KİŞİSEL VERİLERİ KORUMA KURULU'NUN YENİ YAYINLANAN KARAR ÖZETLERİ

1- BİR PAREKENDE GİYİM FİRMASININ VERİ İHLAL BİLDİRİMİNE İLİŞKİN KARAR

2- ELEKTRONİK SATIŞ HİZMETİ SAĞLAYAN BİR ŞİRKETİN VERİ İHLAL BİLDİRİMİNE İLİŞKİN KARAR

3- BİR BANKANIN VERİ İHLAL BİLDİRİMİNE İLİŞKİN KARAR

4- BİR SİGORTA ŞİRKETİNİN VERİ İHLAL BİLDİRİMİNE İLİŞKİN KARAR

5- BİR OYUNCAK PAREKENDECİSİNİN VERİ İHLAL BİLDİRİMİNE İLİŞKİN KARAR

6- BİR E-TİCARET ŞİRKETİNİN VERİ İHLAL BİLDİRİMİNE İLİŞKİN KARAR

7- BİR TEKNOLOJİ ŞİRKETİNİN VERİ İHLAL BİLDİRİMİNE İLİŞKİN KARAR

8- BİR İLAÇ ŞİRKETİNİN VERİ İHLAL BİLDİRİMİNE İLİŞKİN KARAR

Turgut AVUKATLIK DANIŞMANLIK Attorneyship & Consultancy

1.Bir Perakende Giyim Firmasının Veri İhlal Bildirimi Hakkında Karar

Kişisel Verileri Koruma Kurulu'nun işbu Kararına konu veri ihlal bildiriminde; veri sorumlusu tarafından kısaca;

- 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 ve 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 ve ilgili kişilere 23.07.2019 tarihinde e-posta yoluyla bildirim yapıldığı

ifade edilmiştir.

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 veri sorumlusu hakkında **50.000 TL idari para cezası** uygulanmasına karar verilmiştir.

2. Elektronik Satış Hizmeti Sağlayan Bir Şirketin Veri İhlal Bildirimi Hakkında Karar

Kişisel Verileri Koruma Kurulu'nun işbu Kararına konu veri ihlal bildiriminde; veri sorumlusu tarafından kısaca;

- 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

ifade edilmiştir.

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 **200.000 TL idari para cezası** uygulanmasına karar verilmiştir.

3. Bir Bankanın Veri İhlal Bildirimi Hakkında Karar

Kişisel Verileri Koruma Kurulu'nun işbu Kararına konu veri ihlal bildiriminde; veri sorumlusu tarafından kısaca;

- Veri sorumlusu Şirketin e-ticaret sektöründe faaliyet göstermekte olduğu,
- 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,

ifade edilmiştir.

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 alınarak Banka hakkında **75.000 TL idari para cezasının** uygulanmasına karar verilmiştir.

4. Bir Sigorta Şirketinin Veri İhlal Bildirimi Hakkında Karar

Kişisel Verileri Koruma Kurulu'nun işbu Kararına konu veri ihlal bildiriminde; veri sorumlusu tarafından kısaca;

- 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

ifade edilmiştir.

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 şirket hakkında **90.000 TL idari para cezası** uygulanmasına karar verilmiştir.

5. Bir Oyuncak Perakendecisinin Veri İhlal Bildirimi Hakkında Karar

Kişisel Verileri Koruma Kurulu'nun işbu Kararına konu veri ihlal bildiriminde; veri sorumlusu tarafından kısaca;

- 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

ifade edilmiştir.

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

- değerlendirmelerinden hareketle şirket hakkında **75.000 TL idari para cezası** uygulanmasına karar verilmiştir. Bununla birlikte **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 bulunmadığı ifade edilmiştir.**

6. Bir E-Ticaret Şirketinin Veri İhlal Bildirimi Hakkında Karar

Kişisel Verileri Koruma Kurulu'nun işbu Kararına konu veri ihlal bildiriminde; veri sorumlusu tarafından kısaca;

- 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

ifade edilmiştir.

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 şirket hakkında **165.000 TL idari para cezası** uygulanmasına karar verilmiştir.

7. Bir Teknoloji Şirketinin Veri İhlal Bildirimi Hakkında Karar

Kişisel Verileri Koruma Kurulu'nun işbu Kararına konu veri ihlal bildiriminde; veri sorumlusu tarafından kısaca;

- 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

ifade edilmiştir.

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.**

8. Bir İlaç Şirketinin Veri İhlal Bildirimi Hakkında Karar

Kişisel Verileri Koruma Kurulu'nun işbu Kararına konu veri ihlal bildiriminde; veri sorumlusu tarafından kısaca;

- 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

ifade edilmiştir.

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 karar verilmiştir.