Temmuz 2021

KVKK KURUL KARARLARI

BERKER BERKER

Yayım Tarihi : 05/07/2021
Karar Tarihi : 12/03/2020
Karar No : 2020/216
Konu Özeti : **Bir bilişim şirketinin kişisel veri ihlali bildirimi**

Veri sorumlusunun Kurumumuza intikal eden veri ihlal bildiriminde;

- Veri sorumlusu Şirketin sistemlerine siber saldırı gerçekleştirilerek sistemlerinde yer alan verilerin elde edilmeye çalışıldığı,

- Pilot adı verilen uygulamada debugging özelliğinin açık olduğu ve şirket için sistem geliştirmesi yapan geliştiricilerin bu özelliği kullanarak uygulamadaki hataları tespit ettiği ve iyileştirme gerçekleştirdiği,

- İhlale konu siber saldırı ile Pilot uygulamasına internet üzerinden erişim sağlamaya çalışan kişinin(lerin), uygulamaya daha önce giriş yapmış kişilere ait “PHPSESSID” değerini elde ettiği ve Pilot uygulamasına erişim sağladığı,

- Debugging özelliğinin açık olmasının sebebinin sisteme internet üzerinden erişilerek geliştirmelerin yapılmasına olanak sağlamak olduğu, ancak bu durumun internet üzerinden siber saldırılar gerçekleştirilerek sisteme erişilmesine olanak tanıdığı,

- Sistemde saldırganlar tarafından erişilen verilerin neler olduğunun net bir şekilde tespit edilemediği ancak veri sorumlusunun sistemlerinde yer alan verilerin tümü dikkate alındığında sistemde 65.993 kişinin yer aldığı, bu kişilerin sadece teklif almış, üyelik oluşturmuş, herhangi bir şekilde hizmet almış, aktif olan ve olmayan kişileri içerdiği,

- İlgili kişilere ilişkin sistemde yer alan kayıtların 1259 sözleşme, 701 alan adı başvuru dosyası (içerisinde imza sirküleri, vergi levhası ve kişi kimlik fotokopisi kayıtları) olduğu,

- Sistemde ayrıca 50.000 kredi kartı bilgisi yer aldığı, ancak bu kredi kartı bilgilerinin büyük çoğunluğunun son kullanma tarihinin geçmiş olduğu ve kullanılamayacağı, sadece 8000 kartın aktif olduğunun tespit edildiği,

- İhlalden etkilenen kişi kategorilerinin müşteriler ve potansiyel müşteriler olduğu,

- Saldırganların hangi verilere eriştiklerinin tespit edilemediği, sistemde yer alan verilerin kimlik, iletişim, işlem güvenliği (kullanıcı adı ve parola bilgileri), ödeme Bilgileri (kredi kartı numarası) olduğu,

- Ele geçirilen kredi kartı bilgilerinin 2018 tarihi öncesinde veri sorumlusu Şirkete aktarılan bilgiler olduğu, 2016 tarihi itibari ile ödeme hizmetlerinde iyileştirme çalışmaları kapsamında bir proje başlatıldığı, 2018 yılı itibariyle kredi kartı bilgilerinin yetkilendirilmiş ödeme hizmet sağlayıcıları üzerinden toplanmakta ve onlar tarafından saklanmakta olduğu,

- Veri ihlalinden doğrudan etkilenen özel nitelikli bir veri bulunmadığı, ancak tüzel kişi müşterilerin imza sirkülerinin ekinde yer alan eski kimlik fotokopilerinde kan grubu ve din bilgisi hanelerinin bulunduğu ve bazı imza sirkülerinde kimlik fotokopisinin arka yüzünün de yer alabildiği dikkate alınarak; bazı müşteriler için saldırganların bu verilere de erişme ihtimali olabileceği,

- Sistemde yer alan tüm kayıtların incelendiği ve sayımlarda (imza sirkülerlerinde yer alan kimlik fotokopileri de dahil) 1.784 adet eski kimlik fotokopisinin arkalı önlü yüzünün bulunduğunun tespit edildiği,

- İhlalden etkilenen tüm müşterilere e-posta göndermek suretiyle bildirimde bulunulduğu, bir kısım müşterilere mümkün olduğunca telefonla da bilgilendirme gerçekleştirildiği

ifadelerine yer verilmiştir.

Söz konusu bildirimin incelenmesi neticesinde Kişisel Verileri Koruma Kurulunun 12/03/2020 tarih ve 2020/216 sayılı sayılı Kararı ile;

- Sistemde saldırganlar tarafından erişilen verilerin neler olduğunun net bir şekilde tespit edilememesinin, veri sorumlusu tarafından sızma veya herhangi bir anomali olup olmadığının belirlenmesi noktasında kontrol ve uyarı mekanizmalarının etkin bir şekilde kullanılmadığının göstergesi olduğu,

- Veri sorumlusu tarafından hangi kişisel verilerin etkilendiğinin tespit edilemediği ancak sistemlerde 65.993 kişinin yer aldığı, bu kişilerin sadece teklif almış, üyelik oluşturmuş, herhangi bir şekilde hizmet almış, aktif olan ve olmayan kişileri içerdiği, bu kişilerden 1.784 tanesinin eski kimlik fotokopisinin arkalı önlü yüzünün bulunduğu ayrıca 50.000 kredi kartı bilgisi yer aldığı,

- Veri sorumlusunun kredi kartı bilgilerinin büyük çoğunluğunun son kullanma tarihinin geçmiş olduğu ve kullanılamayacağı, sadece 8000 kartın aktif olduğu, 2018 yılı itibariyle kredi kartı bilgilerinin yetkilendirilmiş ödeme hizmet sağlayıcıları üzerinden toplandığı ve onlar tarafından saklandığı bu çerçevede veri sorumlusunun ödeme sistemini değiştirmiş olmasına rağmen sistemde bulunan kredi kartı bilgilerini imha etmeyerek 6698 sayılı Kişisel Verilerin Korunması Kanununun **("Kanun")** 4. Maddesinin 2. Fıkrasının (b) ve (ç) bendine aykırı hareket ettiği,

- Şirket dışından erişim için güvenlik amacıyla VPN ile Şirket IP'sine bağlanıldığı ve kişilere özel kullanıcı adı ve VPN şifresi verildiği, saldırganların da sisteme SFTP ve VPN aracılığı ile bağlandığı, ihlalden sonra 29.01.2020 tarihinde yapılan ve veri sorumlusu tarafından Kurumumuza gönderilen sızma testinde özellikle web uygulamalarında yüksek ve orta seviyede açıklıkların tespit edildiği göz önüne alındığında bu durumun veri sorumlusu tarafından gerekli teknik tedbirlerin alınmadığının göstergesi olduğu,

- Veri sorumlusunun https://www.****.com.tr adresinde domain ve hosting hizmetlerinin satın alındığı ekranları incelendiğinde satın alma süreçlerinde kimlik ve iletişim bilgilerinin talep edildiği ancak herhangi bir aydınlatma metninin bulunmadığı göz önüne alındığında veri sorumlusunun 6698 sayılı Kişisel Verilerin Korunması Kanunu kapsamında yükümlülüklerini yeterli seviyede yerine getirmediği kanaatine varıldığı,

- Veri sorumlusu tarafından ihlal öncesi alınması gereken teknik tedbirlerin (çift faktör özelliği olan sistemlerde bu özelliğin aktifleştirilmesi, VPN erişimde kullanılan sertifikaların yenilenmesi, çalışanlarının e-posta erişimlerinin iki aşamalı kimlik doğrulama olarak güncellenmesi, log kayıtlarının adli olaylarda kanıt niteliğinde kullanılabilmesi için zaman damgasıyla damgalanması, logların korelasyonunun sağlanması vb.) ihlal sonrası devreye alınmasının gerekli teknik ve idari tedbirlerin alınmadığının göstergesi olduğu

değerlendirmelerinden hareketle, Kanunun 12. maddesinin 1 numaralı fıkrası çerçevesinde veri güvenliğini sağlamaya yönelik gerekli teknik tedbirleri almayan veri sorumlusu hakkında Kanunun 18. Maddesinin 1. Fıkrasının (b) bendi uyarınca **450.000 TL idari para cezasının uygulanmasına,**

- Veri ihlalinin 09.10.2019 tarihinde 14:04'de gerçekleştiği, 11.10.2019 tarihinde saat 14.04'de veri sorumlusu tarafından tespit edildiği, 14.10.2019 tarihinde **Kurula 72 saat içinde bildirildiği dikkate alındığında bu hususta yapılacak bir işlem bulunmadığına**

karar verilmiştir.

