KİŞİSEL VERİLERİ KORUMA KURULUNUN 2 AĞUSTOS 2021 TARİHLİ KARAR ÖZETLERİ

Kişisel Verileri Koruma Kurulu (“KVK Kurulu” veya “Kurul”)’nun on bir yeni karar özeti, Kurumun internet sitesi üzerinden 02.08.2021 tarihli duyuru ile yayımlandı.

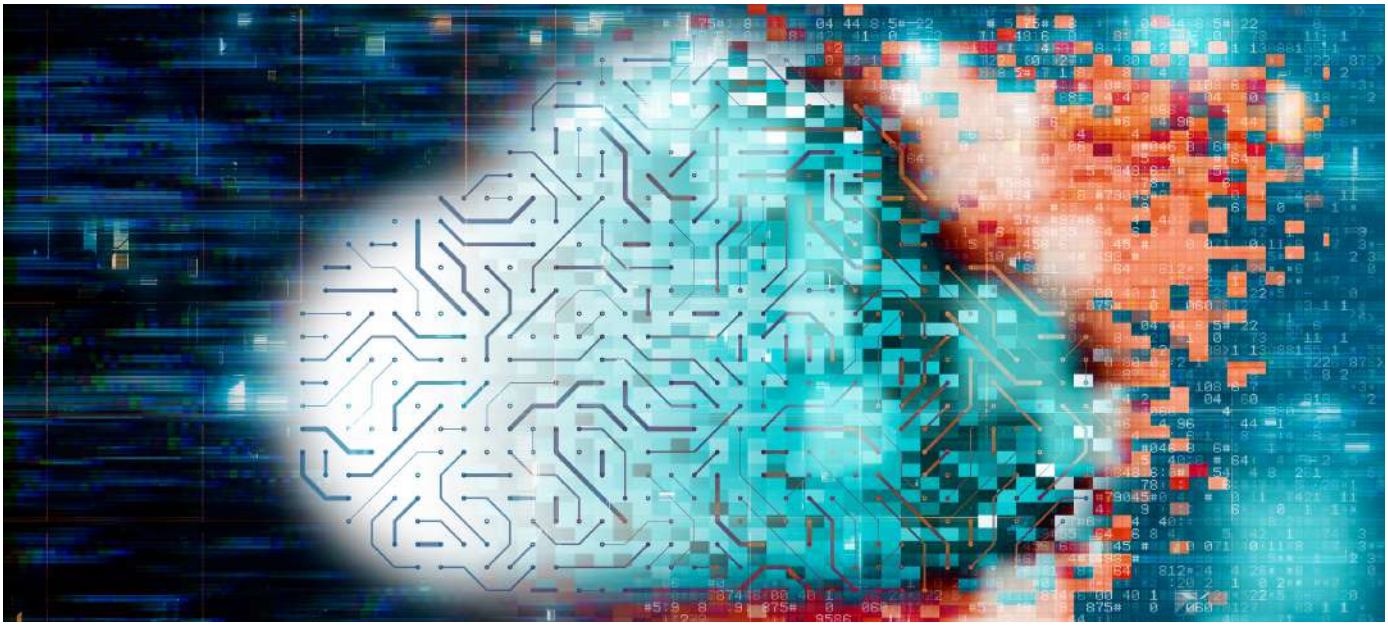
Sigortacılık ve bankacılık başta olmak üzere bilişim, e-ticaret, e-hizmet, perakendecilik ve belki de en önemlisi avukatlık faaliyetlerine kadar farklı alanlarda faaliyet gösteren veri sorumluları hakkında veri ihlal bildirimi konulu karar özetlerinde yüksek miktarda idari para cezaları uygulandığı dikkat çekmekte.

İlgili Kurul karar özetleri duyurusuna buradan, kişisel verilerin korunması kararları, veri ihlallerine ilişkin duyurular ve diğer KVKK haberlerine ise buradan ulaşabilirsiniz. KVK kararlarına ilişkin detaylı incelemelerimiz için ise aylık KVK & Siber Güvenlik bültenimizi ve makalelerimizi takip etmenizi öneririz

Levent Mah. Karanfil Aralığı Sok. No:8
Beşiktaş / İSTANBUL
www.mclegal.com.tr

MCLEGAL
Metin-Çiçek Avukatlık Ortaklığı
Attorney Partnership

“BİR PERAKENDE GİYİM FİRMASININ VERİ İHLAL BİLDİRİMİ HAKKINDA” KİŞİSEL VERİLERİ KORUMA KURULUNUN 18/06/2019 TARİH VE 2019/170 SAYILI KARAR ÖZETİ



