KİŞİSEL VERİLERİ KORUMA KURULUNUN 5 TEMMUZ 2021 TARİHLİ KARAR ÖZETLERİ

Kişisel Verileri Koruma Kurulu (“KVK Kurulu” veya “Kurul”)’nun on yeni karar özeti, Kurumun internet sitesi üzerinden 05.07.2021 tarihli duyuru ile yayımlandı.

Sigortacılık ve bankacılık başta olmak üzere bilişim, kozmetik ve hastanecilik sekörlerine kadar farklı alanlarda faaliyet gösteren veri sorumluları hakkında veri ihlal bildirimi konulu karar özetlerinde yüksek miktarda idari para cezaları uygulandığı dikkat çekmekte.

Igili 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 BİLİŞİM ŞİRKETİNİN VERİ İHLAL BİLDİRİMİ HAKKINDA KİŞİSEL VERİLERİ KORUMA KURULUNUN 12/03/2020 TARİH VE 2020/216 SAYILI KARAR ÖZETİ

VERİ SORUMLUSU:
BİR BİLİŞİM ŞİRKETİ

KARAR TARİH: 12/03/2020
KARAR SAYI. : 2020/216

İLGİLİ İLKELER :
KİŞİSEL VERİ İŞLEME GENEL İLKELERİ

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

UYGULANAN YAPTIRIM :
450.000-TL İPC

Veri sorumlusu bilişim şirketi, Kuruma bulunduğu veri ihlal bildirimi ile, sistemlerine siber saldırı gerçekleştirilerek sistemlerinde yer alan verilerin elde edilmeye çalışıldığı bildirilmiş, söz konusu saldırının şirket için sistem geliştirmesi yapan geliştiricilerin hata tespit ve iyileştirme çalışmalarını gerçekleştirdiği debugging özelliği açık olan Pilot isimli uygulamaya, daha önce giriş yapan kişilere ait "PHPSESSID" değeri elde edilerek erişim sağlaması suretiyle meydana geldiği açıklanmıştır.

Saldırganlar tarafından erişilen verilerin neler olduğunun net bir şekilde tespit edilememesine rağmen veri sorumlusunun sistemlerinde yer alan verilerin tümü dikkate alındığında şirketten teklif almış, üyelik oluşturmuş, herhangi bir şekilde hizmet almış, aktif olan veya olmayan **65.993 kişinin yer** aldığı sistemde yer alan içerisinde imza sirküleri, vergi levhası ve kişi kimlik fotokopisi kayıtlarının olduğu **1259 sözleşme** ve 701 alan adı başvuru dosyası bulunduğu bildirilmiştir. Bununla birlikte **50 bin** kredi kartı bilgisi yer aldığı ifade edilmiş, ancak bu kredi kartı bilgilerinin büyük çoğunluğunun son kullanma tarihinin geçmiş olduğu ve kullanılamayacağı, sadece **8 bin** kartın aktif olduğunun tespit edildiği açıklanmıştır.

İhlalden etkilenen kişilerin müşteriler ve potansiyel müşteriler olduğunu ifade eden veri sorumlusu, veri ihlalinden doğrudan etkilenen özel nitelikli bir veri bulunmadığını, ancak tüzel kişi müşterilerin imza sirkülerinde yer alan eski kimlik fotokopilerinde kan grubu ve din bilgisi hanelerinin bulunduğunu bildirmiştir.

Bu kapsamda veri sorumlusu tarafından sistem kayıtlarında 1784 adet eski kimlik fotokopisinin arkalı önlü yüzünün bulunduğu tespit edilmiştir.

Kurul yapmış olduğu incelemeler neticesinde söz konusu ihlale dair 12/03/2020 tarih ve 2020/216 sayılı sayılı Kararı ile;

- Veri sorumlusu tarafından saldırganların eriştiği verilerin neler olduğunun net bir şekilde tespit edilememesinin, kontrol ve uyarı mekanizmalarının etkin bir şekilde kullanılmadığının göstergesi olduğuna,

- Veri sorumlusunun ödeme sistemini değiştirmiş olmasına rağmen sistemde bulunan kredi kartı bilgilerini imha etmeyerek 6698 sayılı Kanunun 4. Maddesi uyarınca işlenen verilerin doğru, güncel, işlendiği amaçla bağlantılı, sınırlı ve ölçülü olma ilkelerine aykırılık teşkil ettiğine,

- Veri sorumlusu tarafından Kuruma gönderilen, ihlalden sonra yapılmış sızma testinde yüksek ve orta seviyede açıklıkların bulunması sebebiyle gerekli teknik tedbirlerin alınmamış olduğunu,

- Veri sorumlusunun ilgili kişilerden veri talep edilen internet adresinde herhangi bir aydınlatma metninin bulunmadığına kanaat getirerek Veri sorumlusu hakkında veri güvenliğini sağlamaya yönelik gerekli teknik tedbirleri almadığı gerekçesiyle **450.000-TL idari para cezasının** uygulanmasına karar verilmiştir

BİR OTOYOL İŞLETMESİNİN VERİ İHLAL BİLDİRİMİ HAKKINDA KİŞİSEL VERİLERİ KORUMA KURULUNUN 16.06.2020 TARİH VE 2021/464 SAYILI KARAR ÖZETİ

VERİ SORUMLUSU:
BİR OTOYOL ŞİRKETİ

KARAR TARİH :16/06/2020
KARAR SAYI : 2020/464

İLGİLİ İLKELER :

