;

- 06.03.2020 tarihinde veri sorumlusu e-posta adresine kimliği belirsiz bir şahıstan veri sorumlusu web sitesi üyelerinin e-posta adresini/şifrelerini ele geçirdiğine dair bir mesaj geldiği,

- Yapılan incelemelerde, veri sorumlusu ile herhangi bir ilişkisi olmayan üçüncü kişilerin veri sorumlusunun kullanımındaki veri tabanlarından herhangi bir sızıntı olmaksızın dışı kaynaklardan elde ettikleri elektronik posta adresleri/şifreler ile veri sorumlusuna ait internet sitesine giriş yaptıkları,

- 04.03.2020 tarihinde bu olayın meydana geldiği, anılan kişi veya kişilerin ellerindeki e-posta şifre bilgilerini 14.000'den fazla IP'den bağlantı kurarak ve 500.000'in üzerinde e-posta/şifre kombinasyonunun sitede denedikleri,

- Her başarısız denemeden sonra bir başka e-posta/şifre denemesi yaptıkları ve bu yolla 2092 site kullanıcısının hesaplarının şifrelerini doğruladıklarının tespit edildiği,

- İhlalden etkilenen kişisel verilerin müşterilere ait ad, soyad, cep telefonu numarası, e-posta adresi, cinsiyet, doğum günü, teslimat/fatura adresleri ve sipariş geçmişi bilgileri olduğu

ifadelerine yer verilmiştir.

Veri ihlal bildiriminin Kurumumuzun yetki ve görev alanı çerçevesinde incelenmesi neticesinde; Kişisel Verileri Koruma Kurulunun 22/05/2020 tarih ve 2020/421 sayılı Kararı ile;

- İhlalin 04.03.2020 tarihinde meydana geldiği, anılan kişi veya kişilerin ellerindeki elektronik posta şifre bilgilerini 14.000'den fazla IP'den bağlantı kurarak sitede denedikleri ve her denemeden sonra başka bir e-posta/şifre denemesi yaptıkları,

- Veri sorumlusu tarafından yapılan inceleme neticesinde bu denemelerin sonucunda 2092 kullanıcının hesaplarına başarılı şekilde giriş yapıldığı,

- İhlalden veri sorumlusu müşterilerine ait ad-soyad, e-posta, cep telefonu, cinsiyet, doğum günü, teslimat/fatura adresleri ve sipariş geçmişi bilgilerinin etkilendiği,

- Veri sorumlusunun kendi olağan trafiğine ek bu trafiğin veri sorumlusunca fark edilmediği ve ihlali gerçekleştiren kimliği belirsiz kişilerce gönderilen e-posta sonucunda ihlalin tespit edilebildiği,

- İhlali gerçekleştiren kişi ya da kişiler tarafından veri sorumlusu dışı kaynaklardan elde edildiği belirtilen 500.000'in üzerinde e-posta/şifre kombinasyonuna ilişkin denemeler yapıldığı veri sorumlusu tarafından belirtilmiş olup, Kurumumuz tarafından yayınlanan Kişisel Veri Güvenliği Rehberi (Teknik ve İdari Tedbirler)'nde yer alan 3.2. Kişisel Veri Güvenliğinin Takibi maddesinde veri sorumlularının sistemlerinin çoğunlukla hem içeriden hem de dışarıdan gelen saldırılar ve siber suçlara veya kötü amaçlı yazılımlara maruz kalmakta olduğu, çeşitli belirtilere rağmen bu durumun uzun süre fark edilemediği ve müdahale için geç kalınabildiği ifade edilmekte olup; hesabına giriş yapılan 2092 kullanıcı dışında başarısız denemelerin sayısının fazlalığının veri sorumlusu tarafından fark edilememesinin bilişim ağlarının izlenmesi ve olmaması gereken durumların fark edilmesi hususunda eksiklik olduğu

hususları dikkate alındığında Kanunun 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 **210.000 TL idari para cezası uygulanmasına**

karar verilmiştir.

Yayım Tarihi : 09/08/2021
Karar Tarihi : 16/06/2020
Karar No : 2020/463
Konu Özeti : İlaç sektöründe faaliyet yürüten bir veri sorumlusunun veri ihlali bildirimi hakkında

Veri sorumlusunun Kurumumuza intikal eden veri ihlali bildiriminde;

- Veri ihlalinin zararlı yazılımlardan ve fidye yazılımlarından kaynaklı bir siber saldırı olarak veri sorumlusunun yetkili kullanıcı şifresi ele geçirilerek sistemlerine erişimin engellenmesi şeklinde gerçekleştiği ve saldırının çalışanlarının sistemlere erişememesi sonucu tespit edildiği,

- Veri sorumlusunun faaliyetlerini sürdürmesi için kritik öneme sahip tüm sunucu ve verilerinin ve bunlara ek olarak diğer sunucuların yedek dosyalarının depolandığı Data Domain Sunucusu verilerinin silindiği,

- Yetkisiz erişim sağlama girişimlerinin 8 – 11 – 12 Ocak tarihlerinde gerçekleştiği, saldırının 12/01/2020 tarihinde tespit edildiği,

- Veri sorumlusunun yaptığı incelemede, saldırının, LDAP servislerinde kullanılan Domain Admin yetkili anonim isimli bir kullanıcı hesabı ile gerçekleştirildiği, ihlalin yapılmış olduğu bilgisayarın tespit edildiği ve şüpheliler aleyhine İstanbul Cumhuriyet Başsavcılığına şikâyette bulunulduğu,

- Saldırının veri sorumlusunun bizzat siber güvenlik desteği almakta olduğu firmaya ait IP adresi üzerinden ve firma çalışanı tarafından gerçekleştirildiğinin tespit edildiği ve bu tespitin firma tarafından kabul edildiği,

- İhlali gerçekleştiren siber güvenlik desteği alınan firmanın çalışanının aynı zamanda veri sorumlusu eski çalışanı olduğu,

- İhlalden etkilenen kişi ve kayıt sayısının tam ve kesin olarak belirlenememiş olduğu ancak 1000 kişi civarında olduğunun tahmin edildiği belirtilmekte olup bunlardan 297 kişinin şirket çalışanı olduğu; bunlar dışında kalanların ise tedarikçi, müşteri ve taşeronlara ait olduğu,

ifadelerine yer verilmiştir.