VERİ SORUMLUSU:
PERAKENDE GİYİM FİRMASI

KARAR TARİH: 18/06/2019
KARAR SAYI. : 2019/170

İLGİLİ İLKELER :
KİŞİSEL VERİ İŞLEME GENEL İLKELERİ

- **DOĞRU VE GEREKTİĞİNDE GÜNCEL OLMA**
- **İŞLENDİKLERİ AMAÇLA BAĞLANTILI, SINIRLI VE ÖLÇÜLÜ OLMA**

UYGULANAN YAPTIRIM :
50.000-TL İPC

Kuruma yapılan söz konusu veri ihlali bildiriminde ihlalin 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 bildirilmiştir. İhlal bildiriminde, ihlalden aboneler/üyeler ve müşteriler/potansiyel müşterilerin etkilendiği, etkilenen ilgili kişi sayısının 44 olduğu, 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, ilgili 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 değerlendirilmektedir. Bununla birlikte URL üzerinden kişisel verilerin üçüncü taraf satıcı/sağlayıcılar tarafından görülmesinin web sayfası tasarım aşamasında iken yapılan testlerin yetersiz olduğunun veya gerekli testlerin yapılmadığının göstergesi olduğukanaatine varılarak Web sayfası tasarım aşamasında iken yapılan testlerin yetersiz olması sebebiyle veri güvenliğini sağlamaya yönelik gerekli teknik ve idari tedbirleri almadığı gerekçesiyle veri sorumlusu hakkında 50.000 TL idari para cezası uygulanmasına karar verilmiştir.

“ELEKTRONİK SATIŞ HİZMETİ SAĞLAYAN BİR ŞİRKETİN VERİ İHLAL BİLDİRİMİ HAKKINDA” KİŞİSEL VERİLERİ KORUMA KURULUNUN 11/02/2020 TARİH VE 2020/113 SAYILI KARAR ÖZETİ

VERİ SORUMLUSU:
E-HİZMET SAĞLAYICISI

KARAR TARİH :11/02/2020
KARAR SAYI : 2020/113

İLGİLİ İLKELER :

- **VERİ GÜVENLİĞİNE İLİŞKİN GEREKLİ HER TÜRLÜ TEKNİK VE İDARİ TEDBİRLERİ ALMA YÜKÜMLÜLÜĞÜ**

UYGULANAN YAPTIRIM :
200.000-TL İPC

Kuruma yapılan söz konusu veri ihlali bildiriminde e-ticaret sektöründe faaliyet gösteren veri sorumlusu sıfatını haiz şirketin, 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 belirtilmiştir. Veri sorumlusu şirket, tarafına web sitesinin hacklendiği iddiasının iletildiğini belirterek personeli tarafından zaman zaman halka açık bağlantıların paylaşıldığı kafe ortamlarında çalışıldığını ve ağ dinlemesinin bu sırada gerçekleşmiş olabileceğini bildirmiştir.

İhlal bildiriminde veri ihlalinden azami olarak 257.000 kişinin etkilenme ihtimalinin bulunduğu ancak yapılan incelmeler sonucu 25 kişi dışında kimsenin veri ihlalinden etkilenmiş olduğuna dair kayıt tespit edilemediği ifade edilmiş, ihlalden etkilenen veri kategorisinin kullanıcılar olduğu ve kişisel verilerin ad, soyadı, e-posta adresi, kriptolanmış kullanıcı hesabı şifreleri olduğu ve özel nitelikli kişisel verilerin etkilenmediği belirtilmiştir. Veri sorumlusu şirketin beyanına göre, 973.147 üyeye kadar olan kullanıcılardan 172.490 tanesinin sisteme Facebook profili üzerinden kaydolduğu için e-posta adreslerinin sistemde bulunmadığı, ancak veri ihlalinin gerçekleştirildiği e-posta adresi ile Şirket arasında gerçekleştirilen konuşmalarda; tüm veri tabanları, kaynak kodlar, dosya ve müşteri verilerinin ele geçirildiği iddia edilmektedir. Veri sorumlusu şirket, internet sitesini kullanan tüm kullanıcılara veri ihlali hakkında bildirimde bulunduğunu açıklamıştır.

Kurul tarafından yapılan incelemede; veri ihlalinden önce veri sorumlusuna ait internet ağı dışında halka açık bağlantıların paylaşıldığı kafe ortamlarından sisteme herhangi bir kısıt bulunmaksızın erişildiği ve sızma testlerinin ihlalden sonra yapıldığı tespit edilmiştir. İlaveten, ihlal öncesi sistemlerinde kritik bilgilere erişime neden olabilecek SQL Injection, Cross Site Scripting gibi zafiyetlerin bulunduğu ve mobil uygulama içerisine tanımlanmış SSL Sertifikası olmamasından dolayı uygulama trafiğinin rahatlıkla dinlenebildiği değerlendirilmiştir. Bununla birlikte idari tedbirlere ilişkin politikaların ve müdahale planlarının ihlal gerçekleştikten sonra oluşturulduğunu ve veri ihlali gerçekleşmeden önce kurumsal eğitim ve farkındalık faaliyetlerinin düzenlenmediğini tespit eden Kurul, veri ihlalinin ancak veri ihlalini gerçekleştiren kişinin veri sorumlusu ile iletişime geçmesi neticesinde tespit edilebildiğini de dikkate alarak veri güvenliğini sağlamaya yönelik gerekli teknik ve idari tedbirleri almadığı gerekçesiyle veri sorumlusu hakkında 200.000 TL idari para cezası uygulanmasına karar vermiştir.