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

UYGULANAN YAPTIRIM :
60.000-TL İPC

Veri sorumlusu sıfatına haiz bir otoyol işletmesinin Kuruma intikal eden veri ihlal bildiriminde, çalışanların kendi rıza ve talepleri ile yazılı ve imzalı olarak veri sorumlusuna ilettikleri kişisel e-posta adreslerinin sisteme işlenmesinden sonra bordro programı üzerinden gönderilen bordroların kendilerine ait olmadığı ancak aynı şirket çalışanı olan başka çalışanlara ait olduğunu ve dolayısıyla başkasına ait ad, soyad, T.C. Kimlik No ve sicil numarası görüntülemesi suretiyle veri ihlali gerçekleştiği, ihlalden etkilenen kişi ve kayıt sayısının ise **489** olduğu belirtilmiştir. İhlalin sistemsel bir hata sebebiyle hatalı e-posta gönderimi neticesinde meydana geldiğini bildiren veri sorumlusu, maaş bilgisine dair ise herkeste aynı jenerik bilgisinin görüntülendiğini ifade etmiştir.

Yapılan inceleme sürecinde Kurul tarafından veri sorumlusu şirketten çalışanların neden kişisel e-posta yerine şirket e-postasına gönderim gerçekleştirilmediği ile ilgili bilgi istenmiş; veri sorumlusu, çalışanlarının büyük bir çoğunluğu sahada bulunan bir organizasyon yapısına sahip olunduğundan tüm çalışanlara bir e-posta hesabı tanımlanmadığını, keza şirket e-posta hesaplarına şirketin erişim olanağı bulunduğu da dikkate alınarak bu bildirimlerin çalışanlarının kişisel e-posta hesaplarına yapılmasının daha uygun olacağının değerlendirildiğini belirtmiştir.

Kurul yapmış olduğu incelemeler neticesinde söz konusu ihlale dair 16.06.2020 tarih ve 2021/464 sayılı Kararı ile;

- Çalışanlara yanlışlıkla giden bordroların silinip silinmediğinin kişisel e-posta hesaplarından kontrol imkanı bulunmaması dolayısıyla ihlalin teknik aksaklık değil idari bir eksiklik olduğuna ,
- Bu hususun gerekli risk analizinin yerine getirilmediğini işaret ettiğine,
- Kullanılan aydınlatma metninin de yeterince bilgilendirici bir metin olmadığına,
- Kurumsal e-posta hizmeti alınmadan çalışanların şahsi e-posta hesaplarının kullanılmasının verilerin farklı ülkelerde saklanması durumunu ortaya çıkarabileceği ve veriler üzerinde kontrol kaybı olabileceğinden veri güvenliğini sağlamaya yönelik gerekli teknik ve idari tedbirlerin alınmadığına kanaat getirerek **60.000 TL idari para cezası** uygulanmasına karar vermiştir.

BİR SİGORTA ŞİRKETİNİN ACENTESİNDE GERÇEKLEŞEN VERİ İHLALİ HAKKINDA KİŞİSEL VERİLERİ KORUMA KURULUNUN 16.06.2020 TARİH VE 2020/466 SAYILI KARAR ÖZETİ

VERİ SORUMLUSU:
BİR SİGORTA ŞİRKETİ

KARAR TARİH:16/06/2020
KARAR SAYI : 2020/466

İLGİLİ İLKELER :

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

UYGULANAN YAPTIRIM :
172.000-TL İPC

Veri sorumlusu sigorta şirketinin bir acentesinde işletmelerine ait bilgisayar ekranına bir hacker tarafından erişim sağlanmasıyla veri ihlalinin gerçekleştiği tespit edilmiş, **172** kişinin kimlik ve finans verilerinin etkilendiği, 13.02.2020 tarihinde gerçekleşen ve 20.02.2020 tarihinde tespit edilen veri ihlali, 22.02.2020 tarihinde Kuruma bildirilmiştir.

Bildirim kapsamında gerçekleşen veri ihlalinin veri işleyenin verdiği şikayetçi ifade tutanağı ile anlaşıldığı, ilgili tutanağa göre acente tarafından kullanılan bilgisayarlarda yazışma ekranının açıldığı ve yetkisiz kişinin bu ekran aracılığıyla iletişim kurarak fidye istediği ifade edilmiştir.

Kurul yapmış olduğu incelemeler neticesinde söz konusu ihlale dair 16.06.2020 tarih ve 2020/466 sayılı Kararı ile;

- Veri sorumlusu sigorta şirketinin, veri işleyen acenteye donanımı kendilerinin temin etmediği, vakaya konu bilgisayarın veri işleyenin kendisine ait olduğu, bu nedenle bilgisayar üzerinde aktivite ve kullanıcı kayıtlarının veri sorumlusu tarafından yönetilmediği ve sızma testlerinin yapılmadığı,
- Veri işleyenin herhangi bir şekilde denetlenmemesi Kişisel Veri Güvenliği Rehberi nezdinde düzenlenen veri işleyenler ile ilişkilerin yönetimi tedbirlerine aykırı olduğu,
- Bununla birlikte, veri sorumlusu tarafından ilgili bilgisayarın olayın hemen akabinde formatlanması dolayısıyla gerekli araştırmaların yapılamamış olması, acente yetkilisinin kişisel verilerin korunması ile ilgili eğitimi ihlal sonrasında almış olması, veri işleyen tarafından kullanılan bilgisayar işletim sisteminin eski bir sürüm olması ve güvenlik korumasıyla ilgili güncellemeler desteklememesi, veri ihlali öncesinde anti-virüs yazılımının hiç kullanılmamakta olması gerekli güvenlik önlemlerinin veri sorumlusu ve veri işleyen tarafından tam olarak alınmadığını göstermekte olduğuna kanaat getirerek veri güvenliğini sağlamaya yönelik gerekli teknik ve idari tedbirleri almadığı gerekçesiyle veri sorumlusu hakkında **172.000 TL idari para cezası** uygulanmasına karar verilmiştir.