Veri ihlal bildiriminin Kurumumuzun yetki ve görev alanı çerçevesinde incelenmesi neticesinde; Kişisel Verileri Koruma Kurulunun 16/06/2020 tarih ve 2020/463 sayılı Kararı ile;

- Veri sorumlusunun faaliyetlerini sürdürmesi için kritik öneme sahip tüm sunucu ve verilerinin ve bunlara ek olarak diğer sunucuların yedek dosyalarının depolandığı Data Domain Sunucusu verilerinin silindiği,

- İhlalden etkilenen kişi ve kayıt sayısının tam ve kesin olarak belirlenememiş olduğu ancak 1000 kişi civarında olduğu ve ihlalden özel nitelikli kişisel verilerinde etkilenmiş olabileceği,

- Veri sorumlusu, sistemlerine düzenlenen söz konusu saldırıyı şirket çalışanlarının sistemlere erişememesi sonucu tespit ettiği; özel nitelikli kişisel veriler üzerinde çalışan çok uluslu bir şirketin, böylesi saldırılar için sızma testleri ve risk analizleri yapıp tehditleri belirlemesi ve güvenlik açıklarını kapatması ve log kaydı takibi ile veri güvenliğini sağlayacak önlemler alması gerektiği ve bu durumun Kişisel Veri Güvenliği Rehberi 3.2. maddesinde; "Kişisel Veri Güvenliğinin Takibi" başlığı altında; *"…güvenlik yazılımı mesajları, erişim kontrolü kayıtları ve diğer raporlama araçlarının düzenli olarak kontrol edilmesi, bu sistemlerden gelen uyarılar üzerine harekete geçilmesi, bilişim sistemlerinin bilinen zaafiyetlere karşı korunması için düzenli olarak zaafiyet taramaları ve sızma testlerinin yapılması ile ortaya çıkan güvenlik açıklarına dair testlerin sonucuna göre değerlendirmeler yapılması gerekmektedir…"* ifadelerine aykırılık teşkil ettiği,

- Veri sorumlusunun, sunucularının yedek dosyalarının depolandığı Data Domain sunucusunda yer alan verilerinin de silinmesinin, Kişisel Veri Güvenliği Rehberi 3.6. maddesinde; "Kişisel Verilerin Yedeklenmesi" başlığı altında; *"…veri sorumlusunu fidye ödemeye zorlayan kötü amaçlı yazılımlar olabilir. Bu tür kötü amaçlı yazılımlara karşı kişisel veri güvenliğini sağlamak için veri yedekleme stratejilerinin geliştirilmesi önerilmektedir. Öte yandan, yedeklenen kişisel veriler sadece sistem yöneticisi tarafından erişilebilir olmalı, veri seti yedekleri mutlaka ağ dışında tutulmalıdır. Aksi halde, veri seti yedekleri üzerinde kötü amaçlı yazılım kullanımı veya verilerin silinmesi ve yok olması durumlarıyla karşı karşıya kalınabilecektir…"* ifadelerine aykırılık teşkil ettiği,

hususları dikkate alındığında, Kanun'un 12 nci maddesinin (1) numaralı fıkrası çerçevesinde veri güvenliğini sağlamaya yönelik gerekli teknik ve idari tedbirleri almayan veri sorumlusu hakkında kabahatin haksızlık içeriği, veri sorumlusunun kusuru ve ekonomik durumu da göz önünde bulundurularak Kanunun 18 nci maddesinin (1) numaralı fıkrasının (b) bendi uyarınca 125.000 TL idari para cezası uygulanmasına

- İhlalden etkilenen şirket çalışanlarına 13.01.2020 tarihinde e-posta ile bildirim yapıldığı buna yönelik tevsik edici belgenin gönderildiği, ihlalden etkilenen şirket çalışanı dışındaki kişilere ise web sayfasından genel duyuru yapıldığı ve yapılan bu duyurunun ise Kişisel Verileri Koruma Kurulunun 18.09.2019 tarih ve 2019/271 sayılı Kararı gerekliliğine uygun olduğu,

- 11.01.2020 tarihinde gerçekleşen veri ihlali, 12.01.2020 tarihinde tespit edilmiş ve Kurumumuza 14.01.2020 tarihinde bildirilmiş olup veri sorumlusunun Kanunun 12 nci maddesinin (5) numaralı fıkrasında yer verilen "en kısa sürede" (24.01.2019 tarih ve 2019/10 sayılı Kurul kararında belirtilen 72 saatlik süre içerisinde) bildirimde bulunma yükümlülüğüne uygun hareket ettiği

hususları dikkate alındığında; Kanunun 12 nci maddesinin (5) numaralı fıkrasında yer verilen "en kısa sürede" (Kurul'a bildirim için 72 saat) bildirimde bulunma yükümlülüğüne uygun davranan veri sorumlusu hakkında bu konuda **yapılacak bir işlem bulunmadığına**

karar verilmiştir.