“BİR BANKANIN VERİ İHLAL BİLDİRİMİ HAKKINDA” KİŞİSEL VERİLERİ KORUMA KURULUNUN 03/03/2020 TARİH VE 2020/201 SAYILI KARAR ÖZETİ

VERİ SORUMLUSU:
BANKA

KARAR TARİH:03/03/2020
KARAR SAYI : 2020/201

İLGİLİ İLKELER :

- **VERİ GÜVENLİĞİNE İLİŞKİN GEREKLİ TEKNİK VE İDARİ TEDBİRLERİ ALMA YÜKÜMLÜLÜĞÜ**
- **VERİ İŞLEYENİ DENETİM YÜKÜMLÜLÜĞÜ**

UYGULANAN YAPTIRIM :
75.000-TL İPC

Kuruma yapılan söz konusu veri ihlali bildiriminde veri ihlalinin, veri sorumlusu şirket müşterilerinin finansman taksit ödemesi tahsilatlarının gerçekleştiğine ilişkin ilgili müşterilere gönderilmesi gereken 905 kişiye ait e-posta ve kısa mesaj yoluyla yapılacak bildirimin işlem dışı ve Banka sisteminde kayıtlı diğer müşterilere gönderilmesi şeklinde gerçekleştiği bildirilmektedir.

Bu kapsamda, iç sistem uygulamasında yazılım değişikliğine gidilmesi neticesinde sehven gönderilen bildirimler neticesinde gerçekleşen ihlalden müşterilere ait; kimlik bilgisi (isim-soy isim), müşteri işlem bilgisi (cari hesap numarası, finansman hesap numarası, işlem tarihi) ve finans bilgisi (finansman taksit numarası, finansman taksit tutarı, finansman taksit tarihi) kategorilerine giren kişisel verilerin etkilendiği; ihlalden etkilenen kişi sayısının 905, kayıt sayısının 1831 olduğu ifade edilmiştir.

Kurul tarafından yapılan incelemede, 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" tespitine varılmış, bu teknik tedbir eksikliğinin de ihlale yol açtığı anlaşılmıştır. Kurul ayrıca, bahsi geçen "Notification" uygulama sisteminin hata sonucu veya kasıtlı olarak bozulup bozulmadığını kontrol etmek için yerleştirilen kontrol mekanizmasının yeterli düzeyde olmadığını ve bu tip hataların test aşamasında tespit edilerek değişikliklerin yayına alınmadan evvel düzeltilmesi gerektiğini belirtmiştir. Sonuç olarak, veri sorumlusu şirket hakkında veri güvenliğini sağlamaya yönelik gerekli teknik ve idari tedbirleri almadığı gerekçesiyle 75.000 TL idari para cezasının uygulanmasına karar verilmiştir.

“BİR SİGORTA ŞİRKETİNİN VERİ İHLAL BİLDİRİMİ HAKKINDA” KİŞİSEL VERİLERİ KORUMA KURULUNUN 07/05/2020 TARİH VE 2020/357 SAYILI KARAR ÖZETİ

VERİ SORUMLUSU:
BİR SİGORTA ŞİRKETİ

KARAR TARİH: 07/05/2020
KARAR SAYI. : 2020/357

İLGİLİ İLKELER:
VERİ GÜVENLİĞİNE İLİŞKİN GEREKLİ TEKNİK VE İDARİ TEDBİRLERİ ALMA YÜKÜMLÜLÜĞÜ

UYGULANAN YAPTIRIM :
90.000-TL İPC

Veri sorumlusunun Kuruma 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 ekranları vasıtasıyla müşterilerin poliçe bilgilerini, portföy takibi için kullandığı yönündeki tereddütlerin iletilmesi üzerine, Teftiş Kurulu Başkanlığınca inceleme yapılmasına karar verilerek veri ihlalinin gerçekleştiğinin anlaşıldığı bildirilmiştir. Teftiş Kurulu tarafından yapılan inceleme neticesinde ihlalin sistemde 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 gerçekleştiği, ihlalden etkilenen kişisel veri kategorilerinin müşterilere ait kimlik, iletişim ve risk yönetimi bilgisi olduğu ve toplam 91 kişinin ihlalden etkilendiği tespit edilmiştir.