Bununla birlikte, veri ihlalinden etkilenen 172 ilgili kişiden 95 kişiye veri ihlalinin bildirilmediği, ihlalin bildirildiği 77 kişiden 33'üne bildirimin 26.03.2020, 9'una 16.04.2020, 35'ine 20.04.2020 tarihinde yapıldığı, dolayısıyla ihlalin tespit tarihi ile bildirim tarihleri arasında 1 ayı aşkın süre bulunduğu dikkate alınarak, ilgili kişilere "en kısa sürede" bildirimde bulunma yükümlülüğünü yerine getirmeyen veri sorumlusuna ilgili kişilere bildirim usulünün hatırlatılmasına karar verilmiştir.

BİR SİGORTA ŞİRKETİNİN VERİ İHLAL BİLDİRİMİ HAKKINDA KİŞİSEL VERİLERİ KORUMA KURULUNUN 30.06.2020 TARİH VE 2020/511 SAYILI KARAR ÖZETİ

VERİ SORUMLUSU:
BİR SİGORTA ŞİRKETİ

KARAR TARİH: 30/06/2020
KARAR SAYI. : 2020/511

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

UYGULANAN YAPTIRIM :
100.000-TL İPC

Veri sorumlusu sigorta şirketinin, sağlık sigortası müşterilerine yönelik eczane provizyon uygulamasının 2018 yılında değiştirilmesi esnasında, sürekli ilaç kullanım raporu olan **683** farklı müşterinin ilaç geçmişinin yeni sisteme aktarılması amacıyla ilgili kişilerin kimlik ve ilaç kullanım bilgilerinin yer aldığı bir excel dosyasının oluşturulması amaçlanmış, ancak söz konusu dosyada yer alan bilgilerin provizyon sistemine entegre olarak çalışan doküman yönetim sistemine excel dokümanı olarak sehven bütün halinde yüklenmesi suretiyle veri ihlali meydana geldiği tespit edilmiştir. Söz konusu ihlalden etkilenen kişi sayısı **683** ve kayıt sayısı ise **2413** olup, ihlale konu olan kişisel veri kategorilerinin kimlik, müşteri işlem ve sağlık bilgileri olduğu belirtilmiştir.

Kurul yapmış olduğu incelemeler neticesinde söz konusu ihlale dair 30/06/2020 tarih ve 2020/511 sayılı Kararı ile,

- Yaklaşık sekiz ay kadar devam eden açıklığın dosyaya erişim sağlayan kişi tarafından bilgilendirilinceye kadar veri sorumlusu tarafından tespit edilememiş olması Kişisel Veri Güvenliği Politikalarının ve Prosedürlerinin Belirlenmesi nezdinde yükümlülüklerin yerine getirilmediğini değerlendirmiş,
- Çalışanlara dair yetki matrisi tedbirinin de alınmamış olması dolayısıyla ihlale sebep olan kişisel veri içeren ve yetkisiz kişiler tarafından görüntülenebilir hale gelen excel dosyalarının doküman yönetim sistemine yüklenmesini engelleyecek herhangi bir teknik ve idari tedbir almadığına kanaat getirmiştir.
- Bununla birlikte ihlalden etkilenen kişisel verilerin içinde özel nitelikli kişisel veriler olarak sağlık verilerinin de bulunması nedeniyle, Özel Nitelikli Kişisel Verilerin İşlenmesinde Veri Sorumlularınca Alınması Gereken Yeterli Önlemlere ilişkin ilke kararını gözeten Kurul, kriptografik yöntemler ile muhafaza etme tedbirinin gözetilmediğini tespit etmiş,

- İhlale konu olayda ilgili kişiler önemli bir zarara uğramamış olsa da öğrenilmesi halinde mağduriyete sebep olabilecek nitelikteki verilerin konu olmasını da dikkate alınarak, veri güvenliğini sağlamaya yönelik gerekli teknik ve idari tedbirleri almadığı gerekçesiyle veri sorumlusu hakkında 100.000 TL idari para cezası uygulanmasına karar verilmiştir.

BİR BANKANIN VERİ İHLAL BİLDİRİMİ HAKKINDA KİŞİSEL VERİLERİ KORUMA KURULUNUN 29.09.2020 TARİH VE 2020/744 SAYILI KARAR ÖZETİ

VERİ SORUMLUSU:
BANKA

KARAR TARİH: 29/09/2020
KARAR SAYI. : 2020/744

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

UYGULANAN YAPTIRIM :
275.000-TL İPC

Veri sorumlusu bankanın veri sızıntısı ekibi tarafından Teftiş Kurulu Başkanlığı'na iletilen bildirim ile tespit edilen veri ihlalinde, bir çalışanının veri sorumlusu nezdinde kullandığı e-posta adresine gelen ve ilgili adresten iletilen e-postalara ilişkin kayıtların incelenmesi neticesinde ilgili çalışanın 346 müşteriye ait bilgileri bir word dokümanına işlediği ve söz konusu dokümanı e-posta ile bir yatırım firmasında çalıştığını ve arkadaşı olduğunu iddia ettiği 3. kişiye gönderdiği anlaşılmıştır. Veri sorumlusunun bildirimine göre, söz konusu müşterilerin hepsinin bir yatırım şirketine para transferlerinin bulunduğu ve ihlalden etkilenen kişisel veri kategorilerinin kimlik, iletişim, müşteri işlem ve finans verileri olduğu tespit edilmiştir.