Yayım Tarihi : 09/08/2021
Karar Tarihi : 16/06/2020
Karar No : 2020/465
Konu Özeti : **Kurumsal yazılım hizmeti sunan bir veri sorumlusunun veri ihlali bildirimi hakkında**

Veri sorumlusunun Kurumumuza intikal eden veri ihlali bildiriminde;

- Siber suçlularının "parola püskürtme" saldırısı ile veri sorumlusunun bilgi sistemleri iç ağına eriştiklerini bilgisinin 6 Mart 2019 tarihinde emniyet birimlerinin siber güvenlik uzmanları tarafından veri sorumlusuna bildirildiği,

- Bilgilendirme sonrası, veri sorumlusu siber suçluları kendi dahili sistemlerinden çıkarmak için harici adli bilişim ve güvenlik uzmanlarını görevlendirdiği ve ek güvenlik önlemleri aldığı, ayrıca önde gelen bağımsız bir siber güvenlik firması tarafından yönetilen kapsamlı bir adli soruşturma çalışması başlattığı,

- Parola püskürtme saldırılarının, saldırganların kurumsal kullanıcı hesaplarında başarıyla kimlik doğrulaması yapmasını sağladığı,

- Saldırganlar, 5 kullanıcı hesabı için kimlik doğrulama anahtarını kaydettiği, bu da bir cep telefonu ortamı dışındaki XenDesktop Sanal Masaüstü Altyapısı (VDI) ortamına erişimi mümkün kıldığı,

- Ekim 2018'den Mart 2019'a kadar altı ayrı durumda, Dosya Aktarım Protokolü (FTP) ve Güvenli Dosya Aktarım Protokolü'nü (SFTP) kullanarak verileri dışarı sızdırdığı,

- Veri sorumlusu soruşturma sırasında 6 terabayttan fazla verinin muhtemelen sistemlerinden dışarı sızdığını öğrendiği,

- 06.03.2019 tarihinde tespit edilen veri ihlali, 29.04.2020 tarihinde Kurumumuza bildirildiği,

- İhlalden 22 gerçek kişiye ait kimlik *(ad soyad, TCKN)*, özlük *(iş beyanları, müşteri bağlılık belgeleri) ve finans (satış kayıtları, pazarlama materyalleri, bordro)* verilerinin etkilendiği,

- İhlalden etkilenen 18 çalışanına (7 eski çalışan, 11 halihazırda çalışıyor olan) ihlal sonrası posta yolu ile 29 Nisan 2019 tarihinde bildirim yapıldığı, fakat Türkiye'de ikamet ettikleri düşünülen 4 kişinin ise iletişim bilgileri kendilerinde mevcut olmadığı için bildirim yapamadıkları,

ifadelerine yer verilmiştir.

Veri ihlal bildiriminin Kurumumuzun yetki ve görev alanı çerçevesinde incelenmesi neticesinde; Kişisel Verileri Koruma Kurulunun 16/06/2020 tarih ve 2020/465 sayılı Kararı ile;

- Veri sorumlusunun veri ihlalini, gerçekleşme tarihinden yaklaşık 5 ay sonra 06 Mart 2019' da tespit ettiği ve bu durumun; Kurumumuz tarafından yayınlanan Kişisel Veri Güvenliği Rehberi (Teknik ve İdari Tedbirler)'nde 3.2. Kişisel Veri Güvenliğinin Takibi başlığında *"… güvenlik yazılımı mesajları, erişim kontrolü kayıtları ve diğer raporlama araçlarının düzenli olarak kontrol edilmesi, bu sistemlerden gelen uyarılar üzerine harekete geçilmesi, bilişim sistemlerinin bilinen zaafiyetlere karşı korunması için düzenli olarak zaafiyet taramaları ve sızma testlerinin yapılması ile ortaya çıkan güvenlik açıklarına dair testlerin sonucuna göre değerlendirmeler yapılması gerekmektedir*." ifadesi gereği, veri sorumlusu tarafından gerekli güvenlik kontrol ve denetimlerinin zamanında yapılmadığının göstergesi olduğu,

- Parola püskürtme saldırıları, çok sayıdaki hesaba zayıf olarak nitelendirilen parolalar kullanarak erişen kullanıcıların, parolalarının saldırganlar tarafından şifre tahmini yöntemiyle ele geçirilmesi şeklinde gerçekleştiği, söz konusu ihlalin; Kurumumuz tarafından yayınlanan Kişisel Veri Güvenliği Rehberi (Teknik ve İdari Tedbirler)'nde 2.2. Çalışanların Eğitilmesi ve Farkındalık Çalışmaları başlığında *"… 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."* ifadesine göre, veri sorumlusunun son kullanıcıları tarafından parola güvenliği farkındalığının tam olarak oluşmamasından kaynaklandığı,

- Bir paylaşım sürücüsünde bulunan 6 TB'tan fazla verinin çalınmasının, bu paylaşım sürücüsünde yüksek miktarda veri depolanması durumundan kaynaklanması sebebiyle, Kurumumuz tarafından yayınlanan Kişisel Veri Güvenliği Rehberi (Teknik ve İdari Tedbirler)'nde 2.1. Mevcut Risk ve Tehditlerin Belirlenmesi başlığında *"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 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"* ifadesi gereği, bu gibi saldırılara karşı veri kaybı riskini azaltmaya yönelik gerekli idari tedbirleri almadıkları,

dikkate alındığında Kanunun 12 nci maddesinin (1) numaralı fıkrası çerçevesinde veri güvenliğini sağlamaya yönelik gerekli teknik ve idari tedbirleri almayan veri sorumlusu hakkında kabahatin haksızlık içeriği, veri sorumlusunun kusuru ve ekonomik durumu da göz önünde bulundurularak Kanunun 18 inci maddesinin (1) numaralı fıkrasının (b) bendi uyarınca 75.000 TL,

- 06.03.2019 tarihinde tespit edilen veri ihlali, veri sorumlusu tarafından 29.04.2019 tarihinde Kurumumuza bildirilmiş olup bu durumda Kurumumuza 55 günlük geç bildirimde bulunduğu,

- Veri sorumlusunun ihlalden etkilenen ilgili kişilere ihlal tespit edildikten 55 gün sonra bildirim yaptığı

dikkate alındığında, Kanunun 12'nci maddesinin (5) numaralı fıkrasında yer verilen "en kısa sürede" bildirimde bulunma yükümlülüğüne aykırılık teşkil etmesi nedeniyle veri sorumlusu hakkında Kanunun 18 inci maddesinin (1) numaralı fıkrasının (b) bendi uyarınca 50.000 TL

olmak üzere **toplam 125.000 TL idari para cezası uygulanmasına**

karar verilmiştir.