Veri sorumlusu tarafından ayrıca, veri sızıntısı önleme uygulamasının belirli anahtar kelimeleri yakalamak üzere kurgulandığı ancak veri sızıntısına konu olan ihlal bu anahtar kelimeleri içermediğinden herhangi bir uyarının oluşmadığı ve 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 belirtilmiştir.

Kurul incelemesi sonucunda, veri sorumlusunun veri sızıntısı önleme uygulamasına ilişkin beyanları dikkate alınarak ihlal konusu olan kişisel verilerin veri sızıntısı önleme uygulamasında tanımlanabilir kişisel veriler olduğu dolayısıyla bu durumun kişisel veri güvenliğine ilişkin doğru ve tutarlı bir prosedürün veri sorumlusunun çalışma ve işleyişine uygun şekilde entegre edilmediğinin göstergesi olduğu değerlendirilmiştir. Bununla birlikte veri ihlalinin, gerçekleşmesinden yaklaşık iki ay sonra ancak tespit edilebildiği ve olaya ilişkin tereddütlerin bildirilmemesi ya da tereddüt oluşmaması durumunda veri ihlalinin tespit edilemeyeceği gözetilerek bu hususun, alınacak tedbirlerin önceden belirlendiği iyi bir olay yönetiminin kurgulanmadığı ve bu nedenle veri sorumlusunun, Kurum tarafından yayınlanan Kişisel Veri Güvenliği Rehberinde düzenlenen bilişim ağlarında sızma veya olmaması gereken bir hareket olup olmadığının takip edilmesi noktasında alınan teknik tedbirler açısından yetersiz kaldığının göstergesi olduğuna kanaat getirilmiştir.

Tüm bunlarla birlikte 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 da dikkate alınarak veri güvenliğini sağlamaya yönelik gerekli teknik tedbirleri almadığı gerekçesiyle veri sorumlusu hakkında 90.000 TL idari para cezası uygulanmasına karar verilmiştir.

“BİR BANKANIN VERİ İHLAL BİLDİRİMİ HAKKINDA” KİŞİSEL VERİLERİ KORUMA KURULUNUN 09/07/2020 TARİH VE 2020/530 SAYILI KARAR ÖZETİ

VERİ SORUMLUSU:
BANKA

KARAR TARİH: 09/07/2020
KARAR SAYI. : 2020/530

İLGİLİ İLKELER:
VERİ GÜVENLİĞİNİN SAĞLANMASI İÇİN GEREKLİ İDARİ VE TEKNİK TEDBİRLERİ ALMA YÜKÜMLÜLÜĞÜ

UYGULANAN YAPTIRIM :
200.000-TL İPC

Veri sorumlusu bankanın Kuruma 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 (KKB) skorlarını veya TCKN bilgisini 01.01.2019 ile 05.12.2019 tarihleri arasında Whatsapp uygulaması aracılığıyla bir tanıdığı (3. kişi) ile paylaştığının tespit edildiği belirtilmiştir.

Personelin 23 banka müşterisine ait paylaşımlardan menfaat temin ettiğine dair somut bir tespite ulaşılmadığı da belirtilerek veri ihlalinden, 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 bildirilerek ihlal ile ilgili olan personelin son bir yıl içerisinde kişisel veri koruma eğitimi aldığı ifade edilmiştir.

Kurul incelemesinde ihlalden 23 kişiye ait verilerin etkilendiği bildirilmesine rağmen ihlale sebebiyet veren personelin belirtilen tarihler arasında 1052 kişi için 10529 adet KKB sorgulaması gerçekleştirdiğini tespit ederek, kişi sayısı göz önüne alındığında karara konu ihlalden 23 kişiden daha fazla kişinin etkilenmiş olabileceğini belirtmiştir. Bu kapsamda Kurul tarafından ihlal öncesinde veri sorumlusu tarafından personelin KKB sorgularının sınırlandırılmadığı, ihlale 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 ve veri sorumlusunca gerçekleştirilen “Kişisel Verilerin Korunması Kanunu Eğitimi”nin yeterli olmadığı kanaatine varılarak veri güvenliğini sağlamaya yönelik gerekli teknik ve idari tedbirleri almadığı gerekçesiyle veri sorumlusu hakkında 200.000 TL idari para cezasının uygulanmasına karar verilmiştir.