Kurul yapmış olduğu incelemeler neticesinde söz konusu ihlale dair 29.09.2020 tarih ve 2020/744 sayılı Kararı ile;

İhlal ile ilgili olan personelin veri ihlalinin gerçekleşmesinden 1 seneyi aşkın süre önce 09.10.2018 tarihinde "Kişisel Verilerin Korunması Kanunu" eğitimini tamamlamış olmasına rağmen, bahse konu eğitimden sonra bizzat ihlali gerçekleştirmiş olmasının verilen eğitimin yeterli olup olmadığı konusunda şüpheler oluşturduğunu belirterek, banka dışına giden e-postalara ilişkin Ver Sızıntısı Tespit/Önleme Sisteminin mevcut olduğunun belirtilmesine rağmen söz konusu ihlale neden olan e-postanın DLP sistemler tarafından engellenmemesi ve ihlale sebep olan çalışanın kişisel verilerin aktarımı gerçekleştirebildiği dikkate alındığında Kişisel Veri Güvenliği Rehberi nezdinde düzenlenen mevcut risk ve tehditlerin belirlenmesine ilişkin hususlara dair veri sorumlusunun aldığı tedbirlerin yetersiz olduğuna kanaat getirilmiştir.

Veri güvenliğini sağlamaya yönelik teknik ve idari tedbirleri almayan veri sorumlusu hakkında 225.000-TL para cezası uygulanmasına karar vermiştir.

Bununla birlikte ilgili kişilere bildirimlerin yapılması ve söz konusu bildirim örneklerinin Kuruma gönderilmesine rağmen, ihlalin 31.10.2019 tarihinde gerçekleştiği ve Bankanın Teknoloji Veri Sızıntısı ekibi tarafından 04.11.2019 tarihinde Teftiş Kurulu Başkanlığı'na iletildiği, veri ihlali bildiriminin ise 06.12.2019 tarihinde gerçekleştirdiği dikkate alındığında veri ihlalinin öğrenilmesinden itibaren başlayan 72 saatlik süre içerisinde bildirimde bulunma yükümlülüğüne uyulmaması sebebiyle ver sorumlusuna ayrıca 50.000-TL idari para cezası uygulanmasına karar verilmiştir.

“BİR SİGORTA ŞİRKETİNİN VERİ İHLAL BİLDİRİMİ HAKKINDA” KİŞİSEL VERİLERİ KORUMA KURULUNUN 25.02.2021 TARİH VE 2021/154 SAYILI KARAR ÖZETİ

VERİ SORUMLUSU:
BİR SİGORTA ŞİRKETİ

KARAR TARİH: 25/02/2021
KARAR SAYI. : 2021/154

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

UYGULANAN YAPTIRIM : 150.000-TL İPC

Kuruma intikal eden veri ihlal bildiriminde veri sorumlusu sigorta şirketinin eski bir çalışanının görevi gereği erişimi bulunan bazı müşterilere ait kişisel verileri kurumsal e-posta adresinden gmail uzantılı şahsi e-posta adresine 3 ayrı tarihte ve 3 ayrı excel dosyasında göndermesiyle veri ihlali gerçekleştiği bildirilmiştir. Veri sorumlusu şirket tarafından tespit edilemeyip, ihlale sebep olan çalışanın yeni işvereni tarafından tespit edilen veri ihlalinden etkilenen 544 kişinin kimlik, iletişim ve araç plaka numaraları verilerinin etkilendiği ve bu kişilerden 422’sine ulaşılarak ihlalin gerçekleşme tarihi, kapsamı ve muhtemel etkileri hakkında bizzat bilgi verildiği belirtilmiştir.

Kurul yapmış olduğu incelemeler neticesinde söz konusu ihlale dair 25/02/2021 tarih ve 2021/154 sayılı Kararı ile,

DLP sistemleri ile kişisel verilerin bulunduğu belgelerin e-posta ile kurum dışında gönderilmesinin engellenmesinin mümkün olduğunu belirten Kurul, veri sorumlusunun DLP sisteminin ihlale konu e-postaların gönderilmesini engelleyememiş olmasını Kişisel Veri Güvenliği Rehberi nezdinde düzenlenen yazılım ve donanımların kurulum ve yapılandırma işlemlerine tabi tutulmasına ilişkin siber güvenlik tedbirine doğru uymaması olarak değerlendirmiştir. Bununla birlikte, eski çalışanın kendi kişisel e-posta adresine yapmış olduğu gönderimin DLP raporuna yansımaması da tüm kullanıcıların işlem hareketleri kaydının düzenli olarak tutulması tedbirine aykırılık teşkil etmektedir.