Yayım Tarihi : 05/07/2021
Karar Tarihi : 20/04/2021
Karar No : 2020/407
Konu Özeti : **Bir hastanenin veri ihlali bildirimi**

Veri sorumlusu bir hastane tarafından Kuruma intikal ettirilen veri ihlal bildiriminde;

- Veri ihlalinin; hastanede çalışan hekimin hastalarına ait dosyaların arşivden alınarak kendisinin talimatıyla bazı hastane çalışanları aracılığıyla hastane dışına çıkarılmasıyla gerçekleştiği,

- Veri ihlalinin; dosyaları hastane dışına çıkarmaya teşebbüs eden bir çalışanın görülmesinden 17 gün sonra kamera kayıtlarının incelenmesi neticesinde tam olarak tespit edildiği,

- İhlalden; 789 hastanın etkilendiği,

- İhlalden; kimlik, iletişim, sağlık bilgileri ve genetik verilerin hasta kartında yer alan bilgiler *(T.C Kimlik numarası, adı, soyadı, baba adı, ana adı, sosyal güvenlik numarası, özel sigorta, anlaşmalı kurum, çalıştığı kurum, uyruğu, doğum tarihi, cinsiyet, medeni hali, kan grubu, mesleği, vergi dairesi, vergi numarası, adres, posta kodu, e-posta, ev telefonu, iş telefonu, cep telefonu, son randevu cep ve ev telefonu, sigortalı durumu, emekli olup olmadığı, poliçe no, engel durumu, çalışan adı, tedavi olunan doktorlar ve branşlar gibi bilgiler)* ile hasta dosyası anamnez içeriğinin (kullandığı ilaçlar, alışkanlıklar, alerjik öyküsü, soygeçmiş, psikolojik durum, bulgular, laboratuvar tetkikleri, öntanı, tanı, tedavi ve bakım planı, geçirmiş olunan hastalıklar, ameliyatlar vb. bilgiler) etkilendiği

ifadelerine yer verilmiştir.

Veri ihlal bildiriminin Kurumumuzun yetki ve görev alanı çerçevesinde incelenmesi neticesinde; Kişisel Verileri Koruma Kurulunun 20/04/2021 tarih ve 2021/407 sayılı Kararı ile,

- İhlalden 789 hastanın etkilendiği ancak karakol tutanağına göre tespit edilen 54 adet hasta dosyasının geri alınarak yedieminliğe teslim edildiği, geri kalan dosyaların akıbetinin ise bilinmediği dikkate alındığından hasta dosyalarının kaybolması durumunun önlenemediği ve bu durumun söz konusu hasta dosyalarının kaybolmasına yönelik risklerin azaltılmasına dair yeterli tedbirlerin alınmadığını gösterdiği,

- İhlalden; kimlik, iletişim, lokasyon, özlük, genetik veri, sağlık verileri gibi veri kategorilerine ait çok sayıda kişisel verinin ve özel nitelikli kişisel verinin etkilenmiş olduğu hususunun ilgili kişilerin ihlal sebebiyle önemli olumsuz etkilere maruz kalmaları olasılığının bulunduğunun göstergesi olduğu,

- İhlal ile ilgili olan çalışanların, sağlık verileri ve genetik veriler de dahil olmak üzere özel nitelikli çok sayıda kişisel verinin işlenme sürecinde yer aldığı göz önünde bulundurulduğunda; 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 Kişisel Verileri Koruma Kurulunun 31/01/2018 Tarihli ve 2018/10 Sayılı "Özel Nitelikli Kişisel Verilerin İşlenmesinde Veri Sorumlularınca Alınması Gereken Yeterli Önlemler" ile ilgili Kararında yer alan *"Özel nitelikli kişisel verilerin işlenmesi süreçlerinde yer alan çalışanlara yönelik, a) Kanun ve buna bağlı yönetmelikler ile özel nitelikli kişisel veri güvenliği konularında düzenli olarak eğitimler verilmesi,…gerekir.*" ifadesine aykırı olarak veri sorumlusu tarafından çalışanlara kişisel verilerin korunmasına yönelik yeterli eğitimin verilmediğinin göstergesi olduğu,

- İhlal 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 kullanılamadığı hususlarının göstergesi olduğu,

- İhlali gerçekleştiren ve diğer çalışanların Başhekimliğin izni ve onayı bulunmaksızın, eski çalışanın ve aynı yerde yer alan bir şirket çalışanının arşiv odasına girebildiği ve hasta dosyalarını dışarı çıkarabildiği, ayrıca söz konusu durumun kamera kayıtlarında görülmesine rağmen 1 ayı aşkın süre boyunca ihlalin devam ettiği ve kamera kayıtlarının ancak ihlal anlaşıldıktan sonra kontrol edildiği hususunun Kişisel Verileri Koruma Kurulunun 31/01/2018 Tarihli ve 2018/10 Sayılı Özel Nitelikli Kişisel Verilerin İşlenmesinde Veri Sorumlularınca Alınması Gereken Yeterli Önlemler" ile ilgili Kararında yer alan *"… Bu ortamların fiziksel güvenliğinin sağlanarak yetkisiz giriş çıkışların engellenmesi…gerekir."* ifadesine aykırı olarak kamera kayıtlarının kontrolünün ve hastalara ait kayıtların tutulduğu arşiv odasına yetkili olmayan kişilerin girmemesini sağlayacak yeterli idari tedbirlerin alınmadığını gösterdiği,

- İhlalin gerçekleşmesinden önce, Kişisel Verileri Koruma ve Bilgi Güvenliği Kurulu oluşturulmasına, Veri İhlali Müdahale Planı hazırlanmasına ve KVKK kapsamında ilgili kişilerden veya kurumlardan gelecek talepleri karşılamak üzere algoritma oluşturulmasına rağmen; yedieminliğe teslim edilen hasta dosyalarının hastane arşivindekilerden daha fazla veri içerdiğinin ihlalden sonra tespit edildiği hususlarının Kişisel Veri Güvenliği Rehberi"nin "Kişisel Veri Güvenliği Politikalarının ve Prosedürlerinin Belirlenmesi" başlığı altında yer alan *"Kişisel veri güvenliğine ilişkin belirlenecek doğru ve tutarlı politika ve prosedürler, veri sorumlusunun çalışma ve işleyişine uygun şekilde entegre edilmelidir. Veri sorumlularınca politika ve prosedürler iyi bir şekilde ve zamanında hazırlanamadığında, sorunlu alanlar belirlenemediğinde veya mevcut güvenlik önlemleri kullanılamadığında kişisel veri güvenlik seviyesi yeteri kadar sağlanamamaktadır."* ifadelerinde yer aldığı üzere; veri sorumlusu tarafından alınan mevcut güvenlik önlemlerinin iyi bir şekilde hazırlanmaması veya kullanamaması nedeniyle ihlalin tespit edilmesi ve önlenmesine yönelik tedbirlerin zamanında ve yeterli ölçüde alınamadığı,