“BİR OYUNCAK PERAKENDECİSİ VERİ SORUMLUSUNUN VERİ İHLAL BİLDİRİMİ HAKKINDA” KİŞİSEL VERİLERİ KORUMA KURULUNUN 22/07/2020 TARİH VE 2020/567 SAYILI KARAR ÖZETİ

VERİ SORUMLUSU: PERAKENDE ŞİRKETİ

KARAR TARİH: 22/07/2020
KARAR SAYI. : 2020/567

İLGİLİ İLKELER: VERİ GÜVENLİĞİNİN SAĞLANMASI İÇİN GEREKLİ İFARİ TEDBİRLERİ ALMA YÜKÜMLÜLÜĞÜ

UYGULANAN YAPTIRIM : 75.000-TL İPC

Veri sorumlusunun Kuruma intikal eden veri ihlal bildiriminde; ihlalin 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 belirtilmiştir. Veri sorumlusu şirketin Bilgi İşlem Departmanına şirkete ait markaya ilişkin kurulan uyarılar sayesinde üye hesabı bilgilerinin bulunduğu bir internet sitesine ulaşılmış, söz konusu internet sitesi yöneticilerine bir ihtar gönderilerek internet sitesinde yer alan ihlale konu sayfanın kaldırılmasının sağlandığı ifade edilmiştir. Bildirime göre ihlalden 29 müşteriye ait ad, soyad, e-posta adresi, telefon numarası, kayıtlı adres, müşteri işlem kategorisinde daha önce satın alınan ürün bilgileri etkilenmiştir.

Kurul incelemesinde, kişisel hesaplara erişim hususunda veri güvenliğinin sağlanması amacıyla kullanıcı kimliklerinin doğrulanması gerektiği belirtilerek 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 kanaatine varılmıştır. Bununla birlikte ihlalden etkilenen ilgili kişilerin hesaplarının şifreleri incelendiğinde müşteriler tarafından kullanılan şifrelerin sadece rakamlardan ya da sadece harf dizilerinden oluşabildiği görülerek müşterilere hesap açılırken müşterilerin güçlü şifre oluşturması için zorlanmadığı değerlendirilmiştir. Ayrıca, 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 sağlayamaması veri sorumlusunun uygulama güvenliğini sağlayamadığı yönünde değerlendirilmiştir. Tüm bu hususlar dikkate alınarak veri güvenliğini sağlamaya yönelik gerekli teknik tedbirleri almadığı gerekçesiyle veri sorumlusu hakkında 75.000 TL idari para cezası uygulanmasına karar verilmiştir.

Veri sorumlusunun gerçekleşen veri ihlalinin öğrenilmesinden itibaren başlayan 72 saatlik süre içerisinde bildirimde bulunmadığı tespit edilmiş; ancak yaşanan 1 günlük bir gecikmenin pandemi süreci nedeniyle makul olduğuna ve bu çerçevede veri sorumlusu hakkında yapılacak bir işlem bulunmadığına karar verilmiştir.

“BİR E-TİCARET ŞİRKETİNİN VERİ İHLAL BİLDİRİMİ HAKKINDA” KİŞİSEL VERİLERİ KORUMA KURULUNUN 17/09/2020 TARİH VE 2020/715 SAYILI KARAR ÖZETİ