İhlale konu e-posta gönderimlerinin veri sorumlusu tarafından tespit edilemeyişi erişim kontrolü kayıtlarının ve diğer raporlama araçlarının düzenli kontrol edilmediğini göstermediği anlaşılmış, ayrıyeten verilen kişisel verileri koruma eğitimlerinin eksikliği de veri sorumlusunun kişisel verilerin korunması hakkında eğitim verilmesine yeterli önemi vermediği yönünde değerlendirilmiştir. Bütün bu hususlar dikkate alınarak, veri güvenliğini sağlamaya yönelik gerekli teknik ve idari tedbirleri almadığı gerekçesiyle veri sorumlusu hakkında 150.000-TL idari para cezası uygulanmasına karar verilmiştir.

“BİR SİGORTA ŞİRKETİNİN VERİ İHLAL BİLDİRİMİ HAKKINDA” KİŞİSEL VERİLERİ KORUMA KURULUNUN 04.03.2021 TARİH VE 2021/187 SAYILI KARAR ÖZETİ

VERİ SORUMLUSU:
BİR SİGORTA ŞİRKETİ

KARAR TARİH: 04/03/2021
KARAR SAYI. : 2021/187

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

UYGULANAN YAPTIRIM : 125.000-TL İPC

Kuruma intikal eden veri ihlal bildiriminde bir emeklilik hizmeti kapsamında veri sorumlusu sigorta şirketinin müşterisi olan bazı firmalara sigorta hizmetine dâhil olan çalışanlarına dair “Rapor” iletildiği, ancak veri sorumlusunun bilgi sistemleri hizmeti aldığı destek hizmeti sağlayıcısında meydana gelen sistemsel hata nedeniyle müşteriler ile raporların ilişkilendirilmesinde teknik bir hata meydana geldiği, ve neticesinde ilgili raporun sistem hizmeti kapsamındaki 28 müşteri şirkete, diğer 31 müşteri şirketin sisteme dâhil çalışanlarına dair "Rapor" dosyası gönderildiği bildirilmiştir. Bu ihlal sonucunda sistem kapsamında olan 31 işveren şirket çalışanı 681 adet gerçek kişi müşteriye ait bilgilerin, yine sistem kapsamındaki 28 işveren şirkete gönderildiği ifade edilmiştir.

Kurul yapmış olduğu incelemeler neticesinde söz konusu ihlale dair 04.03.2021 tarih ve 2021/187 sayılı Kararı ile;

Veri ihlaline sebep olan sistemsel hatanın uygulama yazılımından kaynaklanmasından hareketle Kişisel Veri Güvenliği Rehberi nezdinde bu tip hataların işlem yayına alınmadan önce düzeltilmesi gerektiği ifade edilerek, ihlale konu olayın gerçekleşme tarihi ile tespit tarihi arasında yaklaşık iki yıllık gecikmenin bulunmasının veri sorumlusunun gerekli kontrol ve denetimleri zamanında yapmadığının göstergesi olduğu değerlendirilmiştir.

Bununla birlikte, ihlalin raporu alan müşteri firmanın konu hakkında veri sorumlusuna bilgi vermesi sonucu tespit edilmesi ve veri sorumlusu tarafından kendiliğinden tespit edilememesini Kişisel Veri Güvenliğinin Takibi gereği sızma testi uygulama tedbirlerine uyulmadığını gösterdiğini belirten Kurul veri güvenliğini sağlamaya yönelik gerekli teknik ve idari tedbirleri almadığı gerekçesiyle veri sorumlusu hakkında 125.000-TL idari para cezası uygulanmasına karar vermiştir.

Ek olarak, yaşanan veri ihlalinin ilgili kişilere bildirilmesine ilişkin usul ve esaslara uygun olarak bildirimde bulunmadığı tespit edilen veri sorumlusunun, ilgili kişilere yapılacak bildirimin Kurulun 18.09.2019 tarih ve 2019/271 sayılı Kararı ile belirlenen asgari unsurları taşıması gerektiği belirtilerek, bundan sonra ilgili kişilere yapılacak bildirimlerde usulüne uygun olarak bildirimde bulunulması hususunda talimatlandırılmasına karar verilmiştir.

“BANKACILIK SEKTÖRÜNDEKİ VERİ SORUMLUSUNUN VERİ İHLAL BİLDİRİMİ HAKKINDA” KİŞİSEL VERİLERİ KORUMA KURULUNUN 04.03.2021 TARİH VE 2021/190 SAYILI KARAR ÖZETİ

VERİ SORUMLUSU: BANKA

KARAR TARİH: 04/03/2021
KARAR SAYI. : 2021/190

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

UYGULANAN YAPTIRIM : 100.000-TL İPC

Kuruma intikal eden veri ihlal bildiriminde bir müşteri şikâyeti üzerine veri sorumlusu banka tarafından yapılan inceleme neticesinde, bir şube çalışanının kendisine tanımlanan Müşteri Bilgileri ve Belgeleri gözlem yetkisini, ilgili müşterinin kimlik görüntüsünü amacı dışında gözlemlemek ve müşteriye ait gözlemlenen bilgilerin şahsi cep telefonu ile fotoğrafını çekerek üçüncü kişiyle paylaşmak suretiyle kötüye kullanması sonucu veri ihlali gerçekleştiği tespit edilmiştir. Bildirilen veri ihlalinin, banka sistemleriyle ilgili bir güvenlik açığı sonucu değil, bir şube çalışanının kendisine tanımlanan Müşteri Bilgileri ve Belgeleri gözlem yetkisini amacı dışında kullanmasından ve 1 (bir) müşterinin kimlik bilgilerini yetkisiz kişiyle paylaşmasından kaynaklandığını ifade eden veri sorumlusu, ihlal ile ilgili olan çalışanların kişisel verilerin korunması ve gizliliğine ilişkin gerekli eğitimleri aldığını belirtmiştir.