- İzinsiz olarak hastaneden çıkarılan birçok hasta dosyasının akıbetinin halen bilinmemesinin *"Kişisel Veri Güvenliği Rehberi"nin "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 olarak hasta dosyalarının kaybolması durumunun önlenemediği veya kaybolması halinde risklerin azaltılmasına dair yeterli tedbir alınmadığını gösterdiği

dikkate alındığında Kanunun 12. Maddesinin 1 numaralı fıkrası çerçevesinde veri güvenliğini sağlamaya yönelik gerekli tedbirleri almayan veri sorumlusu hakkında kabahatin haksızlık içeriği, veri sorumlusunun kusuru ve ekonomik durumu da göz önünde bulundurularak Kanunun 18 . maddesinin 1. Fıkrasının (b) bendi uyarınca **450.000 TL,**

- **İhlalin tespit edilmesinden 25 gün sonra Kuruma bildirildiği,**
- **İlgili kişilerden hastaneye gelen bir kişi dışında, hiç birine ihlalin bildirilmemiş olduğu**

hususları dikkate alındığında Kanunun 12. Maddesinin 5 numaralı fıkrası hükmü ve Kişisel Veri İhlali Bildirim Usul ve Esaslarına İlişkin Kişisel Verileri Koruma Kurulunun 24.01.2019 tarih ve 2019/10 sayılı Kararında yer alan 'en kısa sürede' ifadesinin 72 saat olarak yorumlanmasına yönelik ifadeleri çerçevesinde bildirim yükümlülüğünü yerine getirmeyen veri sorumlusu hakkında kabahatin haksızlık içeriği, veri sorumlusunun kusuru ve ekonomik durumu da göz önünde bulundurularak Kanunun 18. Maddesinin 1. Fıkrasının (b) bendi uyarınca **150.000 TL**

olmak üzere toplam 600.000 TL idari para cezası uygulanmasına,

İlgili kişilere Kurulun 24.01.2019 tarih ve 2019/10 sayılı Kararında yer alan hususları içeren bir bildirim yapılarak sonucundan Kurula bilgi verilmesi hususunda veri sorumlusunun talimatlandırılmasına

karar verilmiştir.

Yayım Tarihi : 05/07/2021
Karar Tarihi : 16/06/2020
Karar No : 2021/464
Konu Özeti : **Bir otoyol işletmesinin veri ihlal bildirimi hakkında karar**

Veri sorumlusunun Kurumumuza intikal eden veri ihlal bildiriminde;

- İhlalin; çalışanların kendi rıza ve talepleri ile yazılı ve imzalı olarak veri sorumlusuna ilettikleri kişisel e-posta adreslerinin sisteme işlenmesinden sonra bordro programı üzerinden bu hesaplara gönderilen bordrolarda, gönderilen kişilerin kendisine ait olmayan ancak aynı şirket çalışanı olan başka çalışanlara ait bordroyu ve dolayısıyla başkasına ait ad, soyad, TC Kimlik No ve sicil numarası görüntülemesi şeklinde gerçekleştiği, maaş bilgisinin ise herkeste aynı jenerik bilgisinin görüntülendiği,

- İhlalin sistemsel bir hata sebebiyle hatalı e-posta gönderimi neticesinde meydana geldiği ve bu teknik hatanın da bordro sisteminde Türkçe dili için bir cihaz türü tanımlı olmaması nedeni ile programın bordro zarflarını anlık göndermek yerine öncelikle kuyruğa gönderip oradaki kayıtları sonrasında e-posta atmak yöntemini kullanması nedeniyle yaşandığı,

- İhlalden etkilenen kişi ve kayıt sayısının 489 olduğu,

ifadelerine yer verilmiştir.

Veri ihlal bildiriminin Kurumumuzun yetki ve görev alanı çerçevesinde incelenmesi neticesinde; Kişisel Verileri Koruma Kurulunun 25.03.2021 tarih ve 2021/311 sayılı Kararı ile;

- Yapılan inceleme sürecinde, kurul kararına istinaden veri sorumlusuna gönderilen tebligatta, "… Çalışanların kendi rıza ve talepleri üzerine sundukları yazılı beyan dilekçesinde yer alan kişisel e-posta adreslerinin sisteme işlendiği ve bu kişisel e-postaların kullanıldığı, ancak neden kişisel e-posta yerine şirket e-postasına gönderim gerçekleştirilmediği…" ile ilgili bilgi istenmiştir. Bu talebe cevaben veri sorumlusu, *"Şirketimiz, çalışanlarının büyük bir çoğunluğu sahada bulunan bir organizasyon yapısına sahiptir. Bu itibarla tüm çalışanlarımıza şirketimiz tarafından tanımlanmış bir e-posta hesabı bulunmadığı, keza şirket e-posta hesaplarına şirketin erişim olanağı bulunduğu da dikkate alınarak bu bildirimlerin çalışanlarımızın kişisel e-posta hesaplarına yapılmasının daha uygun olacağı değerlendirilmiştir."* şeklinde bir geri dönüş yapılmıştır. Bu durum, çalışanlara yanlışlıkla giden bordroların silinip silinmediğinin kişisel e-posta hesaplarından (birçok e-posta sunucusu içerdiği için) kontrol imkânı bulunmadığından ihlalin, aslında veri sorumlusunun belirttiği gibi sadece teknik aksaklık değil; söz konusu çalışanlara kurumsal e-posta hesabı açmayarak ve bu hesaplar üstünden bordro gönderimi

yapmayarak ihlalin idari eksiklikten de kaynaklanmasına sebep olunduğu,

- Kişisel Veri Güvenliği Rehberi (Teknik ve İdari Tedbirler) 3.2 maddesi Kişisel Veri Güvenliğinin Takibi başlığında *"…Çalışanların sistem ve servislerdeki güvenlik zaafiyetlerini ya da bunları kullanan tehditleri bildirmesi için resmi bir raporlama prosedürü oluşturulması gerekmektedir."* ifadesine ve 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…"* ifadesine göre ihlale konu olan riskin veri sorumlusu tarafından değerlendirilmediği,

- Veri sorumlusu tarafından aydınlatma yükümlülüğüne uyularak ve ilgili kişilerin açık rızası alınarak e-postaların gönderildiği belirtilmekle birlikte aydınlatma metninin ilgili kişileri bu hususlara ilişkin olarak yeterince bilgilendiren bir metin olmadığı ve kişilere herhangi bir başka seçenek bırakmadığının görüldüğü,

- 31.05.2019 tarihli ve 2019/157 sayılı Kurul Kararında de belirtildiği üzere, kurumsal e-posta hizmetinin sunucularının yurt dışında olan veri sorumlularından/veri işleyenlerden temin edilmesi durumunda saklama hizmetlerinin de 6698 sayılı Kanunun 9. Maddesi hükümlerine uygun olarak gerçekleştirilmesi gerektiği, veri sorumlusu tarafından Kurumsal e-posta hizmeti alınmadan çalışanların şahsi e-posta hesaplarının çalıştıkları işlerle ilgili e-posta gönderiminde kullanılmasının verilerin farklı ülkelerde saklanması durumunu ortaya çıkarabileceği ve veriler üzerinde kontrol kaybına neden olabileceği

hususları dikkate alındığında, Kanun'un 12. Maddesinin 1. 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. Maddesinin 1. Fıkrasının (b) bendi uyarınca **60.000 TL idari para cezası uygulanmasına,**

karar verilmiştir.

Yayım Tarihi : 05/07/2021
Karar Tarihi : 16/06/2020
Karar No : 2020/466
Konu Özeti : Bir sigorta şirketinin acentesinde gerçekleşen veri ihlali hakkında

Veri sorumlusunun Kurumumuza intikal eden veri ihlal bildiriminde;

- İhlalin veri sorumlusu Sigorta şirketinin bir acentesinde işletmelerine ait bilgisayar ekranına bir hacker tarafından erişim sağlanmasıyla gerçekleştiği,
- İhlalin; veri işleyenin verdiği şikayetçi ifade tutanağı ile anlaşıldığı, ilgili tutanağa göre; Acente tarafından kullanılan bilgisayarlarda yazışma ekranının açıldığı, yetkisiz kişinin bu ekran aracılığıyla iletişim kurup fidye istediği, saldırının bu şekilde tespit edildiği,
- İhlalin 13.02.2020 tarihinde gerçekleştiği, 20.02.2020 tarihinde tespit edildiği ve 22.02.2020 tarihinde Kurumumuza bildirildiği,
- İhlalden etkilenen kişisel veri kategorilerinin kimlik ve finans verileri olduğu,
- İhlalden etkilenen kişi sayısının 172 olduğu,
- Acente yetkilisinin ihlalin gerçekleşmesinden sonra kişisel verilerin korunması ile ilgili eğitim aldığı,

ifadelerine yer verilmiştir.