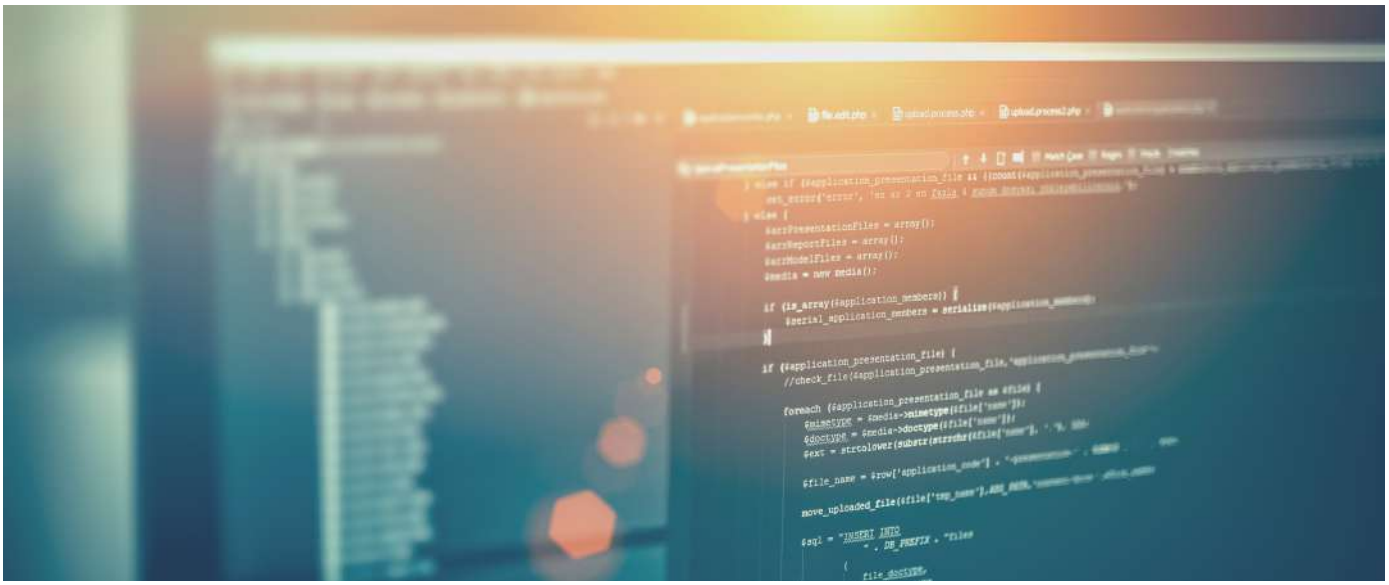
VERİ SORUMLUSU:
E-TİCARET ŞİRKETİ

KARAR TARİH: 17/09/2020
KARAR SAYI. : 2020/715

İLGİLİ İLKELER:
VERİ GÜVENLİĞİNİ SAĞLAMAK İÇİN GEREKLİ İDARİ VE TEKNİK TEDBİRLERİ ALMA YÜKÜMLÜLÜĞÜ

UYGULANAN YAPTIRIM :
165.000-TL İPC

Veri sorumlusunun Kuruma intikal eden veri ihlal bildiriminde; ihlalin, 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 açıklanmıştır. Bildirime göre ihlal, olayın gerçekleştiği gecenin sabahı mesai başlangıcında yapılan rutin kontroller sırasında tespit edilmiş, müteakiben vaka hakkında detaylı araştırma başlatılmıştır. Gerçekleşen ihlalden etkilenen kişi ve kayıt sayısının 832 olduğu bildirilerek ihlalle ilişkili 832 hesabın kullanıcısına e-posta aracılığıyla bildirimde bulunulduğu ifadelerine yer verilmiştir.



Kurul incelemesinde, öncelikle veri sorumlusunun ihlal bildiriminde mevzubahis e-posta adreslerinin ve şifrelerinin internet sitesi üzerinden ele geçirilmediği ve ihlalden etkilenen bir veri bulunmadığı belirtilmesine rağmen ilgili kişilerin hesaplarına yetkisiz kişilerce erişimde bulunulduğu gerekçesiyle kişisel verilerin gizliliğinin bozulduğuna ve bu durumun veri ihlali oluşturduğuna kanaat getirilmiştir. Veri sorumlusunun aynı IP adresinden başarısız oturum açma girişim sayısının veri ihlalinden sonra sınırlandırdığı tespit edilerek, bu hususun veri sorumlusunun veri ihlali öncesinde veri güvenliğini sağlamaya yönelik alması gereken teknik tedbirleri yeterli ve gerekli düzeyde almadığını değerlendiren Kurul, veri sorumlusu tarafından kullanıcıların belirli zaman aralıklarında şifrelerini değiştirmelerinin sağlanması gerektiğini belirtmiştir.

Bununla birlikte "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 alındığını ve ihlale 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 taşıdığını ifade eden Kurul, veri güvenliğini sağlamaya yönelik gerekli teknik ve idari tedbirleri almadığı gerekçesiyle veri sorumlusu hakkında 165.000 TL idari para cezası uygulanmasına karar verilmiştir.

"BİR TEKNOLOJİ ŞİRKETİNİN VERİ İHLAL BİLDİRİMİ HAKKINDA" KİŞİSEL VERİLERİ KORUMA KURULUNUN 22/10/2020 TARİH VE 2020/816 SAYILI KARAR ÖZETİ

VERİ SORUMLUSU: TEKNOLOJİ ŞİRKETİ

KARAR TARİH: 22/10/2020
KARAR SAYI. : 2020/816

İLGİLİ İLKELER: VERİ GÜVENLİĞİNİN SAĞLANMASI İÇİN GEREKLİ İDARİ TEDBİRLERİ ALMA YÜKÜMLÜLÜĞÜ

UYGULANAN YAPTIRIM : YAPILACAK BİR İŞLEM OLMADIĞINA DAİR KARAR

Veri sorumlusunun Kuruma intikal eden veri ihlal bildiriminde; mağazada yapılan bir alışveriş sonrasında adına e-fatura düzenlenen müşterinin sistemde kayıtlı e-posta adresine ilgili faturanın gönderilmesi işleminde, CRM sistemi üzerinde aynı ada sahip iki farklı müşteriye aynı telefon numarası kaydı oluşturulması nedeniyle bu faturanın aynı ad ve soyada sahip farklı bir müşteriye ulaşması suretiyle veri ihlali gerçekleştiği bildirilmiştir. 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 veri ihlali veri sorumlusu şirket tarafından tespit edilmiştir. İhlal bildiriminde, ihlalden etkilenen kişi sayısının 1, etkilenen kişisel verilerin; müşterinin adı soyadı, T.C. Kimlik Numarası, cep telefonu numarası, fatura bilgileri olduğu ve ilgili kişiye telefon görüşmesi ile bildirim yapıldığı ifade edilmiştir.