Kurul yapmış olduğu incelemeler neticesinde söz konusu ihlale dair 04.03.2021 tarih ve 2021/190 sayılı Kararı ile;

Veri sorumlusu tarafından verilen veri gizliliği ve güvenliği eğitimlerine rağmen söz konusu çalışanın rol ve sorumlulukları hakkındaki farkındalığının sağlanamamasının ve çalışanların istediği sıklıkta ve sayıda sorgulama yaparak müşteri bilgilerini sorgulayabilmesinin Kişisel Veri Güvenliği Rehberi nezdinde düzenlenen çalışanların eğitilmesi ve farkındalık çalışmalarına ilişkin tedbirlere aykırılık teşkil ettiği belirtilerek, söz konusu ihlalden ancak yaklaşık iki yıl sonra çalışanlar için sorgulama kota limitinin oluşturulmasının veri güvenliği ölçülü erişim tedbirlerine aykırı olduğuna kanaat getirilmiştir. Veri ihlali öncesinde müşteri bilgilerini sorgulamak isteyen çalışanlara erişecekleri verileri iş ihtiyacı kapsamında ve görev tanımıyla uyumlu bir şekilde kullanabileceklerine dair uyarı sisteminin bulunmadığı hususu da dikkate alınarak veri güvenliğini sağlamaya yönelik gerekli teknik ve idari tedbirleri almadığı gerekçesiyle veri sorumlusuna 100.000-TL idari para cezası uygulanmasına karar verilmiştir.

BİR KOZMETİK ŞİRKETİNİN VERİ İHLAL BİLDİRİMİ HAKKINDA" KİŞİSEL VERİLERİ KORUMA KURULUNUN 25.03.2021 TARİH VE 2021/311 SAYILI KARAR ÖZETİ