Veri ihlal bildiriminin Kurumumuzun yetki ve görev alanı çerçevesinde incelenmesi neticesinde; Kişisel Verileri Koruma Kurulu'nun 16.06.2020 tarih ve 2020/466 sayılı Kararı ile;

- Veri ihlalinin 13.02.2020 tarihinde veri işleyenin sistemlerine yetkisiz erişim sağlanmasıyla gerçekleştiği, ihlalin veri sorumlusu tarafından 20.02.2020 tarihinde tespit edildiği,
- Veri sorumlusu sigorta şirketinin, veri işleyen acenteye donanımı kendilerinin temin etmediği, vakaya konu bilgisayarın veri işleyenin kendisine ait olduğu, bu nedenle bilgisayar üzerinde veri işleyenin kendi aktivite ve kullanıcı kayıtlarının veri sorumlusu tarafından yönetilmediği ve sızma testlerinin yapılmadığı hususlarını belirtildiği, ayrıca; Acente Bilgi Güvenliği İlkeleri dokümanında; Acentelerin bilgi güvenliği politikasına uyumlu olmasını temin etmek için, Bilgi Güvenliği veya Risk Yönetimi ve İç Kontrol birimleri tarafından denetlemelerin yapılabileceği ve gerektiği takdirde ve periyodik olarak kurum dışı bağımsız kaynaklara güvenlik ile uyum test ve denetlemelerin yaptırıldığı ifadelerine de yer verilmiş olmasına rağmen veri işleyenin

herhangi bir şekilde denetlenmemesinin, Kurumumuz tarafından yayınlanan Kişisel Veri Güvenliği Rehberinin (Teknik ve İdari Tedbirler-Rehber) 2.5 maddesinde "Veri işleyenler ile İlişkilerin Yönetimi" başlığı altında; *"…veri sorumlularının, hizmet alırken söz konusu veri işleyenlerin kişisel veriler konusunda en az kendileri tarafından sağlanan güvenlik seviyesinin sağlandığından emin olmaları gerekmektedir. Zira Kanunun 12. Maddesinin 2. Fıkrası gereği veri işleyenler de kişisel verilerin güvenliğinin sağlanması konusunda veri sorumlusuyla müştereken sorumludur."* ifadelerine aykırılık teşkil ettiği,

- Veri sorumlusu tarafından; ilgili bilgisayar hemen olayın akabinde formatlandığı için herhangi bir araştırmanın yapılamadığı, herhangi bir kişisel veriye erişilip erişilmediğinin tespit edilmediği, veri işleyenin ifadesine istinaden araç ruhsatı üzerinde bulunan kimlik bilgileri ile kredi kartı bilgileri kategorilerinin seçildiği belirtilmiş olup bu durumun Rehber'in 3.6. maddesinde; "Kişisel Verilerin Yedeklenmesi" başlığı altında; *"…Kişisel verilerin herhangi bir sebeple zarar görmesi, yok olması, çalınması veya kaybolması gibi hallerde veri sorumlularının yedeklenen verileri kullanarak en kısa sürede faaliyete geçmesi…"* ifadelerine aykırılık teşkil ettiği,

- Acente yetkilisinin kişisel verilerin korunması ile ilgili eğitimi veri ihlalinin gerçekleşmesinden sonra almış olduğu, Rehber'in 2.2. maddesinde; "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 veri sorumlusu tarafından eğitim ve farkındalık çalışmalarının yapılmasının veri sorumlusu tarafından sağlanmadığı,

- Veri işleyenin Windows 7 Professional x64 işletim sistemini kullandığı, Windows'un resmi sayfası üzerinden yapılan duyuruda; Windows 7 işletim sisteminin 14.01.2020 tarihinden itibaren artık yeni Microsoft Security Essentials yüklemelerini desteklememekte olduğundan tüm müşterilerin en iyi güvenlik seçeneği olan Windows 10 ve Windows Defender Virüsten Koruma'ya geçmelerini önerildiği, Rehber'in 2.3 maddesinde; Kişisel Veri Güvenliği Politikalarının ve Prosedürlerinin Belirlenmesi başlığı altında; *"…hemen hemen her yazılım ve donanımın bir takım kurulum ve yapılandırma işlemlerine tabi tutulması gerektiği, ancak yaygın şekilde kullanılan bazı yazılımların özellikle eski sürümlerinin belgelenmiş güvenlik açıkları bulunmakta…"* olduğunun belirtildiği, bahsi geçen işletim sisteminin hâlihazırda eski bir sürüm olduğu ve 14.01.2020 tarihinden itibaren güvenlik korumasıyla ilgili güncellemeleri desteklemediği hususlarının gerekli güvenlik önlemlerinin veri sorumlusu ve veri işleyen tarafından tam olarak alınmadığını gösterdiği,

- Veri işleyen tarafından veri ihlali öncesinde anti-virüs yazılımının hiç kullanılmamakta olmasının Rehber'in 3.2 maddesinde "Siber Güvenliğin Sağlanması başlığı altında"; "*…Kötü amaçlı yazılımlardan korunmak için ayrıca, bilgi sistem ağını düzenli olarak tarayan ve tehlikeleri tespit eden antivirüs, antispam gibi ürünlerin kullanılması gerekmektedir. Ancak bu ürünlerin sadece kurulumu yeterli olmayıp güncel tutularak gereken dosyaların düzenli olarak tarandığından emin olunmalıdır."*, 27 Nisan 2020 tarihinde veri sorumlusunun acentelerin siber saldırılardan korunmalarına yönelik yapmış olduğu duyuruda; Tüm kullanıcı bilgisayarlarına anti-virüs yazılımlar yüklenmesi ve kullanıcılar anti-virüs yazılımlarını kapatmaması veya ayarlarını değiştirmemesinin gerektiği, 01.11.2019 tarihli ve veri sorumlusunun acentelerine 21.01.2020 tarihinde duyurulan Acente Bilgi Güvenliği İlkeleri dokümanında yer alan; tüm kullanıcı bilgisayarlarına anti-virüs yazılımlarının yüklendiği, acente kullanıcılarının anti-virüs yazılımlarını kapatamadığı veya ayarlarını değiştiremediği, ifadelerine aykırı olarak veri sorumlusu ve veri işleyen tarafından bahse konu güvenlik önlemlerinin yerine getirilmediği hatta veri sorumlusunun kendi hazırlamış olduğu dokümanların gereklerinin dahi sağlanmadığı

hususları dikkate alındığında, Kanun'un 12. Maddesinin 1. 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. Maddesinin 1. Fıkrasının (b) bendi uyarınca **172.000 TL idari para cezası uygulanmasına,**

- Veri ihlalinden etkilenen 172 ilgili kişiden 95 kişiye veri ihlalinin bildirilmediği,

- İhlalin 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 alındığında, Kanunun 12. Maddesinin 5. Fıkrasında yer verilen "en kısa sürede" (ilgili kişilere bildirim için) bildirimde bulunma yükümlülüğünün 24.01.2019 tarih 2019/10 sayılı Kararda yer verilen "ilgili kişinin iletişim adresine ulaşılabiliyorsa doğrudan, ulaşılamıyorsa veri sorumlusunun kendi web sitesi üzerinden yayımlanması gibi uygun yöntemlerle bildirim yapılması" şeklinde de yapılabileceği hususunun veri sorumlusuna hatırlatılmasına

karar verilmiştir.