Yayım Tarihi : 09/08/2021
Karar Tarihi : 09/07/2020
Karar No : 2020/532
Konu Özeti : Bir sigorta şirketinin veri ihlal bildirimi hakkında

Veri sorumlusunun Kurumumuza intikal eden veri ihlal bildiriminde;

- Veri sorumlusunun bilgi sistem destek hizmeti aldığı hizmet sağlayıcısında meydana gelen sistemsel bir hata sonucu akıbet dosyası seçen sorgunun hatalı çalışması nedeniyle 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 gönderdiği,

- Veri ihlalinden veri sorumlusunun müşterisi olan 61 şirketin toplam 367 çalışanın etkilendiği,

- 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,

- 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, (Örneğin bu alt yapı, 2010 yılından önce geliştirilseydi ilk kez 2010 yılında karşılaşılacağı ancak 2010 yılından sonra geliştirildiği için ilk problem 2020'de yaşandığı),

- İhlalden 367 gerçek kişiye ait kimlik (TCKN, ad soyad, doğum tarihi, SGK numarası), iletişim (telefon numarası, e-posta adresi), özlük (işe başlama tarihi) ve finans (IBAN numarası, katkı payı tutarı) verilerinin etkilendiği,

- İhlalden etkilenen kişilere ihlal sonrası e-posta ile bildirim yapıldığı, ihlalden etkilenme durumuna göre etkilenen kişi grupları 4'e ayrılarak her bir gruba ayrı bildirimler yapıldığı,

- Yanlış kişisel veri dosyasının gönderildiği 854 firmaya yapılan bildirim aramaları ve e-posta gönderimleri sonunda: 543 firmanın, verileri sildiklerine dair açık teyit verdiği, irtibat bilgilerindeki sorunlar nedeniyle ulaşılamayan bütün firmalara da ayrıca posta yoluyla yazılı olarak bildirim yapılmış ve yanlış bilgilerin kaydedilmiş ise silindiğine dair teyitlerinin beklendiği beyan ettikleri,

ifadelerine yer verilmiştir.

Veri ihlal bildiriminin Kurumumuzun yetki ve görev alanı çerçevesinde incelenmesi neticesinde; Kişisel Verileri Koruma Kurulunun 09/07/2020tarih ve 2020/531sayılı Kararı ile;

- Veri ihlaline sebep olan sistemsel hatanın 2011 yılından itibaren kullanılmaya başlanan uygulama yazılımından kaynaklanması sebebiyle, Kurumumuz tarafından yayınlanan Kişisel Veri Güvenliği Rehberi (Teknik ve İdari Tedbirler)'nde 3.5.Bilgi Teknolojileri Sistemleri Tedariği, Geliştirme ve Bakımı başlığında *"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 sürekli olarak takibinin gerektiği,

- İhlale konu olayın gerçekleşme tarihi (01.01.2020) ile tespit tarihi (06.01.2020) arasında 5 günlük bir gecikmenin bulunduğu hususunun, Kişisel Veri Güvenliği Rehberi (Teknik ve İdari Tedbirler)'nde 3.2. Kişisel Veri Güvenliğinin Takibi başlığında *"…raporlama sürecinde oluşturulacak raporlar, sistem tarafından oluşturulacak otomatik raporlar olabilir. Bu raporların sistem yöneticisi tarafından en kısa sürede toplulaştırılarak veri sorumlusuna sunulması gerekmektedir. Ayrıca güvenlik yazılımı mesajları, erişim kontrolü kayıtları ve diğer raporlama araçlarının düzenli olarak kontrol edilmesi, bu sistemlerden gelen uyarılar üzerine harekete geçilmesi…"* ifadesi gereği veri sorumlusunun gerekli kontrol ve denetimleri zamanında yapmadığının göstergesi olduğu,

- İhlale sebep olan hatanın istisnai bir durum olması ve uygulamanın ana fonksiyonları ile doğrudan ilişkili olmaması durumu ihlal bildiriminde belirtilse de sigortacılık işlemi yürüten bir kuruluşun bilgi sistemleri güvenliğinde daha dikkatli olması gerektiğinden, veri ihlaline sebep olan sistemsel hatanın işlem yayına alınmadan evvel düzeltilmesi gerektiği,

dikkate alındığında Kanunun 12 nci maddesinin (1) numaralı fıkrası çerçevesinde veri güvenliğini sağlamaya yönelik gerekli teknik ve idari tedbirleri almayan veri sorumlusu hakkında ihlale sebep olan hatanın istisnai bir durum olması ve ekonomik durumu da göz önünde bulundurularak Kanunun 18 inci maddesinin (1) numaralı fıkrasının (b) bendi uyarınca 30.000 TL idari para cezasının uygulanmasına,

- İhlale sebep olan sistemdeki hatanın 01 Ocak 2020 tarihinde gerçekleştiği, 06 Ocak 2020 tarihinde tespit edildiği, 08 Ocak 2020 tarihinde Kurumumuza veri ihlal bildiriminde bulunulduğu, bu durumda Kurul'un 24.01.2019 tarih ve 2019/10 sayılı Kararı ile belirlenen veri ihlalinin öğrenilmesinden itibaren başlayan 72 saatlik süre içerisinde bildirim koşulunun sağlandığı,

- Veri sorumlusu tarafından ilgili kişilere posta göndermek suretiyle bildirim yapıldığı, söz konusu metnin tarafımızla paylaşıldığı

dikkate alındığında, veri sorumlusunun bildiriminin Kanunun 12 nci maddesinin (5) numaralı fıkrasında yer verilen "en kısa sürede" (24.01.2019 tarih ve 2019/10 sayılı Kurul kararında belirtilen 72 saatlik süre içerisinde) bildirimde bulunma yükümlülüğüne uygun olması nedeniyle Kanunun 18 nci maddesinin (1) numaralı fıkrasının (b) bendi uyarınca **yapılacak bir işlem bulunmadığına**

karar verilmiştir.