Kurul incelemesi neticesinde; ihlalden 1 kişiye ait kişisel verilerin etkilendiği, ilgili kişiye telefon yoluyla bildirim yapıldığı, ihlale konu kişisel verilerin ilgili kişi üzerinde olumsuz etki doğurma olasılığının düşük olduğu, ihlale konu e-postanın silinmesinin sağlandığı ve veri sorumlusunun ihlale kısa zamanda müdahale ettiği hususlarını dikkate alarak veri ihlalinin idari yaptırımı gerektirecek çapta olmadığına kanaat getirmiş, veri sorumlusu hakkında 6698 sayılı Kişisel Verilerin Korunması Kanununun 12'nci maddesi kapsamında yapılacak bir işlem olmadığına karar vermiştir.

“BİR SİGORTA ŞİRKETİNİN VERİ İHLAL BİLDİRİMİ HAKKINDA” KİŞİSEL VERİLERİ KORUMA KURULUNUN 08/12/2020 TARİH VE 2020/935 SAYILI KARAR ÖZETİ

VERİ SORUMLUSU: SİGORTA ŞİRKETİ

KARAR TARİH: 08/12/2020
KARAR SAYI. : 2020/935

İLGİLİ İLKELER: VERİ GÜVENLİĞİNİN SAĞLANMASI İÇİN GEREKLİ İDARİ TEDBİRLERİ ALMA YÜKÜMLÜLÜĞÜ

UYGULANAN YAPTIRIM: YAPILACAK BİR İŞLEM OLMADIĞINA DAİR KARAR

Veri sorumlusunun Kuruma intikal eden veri ihlal bildirimine göre; ihlal sağlık yenileme talebinde bulunan bir müşteriye, Müşteri İletişim Merkezi (Çağrı Merkezi) tarafından sehven başka bir müşterinin poliçe muafiyet bildirimi bilgisinin iletilmesiyle gerçekleşmiştir. Veri Kaybı Önleme Sistemi (“DLP”) düzenli kontrolleri sırasında tespit edilen veri ihlalinden veri sorumlusu müşterisi olan 1 kişinin kimlik, iletişim ve sağlık kategorilerindeki kişisel verilerin etkilendiği bildirilmiş, veri sorumlusu tarafından ihlal bildiriminde Müşteri İletişim Merkezi çalışanlarının müşteriyle direkt temasta olduklarından dolayı düzenli eğitimlere tabi olduğu ifade edilmiştir.

Kurul incelemesinde; veri sorumlusunun 24.01.2019 tarih ve 2019/10 sayılı Kurul kararında belirtilen 72 saatlik süre içerisinde Kuruma veri ihlalini bildirme yükümlülüğünü yerine getirdiği ve ilgili kişilere ihlale ilişkin 03.12.2020 tarihinde bildirim yapılacağını belirttiğini dikkate alarak gerçekleşen veri ihlalinin idari yaptırımı gerektirecek bir boyutta olmadığına kanaat getirmiş ve veri sorumlusu hakkında 6698 sayılı Kişisel Verilerin Korunması Kanununun 12 inci maddesi kapsamında yapılacak bir işlem bulunmadığına karar vermiştir. Bununla birlikte veri sorumlusu, ilgili kişiye bildirim yapılması ve söz konusu bildirimin yapıldığı ile bahse konu verilerin sehven gönderilen müşteri nezdinde silindiğine dair tevsik edici belgelerin Kuruma iletilmesi hususunda talimatlandırılmıştır.

“BİR İLAÇ ŞİRKETİNİN VERİ İHLAL BİLDİRİMİ HAKKINDA” KİŞİSEL VERİLERİ KORUMA KURULUNUN 15/12/2020 TARİH VE 2020/957 SAYILI KARAR ÖZETİ

VERİ SORUMLUSU:
İLAÇ ŞİRKETİ ŞİRKETİ

KARAR TARİH: 15/12/2020
KARAR SAYI. : 2020/957

İLGİLİ İLKELER:
VERİ GÜVENLİĞİNİN SAĞLANMASI İÇİN GEREKLİ TEKNİK TEDBİRLERİ ALMA YÜKÜMLÜLÜĞÜ

UYGULANAN YAPTIRIM :
YAPILACAK BİR İŞLEM OLMADIĞINA DAİR KARAR

Veri sorumlusunun Kuruma intikal eden veri ihlal bildiriminde; ihlalin 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 teknik eşleştirme hatası nedeniyle çalışanların aylık bordrosuna diğer çalışanlar tarafından erişilebilmesi suretiyle oluştuğu açıklanmıştır. Yanlış bordro giden bir çalışanın e-posta yoluyla İnsan Kaynakları Departmanına bilgi vermesi sonucu anlaşılan ihlalde 337 çalışanın bordrosunun yanlış çalışanlara gönderildiği, ihlalden etkilenen kayıt sayısının 1348, etkilenen verilerin ise bordrolarda yer alan maaş bilgisi, ad-soyad, banka numarası ve T.C. kimlik numarası gibi veriler olduğu bildirilmiştir. Veri sorumlusu şirket tarafından ihlalin 27.11.2020 tarihinde gerçekleştiği ve aynı gün tespit edildiği ifade edilmiştir.