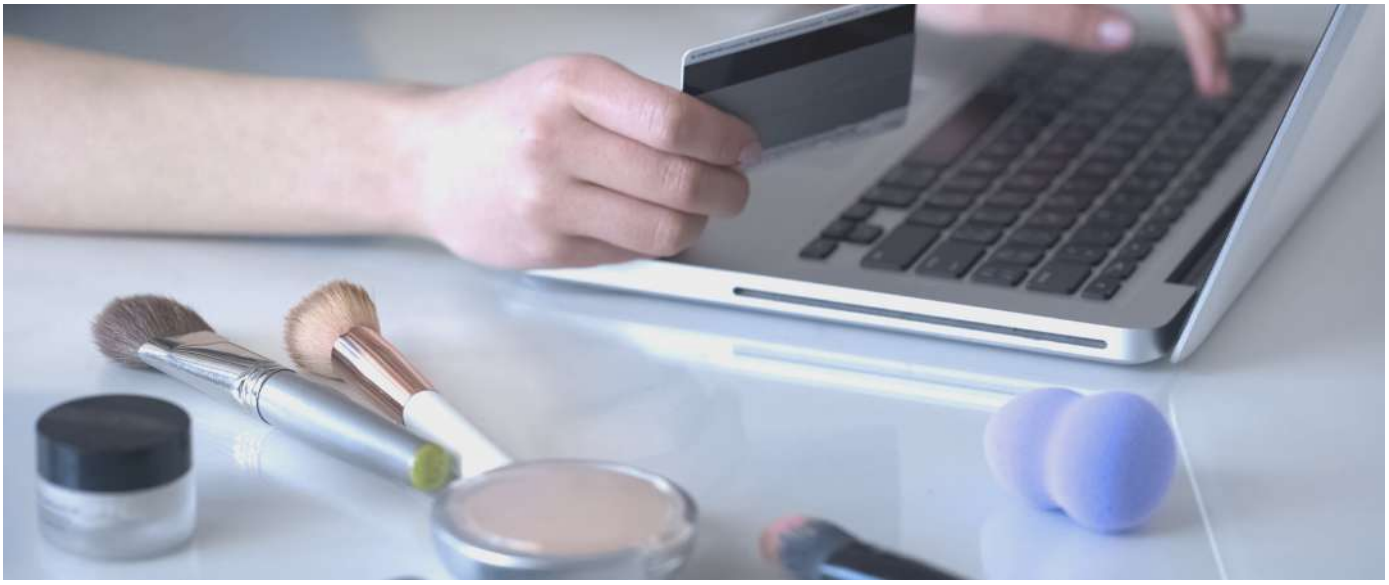
VERİ SORUMLUSU:
BİR KOZMETİK ŞİRKETİ

KARAR TARİH: 25/03/2021
KARAR SAYI. : 2021/311

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

UYGULANAN YAPTIRIM : 200.000-TL İPC

Kuruma intikal eden veri ihlali bildirimi itibariyle, 18.05.2020 tarihinde veri sorumlusu bir kozmetik şirketinin internet sitesinde yer alan yeni bir kampanya sebebiyle siteye yüksek erişim sağlandığı ve uygulama sunucularının yetersiz kaldığı düşünülerek, veri işleyen tarafından sitenin çalışmaması ihtimali gözetilmek suretiyle sitenin mevcut halinin kopyalarının çıkarılıp yeni uygulama sunucuları eklenirken müşterilere sayfanın statik kopyasının gösterilmesinin amaçlandığı, ancak bu işlem gerçekleştirilirken teknik bir aksaklık nedeniyle veri ihlali yaşandığı ifade edilmiştir. İhlal bildirimine göre, söz konusu işlem gerçekleştirilirken DDos ataklarını önlemek için kullanılan ve veri işleyenin üçüncü kişiden aldığı hizmetin içinde tanımlanan bir fonksiyon sebebiyle yalnızca mevcut arayüzün değil kullanıcı profillerin de bir kopyası oluşturulmuş, üye olarak giriş yapan kullanıcılara rastgele kopyası alınan kullanıcı profillerinin bilgileri de görünür halde gelmiştir.



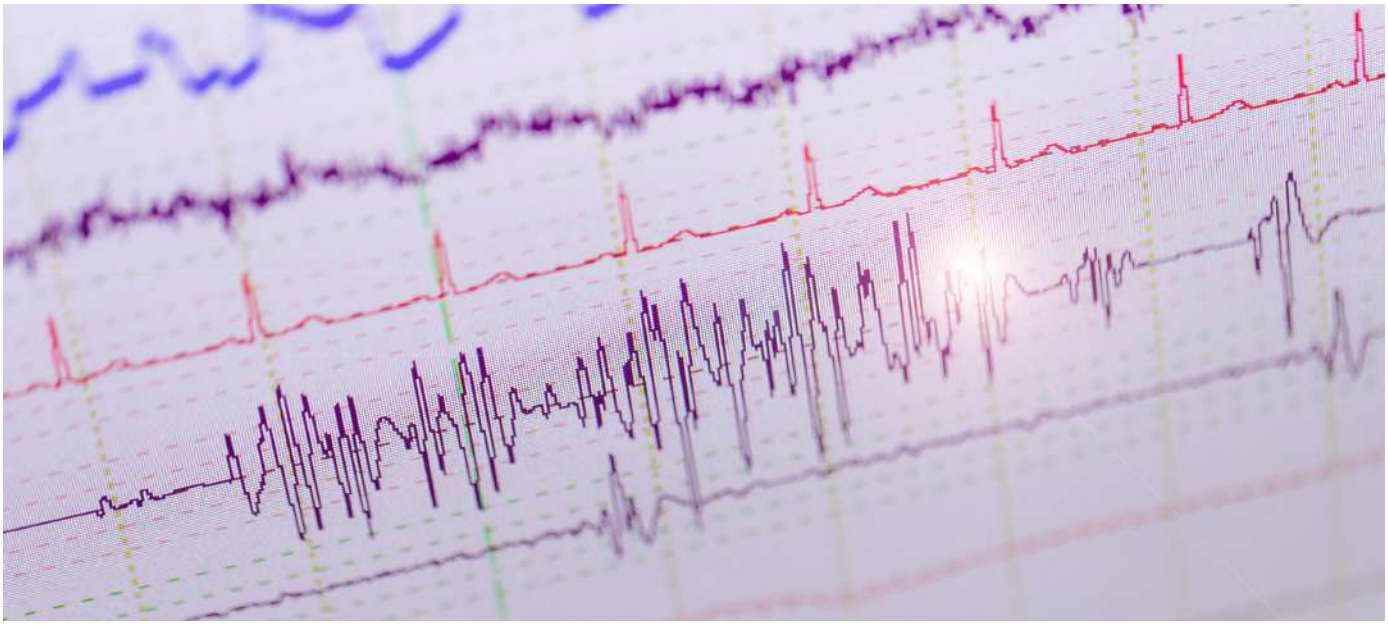
Veri sorumlusu şirket tarafından yapılan bildirimde, görüntülenen profillerde ad-soyad, e-posta, adres gibi kişisel verilerin yer aldığı ve kredi kartı gibi finansal hiçbir verinin bulunmadığı belirtilirken, sitenin olağan dışı davranışlarının tarafına gelen bildirimlerle kısa sürede fark edildiği ve sitenin erişime kapatılıp normal çalışma düzenine çekildiği, ancak müdahale edilene kadar geçen 48 dakikalık süre zarfında toplamda 24 kişinin bilgisinin farklı üyeler tarafından görünür olduğunun tahmin edildiği ifade edilmiştir.

Kurul yapmış olduğu incelemeler neticesinde söz konusu ihlale dair 25.03.2021 tarih ve 2021/311 sayılı Kararı ile;

Kaç kişinin hangi üyelerin profilini görmüş olabileceği hakkında net bir sayı belirtilemediği ve oluşan hatanın kampanya sırasında ve yoğunluğun yüksek düzeyde olduğu dakikalarda olmasından ötürü bu kişilerin kişisel verilerin çok sayıda kişi tarafından görünmüş olabileceği dikkate alınarak,

veri sorumlusu tarafından kampanya sebebiyle yoğunluğun yüksek olacağının öngörülerek bu yoğunluğa uygun bir şekilde yazılımın kontrollerinin gerçekleştirilmesinin ardından uygulamaya konulması gerektiği, başka bir deyişle veri sorumlusu tarafından sitede yapılacak değişiklik ve güncellemelerin sitenin yoğun çalıştığı zaman diliminde yapılmayıp siteye girişin en düşük olduğu saatlerde ve bu tarz ihlallerin yaşanmaması adına sitenin kapatılarak yapılması gerektiği belirtilmiştir. Bu hususun Kişisel Veri Güvenliği Rehberi (Teknik ve İdari Tedbirler)'nde 3.5. Bilgi Teknolojileri Sistemleri Tedariği, Geliştirme ve Bakımı başlığı altında belirtilen tedbirlere uygun düşmediğini, ayrıca şifreleme ve veri maskeleme önlemlerini zamanında yerine getirmeyen veri sorumlusunun risk odaklı bir yaklaşım ile hareket etmediği gözetilerek hakkında veri güvenliğini sağlamaya yönelik gerekli tedbir ve idari tedbirlerin alınmadığı gerekçesiyle 200.000 TL dar para cezası uygulanmasına karar vermiştir.