Yayım Tarihi : 05/07/2021
Karar Tarihi : 30/06/2020
Karar No : 2020/511
Konu Özeti : Bir sigorta şirketinin veri ihlal bildirimi hakkında

Veri sorumlusunun Kurumumuza intikal eden veri ihlal bildiriminde;

- 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 toplu bir liste hazırlanması gerektiği,

- Bu amaçla ilgili kişilerin kimlik ve ilaç kullanım bilgilerinin yer aldığı bir excel dosyasının oluşturulduğu,

- Söz konusu dosyada yer alan bilgilerin provizyon uygulamasına kişi bazlı olarak girilir iken ilgili dosyanın aynı zamanda provizyon sistemine entegre olarak çalışan doküman yönetim sistemine excel dokümanı olarak sehven bütün halinde yüklendiği,

- İhlalden etkilenen kişi sayısının 683; kayıt sayısının 2413 olduğu,

- Etkilenen kişi kategorilerinin müşteriler olduğu,

- İhlalden etkilenen kişisel verilerin kimlik, müşteri işlem ve sağlık bilgileri olduğu,

- İhlale konu excel dosyasına erişimin yalnızca mobil uygulamanın “sağlık geçmişim/Eczane” bölümünden 11 sağlık müşteri açısından mümkün olduğu, bunlardan yalnızca 2 kişinin uygulama kullanıcısı olduğunun tespit edildiği, söz konusu dosyaya erişimin mobil uygulama üzerinden 1 kişi tarafından yapıldığı, diğer kullanıcının ilgili dosyaya herhangi bir erişiminin olmadığı,

- Diğer taraftan ilgili dosyaya erişim sağlayan kullanıcı ile irtibata geçildiği, kendisine ihlal ve sonuçlarına yönelik bilgilendirme yapıldığı, erişim sağladığı dosyanın acil olarak silinmesi konusunda talepte bulunulduğu, bu kapsamda ihlalin ilgili kişiler üzerindeki potansiyel etkilerinin oldukça sınırlı olduğunun değerlendirildiği

ifadelerine yer verilmiştir.

Veri ihlal bildiriminin Kurumumuzun yetki ve görev alanı çerçevesinde incelenmesi neticesinde; Kişisel Verileri Koruma Kurulu'nun 30/06/2020 tarih ve 2020/511 sayılı Kararı ile,

- İhlalin, veri sorumlusunun eczane provizyon ekranlarının değiştirilmesi esnasında, kişi bazında kimlik ve ilaç kullanım bilgilerinin yer aldığı excel dosyasının, yeni sisteme aktarılırken 11 sigortalı tarafından görüntülenebilir hale gelmesi sonucu gerçekleştiği, bunun sonucunda ihlalden ilgili kişilerin; kimlik, müşteri işlem ve özel nitelikli kişisel veri olarak da sağlık bilgileri gibi kişisel verilerinin etkilendiği,

- 25.04.2019 tarihinden 07.12.2019 tarihine kadar açıklığın devam ettiği ve dosyaya erişim sağlayan kişi tarafından bilgilendirilinceye kadar veri sorumlusunun açıklığı tespit edemediği, Kişisel Veri Güvenliği Rehberi'nin Kişisel Veri Güvenliği Politikalarının ve Prosedürlerinin Belirlenmesi başlığı altında da belirtildiği üzere *"...veri sorumlusunun hazırlanmış olan kişisel veri güvenliği politika ve prosedürleri kapsamında; uygulamanın düzenli olarak kontrollerini yapmak, yapılan kontrolleri belgelemek, geliştirilmesi gereken hususlar belirlemek ve gerekli güncellemeler yerine getirildikten sonra da düzenli olarak kontrollere devam etmek gibi yükümlülüklerini"* yerine getirmediği,

- Ayrıca yine Kişisel Veri Güvenliği Rehberi'nin Kişisel Veri Güvenliğinin Takibi başlığı altında belirtilen *"veri sorumlularının gizlilik ve bütünlüğü bozan ihlaller gibi istenmeyen olayların önüne geçilmesi adına veri sorumlusu tarafından düzenli olarak zaafiyet taramalarının yapılmadığının"* göstergesi olduğu, Kişisel Veri İçeren Ortamların Güvenliğinin Sağlanması başlığı altında belirtilen *"çalışanların sistem ağına erişim sağlaması da güvenlik ihlali riskini arttırdığından bunlar için yeterli güvenlik tedbirinin"* alınmadığı,

- Veri sorumlusunun 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 almadığı, bu durumun Kişisel Veri Güvenliği Rehberi'nin Bilgi Teknolojileri Sistemleri Tedariği, Geliştirme ve Bakımı başlığı altında da ifade edildiği üzere *"veri sorumlusu tarafından yeni sistemin geliştirilmesi veya mevcut sistemlerin iyileştirilmesi ile ilgili ihtiyaçlar belirlenirken güvenlik gereksinimlerinin göz önünde bulundurulmadığı, uygulama sistemlerinin girdilerinin doğru ve uygun olduğuna dair kontrollerin yeterli ve gerekli ölçüde yapılmadığı, doğru girilmiş bilginin işlem sırasında oluşan hata sonucunda veya kasıtlı olarak bozulup bozulmadığını kontrol etmek için uygulamalara kontrol mekanizmaları yerleştirilmediği ve belgelerin sisteme yüklenirken bir onay sürecinin işletilmediği"*,

- İhlalden etkilenen kişisel verilerin içinde özel nitelikli kişisel veriler olarak sağlık bilgilerinin bulunduğu, ihlale konu olan dosyanın içerisinde özel nitelikli kişisel verilerin de yer aldığı göz önünde bulundurulduğunda *"Özel Nitelikli Kişisel Verilerin İşlenmesinde Veri Sorumlularınca Alınması Gereken Yeterli Önlemler" ile ilgili Kişisel Verileri Koruma Kurulunun 31/01/2018 Tarihli ve 2018/10 Sayılı Kararında da belirtildiği üzere "özel nitelikli kişisel verilerin işlendiği, muhafaza edildiği ve/veya erişildiği ortamlar, elektronik ortam ise verilerin kriptografik yöntemler kullanılarak muhafaza edilmesi ve kriptografik anahtarların güvenli ve farklı ortamlarda tutulması gerekirken veri sorumlusu tarafından diğer kişisel verilere göre çok daha sıkı şekilde korunmaları gerektiğinin"* göz önünde bulundurulmadığı,

- İhlale konu olayda ilgili kişiler önemli bir zarara uğramamış olsa da öğrenilmesi halinde ilgili kişiler hakkında mağduriyete neden olabilecek nitelikteki verilerin ihlale konu olduğu bu yüzden de ihlalin potansiyel tehdit açısından ciddi bir risk taşıdığı,

dikkate alındığında, Kanunun 12. Maddesinin 1. Fıkrası uyarınca veri güvenliğini sağlamaya yönelik gerekli teknik ve idari tedbirleri almayan veri sorumlusu hakkında Kanunun 18. Maddesinin 1. Fıkrasının (b) bendi uyarınca **100.000 TL idari para cezası uygulanmasına,**

- 07.12.2019 tarihinde tespit edilen veri ihlalinin, Kurumumuza 10.12.2019 tarihinde (72 saatlik süre koşulunun içerisinde) bildirildiği ve ihlalden etkilenen 683 kişiye yeterli bildirimin yapıldığı, bildirim örneklerinin Kurumumuza sunulduğu dikkate alındığında, Kanunun 12. Maddesinin 5. Fıkrası uyarınca **yapılacak bir işlem bulunmadığına**

karar verilmiştir.