Yayım Tarihi : 09/08/2021
Karar Tarihi : 01/10/2020
Karar No : 2020/763
Konu Özeti : İnternetten market alışveriş hizmeti veren veri sorumlusunun veri ihlal bildirimi hakkında

Veri sorumlusunun Kurumumuza intikal eden veri ihlal bildiriminde;

- 400 kişilik bir alıcı grubuna e-posta gönderimi yapılması sırasında alıcı e-posta adreslerinin gizliliğinin korunması amacıyla tüm alıcıların ilgili toplu e-postanın BCC kısmına eklendiği,

- Söz konusu işlem sırasında, e-posta gönderimini yapan çalışan tarafından e-postanın konu kısmına hataen 43 müşteriye ait e-posta adresinin eklendiği, bu nedenle, e-postanın konu kısmında e-posta adresi yer alan 43 alıcı bilgisinin, e-posta gönderimi yapılan 400 kişilik alıcı grubu ile paylaşıldığı,

- Söz konusu e-posta gönderimi yapılır yapılmaz, mailin hataen yukarıda belirtilen şekilde iletilmesinin çalışan tarafından tespit edildiği ve ivedi aksiyon alınması için Teknoloji Departmanından sorumlu kişilerle iletişime geçildiği, ancak e-postanın geri alınmasının mümkün olamayacağının öğrenildiği,

- İhlalden müşterilere ait e-posta adresi bilgilerinin etkilendiği, e-posta adreslerinin kişinin adı-soyadını da içerebildiği, bu nedenle ihlalden kimlik ve iletişim verilerinin etkilendiği,

- 43 ilgili kişinin söz konusu paylaşım hakkında bilgilendirildiği ve ilgili kişilerin ihlalden etkilenme düzeylerinin minimize edilmesinin sağlandığı,

- İhlalin gerçekleşmesini takiben en kısa süre içerisinde (48 saat içerisinde) ilgili kişiler ile doğrudan e-posta adresleri üzerinden iletişime geçilerek 29.09.2020 tarihinde bildirim yapıldığı

ifadelerine yer verilmiştir.

Söz konusu bildirimin incelenmesi neticesinde Kişisel Verileri Koruma Kurulunun 01.10.2020 tarih ve 2020/763 sayılı Kararı ile;

- İhlalden 43 ilgili kişinin etkilenmiş olması,

- İhlalden etkilenen kişisel verilerin sadece müşterilere ait e-posta ve e-posta adreslerinin içerisinde geçen ad-soyad bilgilerinin olması,

- İlgili kişilere ihlale ilişkin 29.09.2020 tarihinde bildirimde bulunulmuş olması ve tevsik edici belgelerin Kurumumuza iletilmiş olması,

- İhlalden etkilenen ilgili kişiler üzerinde ihlalin olumsuz sonuç doğurma riskinin düşük olması,

- Hatalı e-posta gönderimi yapılan 400 müşteriden ihlale konu e-postanın imha edilmesinin talep edilmiş olması,

- Veri sorumlusunun “en kısa sürede” (24.01.2019 tarih ve 2019/10 sayılı Kurul kararında belirtilen 72 saatlik süre içerisinde) Kurumumuza veri ihlalini bildirme yükümlülüğünü yerine getirmiş olması

hususları dikkate alındığında bu aşamada veri sorumlusu hakkında Kanunun 12 nci maddesi kapsamında **yapılacak bir işlem olmadığına** karar verilmiştir.

Yayım Tarihi : 09/08/2021
Karar Tarihi : 08/12/2020
Karar No : 2020/934
Konu Özeti : **Enerji sektöründe faaliyet gösteren veri sorumlusunun veri ihlali bildirimi hakkında**

Veri sorumlusunun Kurumumuza intikal eden veri ihlali bildiriminde;

- Veri sorumlusunun kurumsal internet sitelerinde yayınlama amacıyla kurum içinde hazırlanmış ürün katalogları, dokümanlar, resimler ve sertifikaların yer aldığı bir kurum içi arşiv platformunun bulunduğu,

- Yönetim tarafından kendisine verilen yetki kapsamında, platform kullanıcılarının eğitiminden sorumlu ve bu konuda yetkili bir çalışanın, platformunun kullanımı hakkında uygun şekilde eğitimi için profesyonel görevlerinin yürütülmesi amacıyla platform yöneticisiyle birlikte bir irtibat listesi hazırladığı,

- Eğitimi düzenleyen çalışanın platform yöneticisi tarafından sağlanan kullanıcı listesini, olağan iş koordinasyonu kapsamında yetkili üst düzey kullanıcıları tarafından erişim sağlanabilen bir ortak klasörde sakladığı,

- Bu kullanıcılardan bir tanesinin irtibat listesi ararken kullanıcı listesinde sehven şifre bilgilerinin de bulunduğunu fark ettiği ve durumu raporladığı,

- Söz konusu listede, sehven, kurum içi bir platformun kullanıcılarının şifrelerinin açık bir şekilde, kullanıcı adı, isim, profesyonel e-posta adresi gibi tanımlayıcılarla birlikte yer aldığı,

- İhlalden etkilenen kişi ve kayıt sayısının 2 olduğu,

ifadelerine yer verilmiştir.