“BİR HASTANENİN VERİ İHLAL BİLDİRİMİ HAKKINDA” KİŞİSEL VERİLERİ KORUMA KURULUNUN 20/04/2021 TARİH VE 2021/407 SAYILI KARAR ÖZETİ



VERİ SORUMLUSU: HASTANE

KARAR TARİH: 20/04/2021
KARAR SAYI. : 2021/407

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

UYGULANAN YAPTIRIM : 600.000-TL İPC

Veri sorumlusu sıfatını haiz hastane tarafından Kuruma intikal eden veri ihlal bildirimi nezdinde, hastanede çalışan hekimin hastalarına at dosyaların arşivden alınarak kendisinin talimatıyla bazı hastane çalışanlar aracılığıyla hastane dışına çıkarılmasıyla gerçekleşen veri ihlalinin dosyaları hastane dışına çıkarmaya teşebbüs eden bir çalışanın görülmesinden 17 gün sonra kamera kayıtlarının incelenmesi neticesinde tespit edildiği bildirilmiş, ihlalden 789 hastanın kimlik, iletişim, sağlık bilgileri ve genetik verilerin hasta kartında yer alan bilgiler ve birçok özel nitelikli kişisel verinin etkilendiği belirtilmiştir.

Kurul yapmış olduğu incelemeler neticesinde söz konusu ihlale dair 20/04/2021 tarih ve 2021/407 sayılı Kararı ile,

Veri sorumlusu tarafından çalışanlara tanımlanan kişisel verilerin korunması eğitiminin tamamlanmasının sağlanmadığı, eski çalışanın kişisel verilerin korunması ile ilgili eğitim almış olmasına rağmen arşiv odasındaki belgelerin taşınmasına yardım ettiğinin anlaşıldığı dikkate alındığında veri sorumlusu tarafından çalışanlara yeterli eğitimin verilmediğinin anlaşıldığı, nitekim ihlali gerçekleştiren ve diğer çalışanların Başhekimliğin izin ve onayı bulunmaksızın arşiv odasına girebildiği ve hasta dosyalarını dışarı çıkarabilmesi sebebiyle hastalara at kayıtların tutulduğu arşiv odasına yetkili olmayan kişilerin girmemesini sağlayacak yeterli tedbirlerin alınmadığının anlaşıldığı belirtilmiştir. Bununla birlikte, ihlal şüphesini doğuran olayların bulunmasına rağmen ihlalin 17 gün sonra tespit edilmesinin veri sorumlusu tarafından kişisel veri güvenliği politika ve prosedürlerinin iyi bir şekilde hazırlanmadığı veya takip edilmediği, ayrıca bu durumun alınan mevcut güvenlik önlemlerinin etkili kullanılamadığının da göstergesi olduğuna kanaat getirilmiştir. Ek olarak, kamera kayıtlarının ancak ihlal anlaşıldıktan sonra kontrol edilmesinin Özel Nitelikli Kişisel Verilerin İşlenmesinde Veri Sorumlularınca Alınması Gereken Yeterli Önlemler ile ilgili kararında yer alan özel nitelikli kişisel verilerin bulunduğu fiziksel ortamların güvenliğinin sağlanarak yetkisiz giriş çıkışların engellenmesi tedbirinin alınmadığının göstergesi olduğu ifade edilmiştir.

Veri sorumlusu hastane tarafından alınan mevcut güvenlik önlemlerinin iyi bir şekilde alınamaması ve kullanılamaması nedeniyle ihlalin tespit edilmesi ve önlenmesine yönelik tedbirlerin zamanında ve yeterli ölçüde alınamadığına kanaat getiren Kurul, izinsiz olarak hastaneden çıkarılan birçok hasta dosyasının akıbetinin hala bilinmemesinin de risklerin azaltılmasına dair yeterli tedbir alınmadığının göstergesi olduğunu gözeterek veri güvenliğini sağlamaya yönelik gerekli tedbirleri almayan veri sorumlusu hakkında 450.000-TL idari para cezası uygulanmasına karar vermiştir.

Ayrıca ihlalin tespit edilmesinden 25 gün sonra Kurum'a bildirilmesi ve hastaneye gelen bir kişi dışında ilgili kişilerden hiçbirine ihlalin bildirilmemiş olduğu hususları dikkate alındığında bildirim yükümlülüğünü yerine getirmediği gerekçesiyle veri sorumlusuna ayrıca 150.000-TL idari para cezası uygulanmasına karar verilmiş ve ilgili kişilere usulüne uygun bir bildirim yapılarak sonucundan Kurula bilgi verilmesi hususunda talimatlandırılmıştır.