Yayım Tarihi : 05/07/2021
Karar Tarihi : 29/09/2020
Karar No : 2020/744
Konu Özeti : **Bir bankanın veri ihlal bildirimi hakkında**

Veri sorumlusunun Kurumumuza intikal eden veri ihlal bildiriminde;

- Veri ihlalinin, Bankanın Veri Sızıntısı ekibi tarafından Teftiş Kurulu Başkanlığı'na iletilen bildirime istinaden soruşturma çalışmalarına başlanılarak tespit edildiği,

- Çalışanın veri sorumlusu nezdinde kullandığı e-posta adresine gelen ve ilgili adresten iletilen e-postalara ilişkin kayıtların incelenmesi neticesinde 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,

- Söz konusu müşterilerin hepsinin bir yatırım şirketine para transferlerinin bulunduğu,

- İhlalden etkilenen kişisel veri kategorilerinin kimlik, iletişim, müşteri işlem ve finans verileri olduğu,

- Verileri paylaşılan müşterilerin ihlale sebebiyet veren çalışanın ilişkili olduğu şubenin müşterileri olmadığı, bu nedenle çalışanın verileri toplaması ve paylaşmasının mesnedinin bulunmadığı

ifadelerine yer verilmiştir.

Veri ihlal bildiriminin Kurumumuzun yetki ve görev alanı çerçevesinde incelenmesi neticesinde; Kişisel Verileri Koruma Kurulu'nun 29/09/2020 tarih ve 2020/744 sayılı Kararı ile,

- İhlalden 346 Banka müşterisinin şube no, hesap no, ad-soyadı, cep telefonu numarası ve bu müşterilerin Bankadaki hesaplarından bir yatırım firması hesabına gönderdikleri yatırım işlemi tutar bilgilerinin etkilendiği,

- 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 ve etkin olmadığı hususunda şüphe oluşturduğu,

- Banka dışına giden e-postalara ilişkin Veri Sızıntısı Tespit/Önleme Sisteminin mevcut olduğunun belirtilmesine rağmen söz konusu ihlale neden olan e-postanın DLP sistemleri tarafından engellenmemesi ve ihlale sebep olan çalışanın kişisel verilerin aktarımı gerçekleştirilebildiği dikkate alındığında, Kişisel Veri Güvenliği Rehberi (Teknik ve İdari

Tedbirler)'nde "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."*, ifadeleri uyarınca yetkisiz olarak kişisel veri aktarımı önleme açısından veri sorumlusunun almış olduğu tedbirlerin yetersiz kaldığı,

- Banka tarafından alınan idari ve teknik tedbirlere rağmen Banka personelinin 346 müşteriye ait kişisel verileri, işlenme amacı dışında üçüncü taraflara iletebildiği ve bu durumun, Kişisel Verileri Koruma Kurulu'nun 31/05/2018 tarih ve 2018/63 sayılı ilke kararında *"…Bir veri sorumlusu nezdinde bulundukları pozisyon veya görev itibariyle kişisel verilere erişme yetkisi olanlar tarafından, yetkileri aşmak ve/veya yetkilerini kötüye kullanmak suretiyle, kişisel amaçlara veya nedenlere bağlı olarak işleme amacı dışında söz konusu kişisel verilerin işlenmesi ve/veya bu verilerin üçüncü kişilerle paylaşılması 6698 sayılı Kişisel Verilerin Korunması Kanununun (Kanun) 12. Maddesinin 1 numaralı fıkrasına aykırılık teşkil edeceğinden, bu kapsamdaki eylemlerin önlenmesi amacıyla veri sorumlularınca uygun güvenlik düzeyini temin etmeye yönelik gerekli her türlü teknik ve idari tedbirin alınması gerektiği…"* ifadelerine aykırı olarak veri güvenliğini sağlamaya yönelik veri sorumlusunun almış olduğu teknik ve idari tedbirlerin yetersiz kaldığının göstergesi olduğu

dikkate alındığında, Kanunun 12. Maddesinin 1. 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. Maddesinin 1. Fıkrasının (b) bendi kapsamında **225.000 TL,**

- İlgili kişilere gerekli bildirimlerin yapıldığı ve söz konusu bildirim örneklerinin tarafımıza gönderildiği,

- Ancak, ihlalin 31.10.2019 tarihinde gerçekleştiği ve Bankanın Teknoloji Veri Sızıntısı ekibi tarafından 04.11.2019 tarihinde Teftiş Kurulu Başkanlığı'na iletildiği, veri sorumlusunun Kurumumuza bildirimi 06.12.2019 tarihinde gerçekleştirdiği dikkate alındığında Kurul'un 24.01.2019 tarih ve 2019/10 sayılı Kararı ile belirlenen veri ihlalinin öğrenilmesinden itibaren başlayan **72 saatlik süre içerisinde bildirim koşulunun sağlanmadığı**

dikkate alındığında, Kanunun 12. Maddesinin 5. Fıkrasında yer verilen **“en kısa sürede”** (24.01.2019 tarih ve 2019/10 sayılı Kurul kararında belirtilen 72 saatlik süre içerisinde) bildirimde bulunma yükümlülüğüne aykırı hareket etmesi nedeniyle veri sorumlusu hakkında Kanunun 18. Maddesinin 1. Fıkrasının (b) bendi uyarınca **50.000 TL**

olmak üzere toplam 275.000 TL idari para cezası uygulanmasına

karar verilmiştir.

Yayım Tarihi : 05/07/2021
Karar Tarihi : 25/02/2021
Karar No : 2021/154
Konu Özeti : Bir sigorta şirketinin veri ihlal bildirimi hakkında

Veri sorumlusunun Kurumumuza intikal eden veri ihlal bildiriminde;

- İhlalin; veri sorumlusunun 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 gerçekleştiği,

- İhlalin; veri sorumlusu tarafından tespit edilemeyip, eski çalışanın ihlale konu kişisel verileri çalışmaya başladığı yeni işyeri e-posta adresine göndermesi üzerine yeni işveren tarafında tespit edildiği,

- İhlalden etkilenen kişisel verilerin kimlik, iletişim ve araç plaka numaraları olduğu,

- İhlalden etkilenen kişi sayısının 544 olduğu ve bu kişilerden 422'sine ulaşılarak ihlalin gerçekleşme tarihi, kapsamı ve muhtemel etkileri hakkında bizzat bilgi verildiği,

- Veri sorumlusunun acentelik faaliyetleri kapsamında, ilgili çalışanlar tarafından işleri gereği müşterilere poliçe gönderimleri yapılması nedeni ile yoğun bir şekilde şirket dışına e-posta gönderiminin yapıldığı, bu nedenle ihlal kapsamına alınabilecek olayların bu dönemde derhal fark edilemediği

ifadelerine yer verilmiştir.

Veri ihlal bildiriminin Kurumumuzun yetki ve görev alanı çerçevesinde incelenmesi neticesinde; Kişisel Verileri Koruma Kurulunun 25/02/2021 tarih ve 2021/154 sayılı Kararı ile,

- İhlalin eski çalışanın işinden ayrıldıktan sonra çalışmaya başladığı şirketin ilgili birimleri tarafından tespit edilip veri sorumlusuna bildirdiği,

- İhlalden 544 müşteriye ait; kimlik, iletişim ve araç plaka numaralarının etkilendiği,

- DLP sistemleri ile; belirli adedin üstünde T.C. Kimlik Numarası, kredi kartı numarası, IBAN, telefon numarası, e-posta adresi gibi kişisel verilerin bulunduğu belgelerin e-posta ile kurum dışına gönderilmesinin engellenmesinin mümkün olduğu, hatta veri sorumlusunun 2017 yılında bazı çalışanlara göndermiş olduğu e-postada; TCKN bilgileri, Kredi Kartı bilgileri ve