Veri ihlal bildiriminin Kurumumuzun yetki ve görev alanı çerçevesinde incelenmesi neticesinde; Kişisel Verileri Koruma Kurulunun 05/05/2020 tarih ve 2020/345 sayılı Kararı ile;

- İhlalden Türkiye'den sadece iki (2) kullanıcının etkilenmiş olduğu,

- İhlale ilişkin dosyanın erişimden kaldırılmadan önce yalnızca sekiz (8) kullanıcı tarafından erişilmiş olabileceği,

- Söz konusu sekiz (8) kullanıcı ile görüşüldüğü tamamının gizlilik yükümlüklerini anladığını ve kabul ettiğini ve herhangi bir şifre bilgisini kullanmayacaklarını veya paylaşmayacaklarını teyit ettiği,

- İhlale konu olan verilerin niteliği gereği olumsuz etki doğurma olasılığının düşük olduğu,

- İhlalden sonra ilgili platformdaki şifrelerin maskelenmesinin sağlandığı, bunun da Kişisel Veri Güvenliği Rehberi (Teknik ve İdari Tedbirler)'nde 4.1. Teknik Tedbirler Özet Tablosu'nda da yer aldığı üzere veri maskeleme tedbirine uygun olduğu,

- İhlal gerçekleştikten sonra tespit edilen dosyanın veri sorumlusu tarafından ivedilikle ortadan kaldırıldığı, bu durumun da Kişisel Veri Güvenliği Rehberi (Teknik ve İdari Tedbirler)'nde 2.2. Çalışanların Eğitilmesi ve Farkındalık Çalışmaları başlığı altında yer alan *"Kişisel veri güvenliğini zedeleyecek saldırılar ile siber güvenliğe ilişkin, çalışanların sınırlı bilgileri olsa dahi ilk müdahaleyi yapmaları, kişisel veri güvenliğinin sağlanması konusunda büyük önem taşımaktadır."* ifadesi kapsamında değerlendirilebileceği,

- İhlalden etkilenen platform kullanıcılarının şifrelerinin yenilendiği ve ilgili kullanıcılara şifrelerini değiştirmeleri için bir uyarı e-postası gönderildiği, bu tedbirin de ihlal sonrasında kişisel verilerin olumsuz etki doğurma olasılığı düşük olsa da veri sorumlusunun Kişisel Veri Güvenliği Rehberi (Teknik ve İdari Tedbirler)'nde 2.1. Mevcut Risk ve Tehditlerin Belirlenmesi başlığı altında yer alan *"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"* tedbirini aldığının bir göstergesi olduğu

hususları dikkate alındığında, Kanunun 12 nci maddesinin (1) numaralı fıkrası kapsamında bu aşamada yapılacak bir işlem bulunmadığı

- İhlalin 02.09.2019 ile 16.09.2019 arası gerçekleştiği, 16.09.2019 tarihinde tespit edildiği ve 24.10.2019 tarihinde Kurumumuza bildirildiği dikkate alındığında Kurul'un 24.01.2019 tarih ve 2019/10 sayılı Kararı ile belirlenen veri ihlalinin öğrenilmesinden itibaren başlayan 72 saatlik süre içerisinde veri sorumlusunun bildirimde bulunmadığı,

- Bununla birlikte veri sorumlusunun çok uluslu bir yapısı olduğu ve etkilenen ilgili kişilerin bulunduğu ülkelerin tespit edilmesi ve ilgili ülkelerin bildirim yükümlülüklerinin tespit edilmesi ve değerlendirilmesi için gerekli süre göz önüne alındığında makul kabul edilebileceği,

- Etkilenme ihtimali olan mevcut tüm kullanıcıların e-posta mesajıyla bilgilendirildiği ve aynı şifreyi kullanmış olabilecekleri diğer platformlar da dâhil şifrelerini değiştirmeleri konusunda uyarıldığı, yapılan bilgilendirmenin Kişisel Verileri Koruma Kurulunun 18.09.2019 tarih ve 2019/271 sayılı Kararında belirtilen bildirimde bulunması gereken asgari unsurlardan kişisel veri kategorileri bazında hangi kişisel verilerin ihlalden etkilendiği, veri ihlalinin olumsuz etkilerinin azaltılması için alınan veya alınması önerilen tedbirler, ilgili kişilerin veri ihlali ile ilgili bilgi almalarını sağlayacak irtibat kişilerinin isim ve iletişim detayları ya da veri sorumlusunun web sayfasının tam adresi, çağrı merkezi vb. iletişim yolları hususlarını barındırdığı, ancak, ihlalinin ne zaman gerçekleştiği ve kişisel veri ihlalinin olası sonuçları hakkında yeterli bilgi verilmediği

dikkate alındığında, Kanunun 12 nci maddesinin (5) numaralı fıkrası uyarınca işlenen verilerin kanuni olmayan yollarla başkaları tarafından elde edilmesi halinde en kısa sürede ilgilisine ve Kurula, Kişisel Verileri Koruma Kurulunun 18.09.2019 tarih ve 2019/271 sayılı Kararına uygun olarak bildirimde bulunması hususunda **daha dikkatli olunması yönünde talimatlandırılmasına**

,

karar verilmiştir.

Karar Tarihi : 04/05/2021
Karar No : 2021/463
Konu Özeti : **Bulut Elektromarket Bilgi Teknolojileri ve Dış Tic. A.Ş. Veri İhlal Bildirimi**

Veri sorumlusu sıfatını haiz olan Bulut Elektromarket Bilgi Teknolojileri ve Dış Tic. A.Ş. tarafından Kuruma gönderilen kişisel veri ihlali bildiriminde özetle;

- Veri sorumlusunun sunucularına bir siber saldırı gerçekleştirildiği ve saldırı sonucunda sunuculara erişimin engellendiği,
- İhlalden çalışanlar ve müşterilerin etkilendiği,
- İhlalden etkilenen kişi ve kayıt sayısının henüz bilinmediği, tespit çalışmalarının devam ettiği,
- İhlalden kimlik, iletişim, lokasyon, özlük, hukuk, işlem, müşteri işlem, işlem güvenliği, fiziksel mekan güvenliği, işlem güvenliği, risk yönetimi, finans, mesleki deneyim ve pazarlama verilerinin etkilendiği,
- Özel nitelikli kişisel veriler arasında sağlık bilgileri ve ceza mahkumiyeti ve güvenlik tedbirlerine ilişkin verilerin etkilendiği

ifade edilmiştir.