Kurul incelemesinde; ihlalin, gerçekleşmesinden 13 dakika sonra tespit edildiği ve gerçekleşmesinden 2 saat sonra ise sonlandırıldığı tespit edilerek,ihlal veri sorumlusunun çalışanlarının bordro bilgilerinin diğer çalışanlara gönderilmesi şeklinde gerçekleştiğinden olumsuz etki doğurma olasılığının düşük olduğu değerlendirilmiştir. Kurul, ihlale sebep olan e-postaların silinmiş olduğunu ve e-postaların gönderildiği kişilere gerekli uyarının yapıldığını gözeterek ihlale sebep olan konuda ihlal sonrası gerekli teknik ve idari tedbirlerin alındığına kanaat getirmiş, Kanunun 12 inci maddesinin (1) numaralı fıkrası kapsamında veri sorumlusu hakkında yapılacak bir işlem olmadığına karar vermiştir.

“AVUKATLARIN İCRA TAKİP DOSYALARINDAKİ KİŞİSEL VERİLERE VEKÂLETNAME OLMAKSIZIN HUKUKA AYKIRI OLARAK ERİŞİM SAĞLADIĞINA İLİŞKİN İHBARLAR HAKKINDA” KİŞİSEL VERİLERİ KORUMA KURULUNUN 20/05/2021 TARİHLİ VE 2021/511-512-513 SAYILI KARAR ÖZETİ

VERİ SORUMLUSU:
AVUKAT

KARAR TARİH: 20/05/2021
KARAR SAYI. : 2021/511-512-513

İLGİLİ İLKELER:
VERİ GÜVENLİĞİNİ SAĞLAMA YÜKÜMLÜLÜĞÜ
ÖZEL NİTELİKLİ VERİLERE İLİŞKİN ÖNLEMLER

UYGULANAN YAPTIRIM :
HUKUKA AYKIRILIK OLMADIĞINA DAİR KARAR

Adalet Bakanlığı ve bir avukat hakkında Kuruma intikal ettirilen ihbarlarda özetle; alacaklı vekili avukatların, icra tevzi bürolarına başvuruda bulunarak 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 ihbar başvuruları ile veri sorumlularından alınan bilgi ve belgelerin ilgili mevzuat çerçevesinde incelenerek; ihbar konusu olay 2004 sayılı İcra ve İflas Kanunu ile 1136 sayılı Avukatlık Kanunu nezdinde değerlendirilmiştir. Buna göre, öncelikle 2004 sayılı İcra İflas Kanunu'nun "Taşınır ve taşınmaz malların haczi" başlıklı 85. Maddesi değerlendirilerek haciz yoluyla takip kapsamında borçlunun taşınır ve taşınmaz malları ile alacak ve haklarına haciz konulabileceğinin öngörüldüğü, bu kapsamda borçlunun alacaklı olduğu icra dosyalarına konu alacaklara da haciz konulmasının mümkün olduğu anlaşılmıştır. Akabinde 1136 sayılı Avukatlık Kanunu'nun 46 ve 2 maddeleri gözetilmiş, 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 tespit edilmiştir.

Bu değerlendirmelerden hareketle; 2004 sayılı İcra ve İflas Kanunu'nun 85'inci maddesi çerçevesinde haciz işlemlerini yerine getirmek üzere, 2004 sayılı Kanun'un 8/a ve 78'inci maddeleri uyarınca Ulusal Yargı Ağı Bilişim Sistemi ("UYAP") vasıtasıyla borçluların mal, hak veya alacaklarının sorgulanması ve 1136 sayılı Avukatlık Kanunu'nun 46'ncı maddesi uyarınca dava ve icra takibi dosyalarını vekâletname sunmaksızın inceleme yetkisine haiz avukatların müvekkillerinin alacağını tahsil etmek amacıyla işlem yapabileceği anlaşılmıştır.

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 yürütebileceğine kanaat getirilerek

avukatların vekâletname olmaksızın icra takip dosyalarındaki kişisel verilere hukuka aykırı olarak erişim sağladığı iddiasının isabetsiz olduğu, ilgili kişisel veri işleme faaliyetinin hukuka aykırı olmadığına karar verilmiştir.

Tüm bunlarla birlikte 1136 sayılı Avukatlık Kanunun'un 2'inci maddesinde ilgili makamların avukatların görevlerini yapmak üzere ihtiyaç duyduğu bilgi ve belgeleri avukatların incelemesine sunmakla yükümlü olduğunun düzenleme altına alındığı gözetilerek, bu kapsamda 6698 sayılı Kanun'un 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 aktarılmasının da hukuka aykırı olmadığına karar verilmiştir.