IBAN bilgilerinin kurum içindeki hareketini ve dışına çıkışının izleneceği ve engelleneceğinin ifade edilmiş olduğu hususlarına rağmen, veri sorumlusunun DLP sisteminin ihlale konu e-postaların gönderilmesini engelleyememiş olmasının "Kişisel Veri Güvenliği Rehberi"nin "Siber Güvenliğin Sağlanması" başlığı altında yer alan *"…her yazılım ve donanımın bir takım kurulum ve yapılandırma işlemlerine tabi tutulması gerekmektedir."* ifadesine aykırı olarak bu sistemin doğru yapılandırılmadığını gösterdiği,

- Eski çalışanın kendi kişisel e-posta adresine yapmış olduğu son e-posta gönderiminin, bu tarihten 1 ay sonra, işten ayrılmasından dolayı hesabının kapatılması nedeniyle DLP Raporuna yansımamasının "Kişisel Veri Güvenliği Rehberi"nin "Kişisel Veri Güvenliğinin Takibi" başlığı altında yer alan *"Tüm kullanıcıların işlem hareketleri kaydının düzenli olarak tutulması…"* gerekmektedir ifadesine aykırılık teşkil ettiği,

- İhlale konu e-posta gönderimlerinin; kasım ve aralık aylarında gerçekleştirilmesine rağmen, 24.12.2019 tarihine kadar tespit edilemediği ve bu tarihteki tespitin de yeni çalışmaya başladığı şirket tarafından yapılıp, veri sorumlusuna bildirilmiş olduğu hususu ile 2017 yılında bazı çalışanlara gönderilen e-postada; DLP raporlarının departman yöneticileri ile paylaşılacağı ve ilgili veri paylaşımlarından bilgileri olup olmadığı sorulacağı ifade edilmesine rağmen, 2018 yılına ait 2 DLP raporunda da dosyaların bulunduğu e-postalar hakkında personelin yöneticisine bildirim yapılmadığı hususlarının Veri Güvenliği Rehberi"nin "Kişisel Veri Güvenliğinin Takibi" başlığı altında yer alan *"…erişim kontrolü kayıtları ve diğer raporlama araçlarının düzenli olarak kontrol edilmesi… gerekmektedir."* ifadesine aykırı olarak gerekli kontrollerin sağlanmadığını gösterdiği,

- İhlal ile ilgili olan eski çalışana online kişisel veri koruma eğitimi açılmasına rağmen çalışanın 2 ay boyunca bu eğitime başlamadan işten ayrıldığı, bunun yanında eski çalışanın da içinde bulunduğu kullanıcılar grubuna bilgilendirmeler yapılmakla birlikte ilk bildirimde bilgilendirmede kişisel verilere ilişkin tanımlara yer verilip Kurumumuz internet sayfasında yer alan videoların bağlantısının paylaşıldığı, 2. bilgilendirmede ise sadece ilgili kişilerin hak ve yükümlülüklerinin yer aldığı dikkate alındığında "Kişisel Veri Güvenliği Rehberi"nin "Çalışanların Eğitilmesi ve Farkındalık Çalışmaları" başlığı altında düzenlenen *"… 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."* ifadesine aykırı olarak çalışana yönelik yapılan bilgilendirmelerin kişisel verilerin korunması hakkında bir takım genel hükümlerden ibaret olup, çalışanların kişisel verilerin hukuka aykırı olarak açıklanmaması ve paylaşılmaması gibi örneklendirilen temel konuları dahi içermediği hususlarının veri sorumlusunun kişisel verilerin korunması hakkında eğitim verilmesine yeterli önemi vermediğini gösterdiği

dikkate alındığında, Kanunun 12. Maddesinin 1. 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. Maddesinin 1. Fıkrasının (b) bendi uyarınca, **150.000 TL idari para cezası uygulanmasına**

- İhlalin; 24.12.2019 tarihinde tespit edildiği ve 27.12.2019 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 bildirim koşulunun sağlandığı dolayısıyla Kanun kapsamında yapılacak bir işlem olmadığına,**

- Öte yandan, veri sorumlusu tarafından bundan sonra ilgili kişilere yapılacak bildirimlerin Kişisel Verileri Koruma Kurulunun 18.09.2019 tarih ve 2019/271 sayılı Kararına uygun olarak yapılmasına dikkat edilmesi hususunun veri sorumlusuna hatırlatılmasına

karar verilmiştir.

Yayım Tarihi : 05/07/2021
Karar Tarihi : 04/03/2021
Karar No : 2021/187
Konu Özeti : Bir sigorta şirketinin veri ihlal bildirimi hakkında karar

Veri sorumlusunun Kurumumuza intikal eden veri ihlal bildiriminde;

- İhlalin nasıl gerçekleştiği hakkında;
    - Bir emeklilik hizmeti kapsamında veri sorumlusunun müşterisi olan bazı firmalara sigorta hizmetine dâhil olan çalışanlarına dair “Rapor” iletildiği,
    - Veri sorumlusunun bilgi sistemleri hizmeti aldığı destek hizmeti sağlayıcısında meydana gelen sistemsel hata nedeniyle;
        - Sistem hizmeti kapsamında veri sorumlusunun müşterisi olan bazı firmalar ile "Rapor" ilişkilendirmesinde teknik bir hata nedeniyle sorun yaşandığı,
        - Sistem hizmeti kapsamındaki 28 müşteri şirkete, diğer 31 müşteri şirketin sisteme dâhil çalışanlarına dair "Rapor" dosyası gönderildiği,
        - "Raporu" seçen sorgunun hatalı çalışması" neticesinde, sistem kapsamında olan 31 işveren şirketin çalışanı 681 adet gerçek kişi müşterisine alt bilgilerin, yine sistem kapsamındaki 28 işveren şirkete, sistemsel olarak hatalı şekilde gönderildiği,
- İhlalin raporu alan müşteri firmanın konu hakkında telefonda bilgi vermesi sonucu tespit edildiği,
- İlgili dosyaya erişim sağlayan ve ihlali veri sorumlusuna bildiren firmanın telefon kanalı ile yapılan çağrı esnasında 19.02.2020 saat 09.55’te ihlal hakkında bilgi verdiği,
- Bu firmaya da ihlalden etkilenen tüm firmalara olduğu gibi bilgilendirme yapıldığı ve sehven gönderilen bilgilerin silinmesi gerektiğinin tekrarlandığı,
- İhlale konu yazılımın canlıya alınmadan önce test edildiği,
- İhlalden etkilenen kişisel verilerin TCKN / Mavi Kart No, Ad – Soyad, Planlanan Ara Verme Bitiş Tarihi Sözleşme Durumu bilgilerinin olduğu

ifadelerine yer verilmiştir.

karar verilmiştir.

Veri ihlal bildiriminin Kurumumuzun yetki ve görev alanı çerçevesinde incelenmesi neticesinde; Kişisel Verileri Koruma Kurulunun 04.03.2021 tarih ve 2021/187 sayılı Kararı ile;

- Veri sorumlusunun bilgi sistem destek hizmeti aldığı veri işleyende meydana gelen sistemsel bir hata sonucu sorgunun hatalı çalışması nedeniyle emeklilik hizmeti kapsamında müşteri olan 31 işveren şirketin çalışanı olan 681 ilgili kişinin kişisel verilerini yine emeklilik kapsamında müşterilere gönderdiği (müşteri olan 28 işveren şirkete gönderilmiştir),

- Veri ihlaline sebep olan sistemsel hatanın 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 başlığı altında yer alan *"Veri sorumlusu tarafından yeni sistemlerin tedariki, geliştirilmesi veya mevcut sistemlerin iyileştirilmesi ile ilgili ihtiyaçlar belirlenirken güvenlik gereksinimleri göz önüne alınmalıdır. Uygulama sistemlerinin girdilerinin doğru ve uygun olduğuna dair kontroller yapılmalı, doğru girilmiş bilginin işlem sırasında oluşan hata sonucunda veya kasıtlı olarak bozulup bozulmadığını kontrol etmek için uygulamalara kontrol mekanizmaları yerleştirilmelidir."* ifadesi gereği, bu tip hataların işlem yayına alınmadan evvel düzeltilmesi gerektiği, ihlale konu olaydan önce tespitinin yapılamadığı,