Konuya ilişkin inceleme devam etmektedir.

Karar Tarihi : 04/05/2021
Karar No : 2021/462
Konu Özeti : ClearVoiceResearch.com, LLC Veri İhlal Bildirimi

Veri sorumlusu sıfatını haiz olan ClearVoiceResearch.com, LLC tarafından Kurumumuza gönderilen kişisel veri ihlali bildiriminde özetle;

- İhlalin yetkisiz bir kullanıcı tarafından 2015 Ağustos ve Eylül aylarına ait yedeklerin herkese açık hale getirilmesi sonucunda meydana geldiği,
- 17 Nisan 2021 tarihinde yetkisiz bir kullanıcı tarafından, ClearVoice'un 2015'teki anket katılımcılarının profil bilgilerini içeren eski veritabanlarından birine ilişkin, yedek dosyasına eriştiğini belirten bir e-posta alınması ile ihlalin tespit edildiği,
- İhlalden kimlik, iletişim, doğum tarihi, 2015 yılına ait şifreler, ırk ve etnik köken, siyasi düşünce, sendika üyeliği, sağlık bilgilerine ilişkin kişisel verilerin etkilendiği,
- İhladen etkilenen Türkiye'de yerleşik kişi sayısının 184.205 olduğu,
- İhlalden etkilen ilgili kişi grubunun çalışanlar olduğu

ifade edilmiştir.

Konuya ilişkin inceleme devam etmektedir.

Karar Tarihi : 03/08/2021
Karar No : 2021/752
Konu Özeti : Timurlar Sigorta Aracılık Hizmetleri Ltd. Şti. Veri İhlal Bildirimi

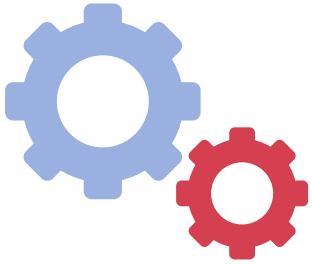
Veri sorumlusu sıfatını haiz olan Timurlar Sigorta Aracılık Hizmetleri Ltd. Şti. tarafından Kuruma gönderilen veri ihlal bildiriminde özetle;

- Veri sorumlusunun sigortacılık faaliyeti kapsamında sigorta teklif işlemleri için dışardan bir firmadan yazılım sistemi alıp kullanmakta olduğu,
- Yazılım sistemine yapılan siber saldırı sonucunda admin yetkisine sahip olunarak müşteri bilgilerine erişildiği,
- İhlalin 25.07.2021 tarihinde başladığı ve aynı gün saldırganlar tarafından para talep edilmesiyle ihlalin tespit edildiği,
- İhlalden etkilenen ilgili kişi grubunun müşteriler ve potansiyel müşteriler olduğu,
- İhlalden etkilenen kişi sayısının bilinmediği,
- İhlalden etkilenen kişisel verilerin; ad soyadı, kimlik numarası, telefon numarası, doğum tarihi, adres ve meslek bilgiler olduğu, ancak doğum tarihi, adres ve meslek bilgileri alanlarının doluluk oranının yüzde on civarında olduğu,
- Konuya ilişkin Cumhuriyet Başsavcılığına suç duyurusunda bulunulduğu,
- İlgili kişilerin veri ihlali hakkında veri sorumlusuna ait 0312 354 10 12 numaralı iletişim kanalı üzerinden bilgi alabileceği

ifade edilmiştir.

Konuya ilişkin inceleme devam etmektedir.

Karar Tarihi : 03/08/2021
Karar No : 2021/758
Konu Özeti : Motor Trend Group LLC Veri İhlal Bildirimi



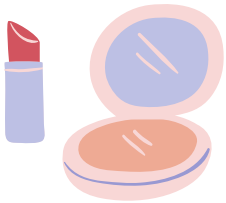
Veri sorumlusu sıfatını haiz olan Motor Trend Group LLC tarafından Kurumumuza gönderilen veri ihlal bildiriminde özetle;

- Veri ihlalinin, veri sorumlusunun bulut sunucularına ve depolama konumlarına bilinmeyen bir üçüncü tarafın erişim sağlamasıyla gerçekleştiği,
- Saldırganlar tarafından toplam 14 veri tabanına ile bir dizi ek dosyalara erişildiği ve söz konusu verilerin sızdırıldığı,
- İhlalin 20.06.2021 tarihinde gerçekleştiği ve aynı tarihte tespit edildiği,
- İhlalden tahmini olarak 2.977 ilgili kişinin etkilendiği,
- İhlalden etkilenen ilgili kişi grubunun kullanıcılar ve üyeler/aboneler olduğu,
- İhlalden kimlik, cinsiyet bilgisi, doğum tarihi, e-posta adresi, kimlik belirleme verileri (örneğin kullanıcı adları ve şifreler), tahmini coğrafi konum hakkında genel bilgiler ve yaklaşık 5 kişi için şifre sıfırlama güvenlik sorularının cevaplarına ilişkin bilgilerin etkilendiği,
- İlgili kişilerin veri sorumlusunun internet adresi, çağrı merkezi ve e-posta adresi aracılığıyla veri ihlali hakkında bilgi alabileceği

ifade edilmiştir.

Konuya ilişkin inceleme devam etmektedir.

Karar Tarihi : 06/08/2021
Karar No : 2021/787
Konu Özeti : Oriflame Kozmetik Ürünleri Ticaret Limited Şirketi Veri İhlal Bildirimi



Veri sorumlusu sıfatını haiz olan Oriflame Kozmetik Ürünleri Ticaret Limited Şirketi tarafından Kurumumuza gönderilen veri ihlal bildiriminde özetle;

- Veri ihlalinin, veri sorumlusunun ağ sunucularından birine trojan virüsü bulaştırılmasıyla gerçekleştiği,
- İhlalin 31.07.2021-01.08.2021 tarihleri arasında gerçekleştiği ve 02.08.2021 tarihinde tespit edildiği,
- Veri sorumlusunun e-posta adreslerine bir fidye e-postası gönderildiği, söz konusu fidyenin ödenmemesi halinde ele geçirildiği iddia edilen kişisel verilerin satışa çıkarılacağı tehdidinde bulunulduğu,
- İhlalden etkilenen ilgili kişi grubunun çalışanlar ve müşteriler olduğu,
- İhlalden etkilenen kişi sayısının 21.655 olduğu,
- İhlalden veri sorumlusunun Türkiye'de yerleşik yabancı marka elçilerinin kimlik bilgileri ile çalışanların ad, soyad, e-posta ve telefon bilgilerinin etkilendiği

ifade edilmiştir.

Konuya ilişkin inceleme devam etmektedir.

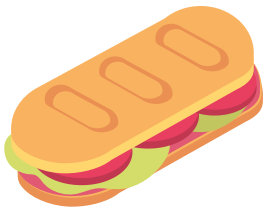
Karar Tarihi : **18/08/2021**
Karar No : **2021/843**
Konu Özeti : **Pied Piper Fansub (piedpiperfb.com) Veri İhlal Bildirimi**

Veri sorumlusu sıfatını haiz olan Pied Piper Fansub (piedpiperfb.com) tarafından Kuruma gönderilen veri ihlali bildiriminde özetle;

- İhlalin kurucunun tüm kullanıcı verilerinin yer aldığı sunucu hesabını bir saldırgana vermesi ve bu verilerin yedeklerinin alınıp taşınması sırasında sızdırılması ile gerçekleştiği,
- İhlalin eski site yöneticisinin verilerin satılık olduğunu fark etmesi ile tespit edildiği,
- İhlalin 14.11.2020 tarihinde gerçekleştiği ve 14.08.2021 tarihinde tespit edildiği,
- İhlalden etkilenen kişi sayısının 50.000 olduğu,
- İhlalden etkilenen kişi gruplarının kullanıcılar ve aboneler/üyeler olduğu,
- İhlalden etkilenen kişisel veri kategorilerinin; kimlik, iletişim, lokasyon, özlük, işlem güvenliği, mesleki deneyim, siyasi düşünce, felsefi inanç, din mezhep ve diğer inançlar, cinsel hayat, genetik veri ve diğer olduğu

ifade edilmiştir.

Konuya ilişkin inceleme devam etmektedir.



Karar Tarihi : **18/08/2021**
Karar No : **2021/844**
Konu Özeti : **Subway International B.V. Veri İhlal Bildirimi**

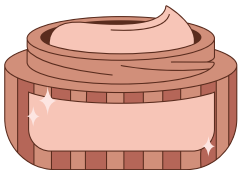
Veri sorumlusu sıfatını haiz olan Subway International B.V. tarafından Kurumumuza gönderilen veri ihlal bildiriminde özetle;

- 13.08.2021 tarihinde, veri sorumlusuna ait "www.subwaysiparis.com" alan adlı uzaktan sipariş sitesinde bir veri ihlali gerçekleştiğinin tespit edildiği,
- Veri ihlalinin SQL veri tabanının bir kopyasının ele geçirilmesiyle meydana geldiği,
- İhlalin 03.07.2021 tarihinde gerçekleştiği ve 13.08.2021 tarihinde bir sosyal medya paylaşımı üzerine yapılan inceleme sonucunda tespit edildiği,
- İhlalden etkilenen kişi grubunun uzaktan sipariş sitesine üye olan kullanıcılar/aboneler olduğu,
- İhlalden etkilenen kişi sayısının 51.295 olduğu,
- İhlalden ilgili kişilere ait ad, soyad, e-posta adresi, uzaktan sipariş hesabının şifresi, telefon numarası, adres ve önceki siparişlere ait bilgilerin etkilendiği

ifade edilmiştir.

Konuya ilişkin inceleme devam etmektedir.

Karar Tarihi : 26/08/2021
Karar No : 2021/874
Konu Özeti : Sinoz Kozmetik Sanayi Ticaret AŞ Veri İhlal Bildirimi



Veri sorumlusu sıfatını haiz olan Sinoz Kozmetik Sanayi Ticaret AŞ tarafından Kurumumuza 26.08.2021 tarihinde gönderilen veri ihlal bildiriminde özetle;

- Veri tabanı güncellemesi sırasında dışarıya açık durumda olan porttan sızıntı ile veri tabanındaki müşteri bilgilerinin ele geçirildiği,
- İhlalin 23.08.2021 tarihinde gerçekleştiği,
- İhlalin güncelleme sonrası yapılan veri tabanı taraması sırasında log kayıtlarının incelenmesiyle tespit edildiği,
- İhlalden etkilenen ilgili kişi grubunun müşteriler/potansiyel müşteriler olduğu,
- İhlalden 1.352.358 kişinin etkilendiği,
- İhlalden etkilenen kişisel verilerin müşteriler ve potansiyel müşterilere ait ad, soyad, eposta ve mobil telefon bilgileri olduğu,
- İlgili kişilerin veri ihlali ile ilgili kvkk@sinoz.com.tr mail adresinden bilgi talebinde bulunabilecekleri

ifade edilmiştir.

Konuya ilişkin inceleme devam etmektedir.

BERKERBERKER
Hukuk Bürosu
Büyükdere Cad. No.185
Kanyon Kompleksi C Blok
K:8 D:9 34394 Şişli, İstanbul
+90 212 353 03 00
+90 212 353 03 02
info@berkerberker.com