- İhlale konu olayın gerçekleşme tarihi (18.01.2018) ile tespit tarihi (19.02.2020) arasında yaklaşık 2 yıllık 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,

- İhlalin raporu alan müşteri firmanın konu hakkında veri sorumlusuna bilgi vermesi sonucu tespit edildiği, veri sorumlusu tarafından kendiliğinden tespit edilemediği, bu durumun da Kişisel Veri Güvenliği Rehberi (Teknik ve İdari Tedbirler)'nde 3.2. Kişisel Veri Güvenliğinin Takibi başlığı altında belirtilen *"Bilişim ağlarında sızma veya olmaması gereken bir hareket olup olmadığının belirlenmesi gerekmektedir"* ifadesine uymadığının bir göstergesi olduğu

hususları dikkate alındığında, Kanunun 12. Maddesinin 1. 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. Maddesinin 1. Fıkrasının (b) bendi uyarınca **125.000 TL idari para cezası uygulanmasına,**

- İhlale sebep olan sistemdeki hatanın 18.01.2018 ve 19.02.2020 tarihleri arasında gerçekleştiği, 19.02.2020 tarihinde ilgili dosyaya erişim sağlayan Şirket tarafından veri sorumlusuna bilgi verilmesi sonucu ihlalden haberdar olunduğu, 21.02.2020 tarihinde Kurumumuza e-posta yoluyla veri ihlal bildiriminde bulunulduğu, ilgili yazının Kurum kayıtlarına 24.02.2020 tarihinde girdiği, bu açıdan veri sorumlusunun Kurulun 24.01.2019 tarih ve 2019/10 sayılı Kararı ile belirlenen veri ihlalinin öğrenilmesinden itibaren başlayan **72 saatlik süre içerisinde bildirim koşulunun sağlandığı,**

- İhlalden etkilenen ilgili kişilere 28.02.2020 tarihinde e-posta olarak bildirim yapılmaya başlandığı, e-posta bilgisi olmayan kişilere arama yapıldığı, görüşme yapılan tarih ve saatler ile bilgilendirme metin örneğinin tarafımıza gönderildiği

görülmekle birlikte, ilgili kişilere yapılacak bildirimin Kurulun 18.09.2019 tarih ve 2019/271 sayılı Kararı ile belirlenen asgari unsurlardan ihlalin ne zaman gerçekleştiği, kişisel veri kategorileri bazında (kişisel veri / özel nitelikli kişisel veri ayrımı yapılarak) hangi kişisel verilerin ihlalden etkilendiği, kişisel veri ihlalinin olası sonuçları, veri ihlalinin olumsuz etkilerinin azaltılması için alınan veya alınması önerilen tedbirler hususlarında eksiklikler olduğu dikkate alındığında bundan sonra ilgili kişilere yapılacak bildirimlerde Kişisel Verileri Koruma Kurulu'nun 18.09.2019 tarih ve 2019/271 sayılı Kararına uygun olarak bildirimde bulunulması hususunda veri sorumlusunun talimatlandırılmasına

karar verilmiştir.

Yayım Tarihi : 05/07/2021
Karar Tarihi : 04/03/2021
Karar No : 2021/190
Konu Özeti : Bankacılık sektöründeki veri sorumlusunun veri ihlal bildirimi hakkında karar

Veri sorumlusunun Kurumumuza intikal eden veri ihlal bildiriminde;

- Bir müşteri şikayeti üzerine Banka tarafından yapılan inceleme neticesinde, bir şube çalışanının kendisine tanımlanan Müşteri Bilgileri ve Belgeleri gözlem yetkisini, Banka erişim ve bilgi güvenliği politikalarına, verilen sınıf içi ve çevrimiçi eğitimlere, Banka ile olan iş sözleşmelerine ve ilgili menüye erişmeden önce çıkan uyarı mesajına aykırı şekilde, söz konusu müşterinin kimlik görüntüsünün amacı dışında gözlemlemesi; müşteriye ait gözlemlenen bilgilerin çalışanın şahsi cep telefonu ile fotoğrafının çekilmesi ve çalışan tarafından üçüncü kişiyle paylaşması suretiyle veri ihlali gerçekleştiği,

- Söz konusu olayda Banka sistemleriyle ilgili herhangi bir güvenlik açığının bulunmadığı, ihlalin çalışanın münferit davranışlarından kaynaklı olduğu sonucuna varıldığı,

- Veri ihlalinin, bir şube çalışanının kendisine tanımlanan Müşteri Bilgileri ve Belgeleri gözlem yetkisini amacı dışında kullanmasından ve 1 müşterinin kimlik bilgilerini yetkisiz kişiyle paylaşmasından kaynaklandığı,

- İhlal ile ilgili olan çalışanların Bilgi Güvenliği Farkındalığı Eğitimi ve Kişisel Verilerin İşlenmesi ve Korunmasında Temel Kavramlar Eğitimi aldığı

ifadelerine yer verilmiştir.

Veri ihlal bildiriminin Kurumumuzun yetki ve görev alanı çerçevesinde incelenmesi neticesinde; Kişisel Verileri Koruma Kurulunun 04.03.2021 tarih ve 2021/190 sayılı Kararı ile;

- Bulunduğu görev pozisyonundan yararlanarak olaya konu Takım Lideri'nin şikayette bulunan ilgili kişinin bilgilerine erişebildiği ve yetkisini kötüye kullanabildiği, bu durumun veri sorumlusu tarafından verilen veri gizliliği ve güvenliği eğitimlerine rağmen söz konusu çalışanın rol ve sorumlulukları hakkındaki farkındalığının sağlanamadığı göz önünde bulundurulduğunda Kurumumuzun yayınlamış olduğu Kişisel Veri Güvenliği Rehberi (Teknik ve İdari Tedbirler)'nin Çalışanların Eğitilmesi ve Farkındalık Çalışmaları başlığı altındaki *"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."* düzenlemelerine aykırılık teşkil ettiği,

- Bankada Takım Lideri olarak çalışan personelin veri ihlali öncesinde müşteri bilgilerini istenilen sıklıkta ve sayıda sorgulama yaparak görüntüleyebildikleri ve bu durumun çalışan personel tarafından müşterilerin kişisel verilerinin ihlaline sebebiyet verebilecek bir durum olduğu ve bu durumun Kurumumuzun yayınlamış olduğu Kişisel Veri Güvenliği Rehberi (Teknik ve İdari Tedbirler)'nin Çalışanların Eğitilmesi ve Farkındalık Çalışmaları başlığı altındaki *"… 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"* hususuna aykırılık teşkil ettiği,

- Risk Merkezi verilerinin sorgulanmasına yönelik sorgulama yapılabilecek kayıt sayısı/kota belirleme işlemlerinin veri ihlalinden önce yapılmadığı, söz konusu ihlalden ancak yaklaşık 2 yıl sonra çalışanlar için sorgulama kota limiti oluşturulduğu ve diğer müşteri sorgulamalarına kota oluşturulmasına yönelik çalışmalara halen devam edildiği,

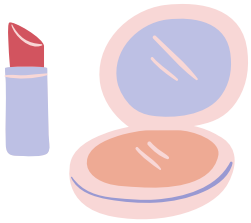
- Veri sorumlusu bünyesinde Çağrı Merkezi Takım Lideri olarak görev yapan çalışanların, müşterilerin rızası dışında, müşteri bilgilerine sınırsız sayıda sorgulama yaparak erişebildiği, söz konusu çalışanlar için gerekli ölçüde yetki verilmediği dikkate alındığında Kurumumuzun yayınlamış olduğu Kişisel Veri Güvenliği Rehberi (Teknik ve İdari Tedbirler)'nin Siber Güvenliğin Sağlanması başlığı altındaki *"… kişisel veri içeren sistemlere erişimin de sınırlı olması gerekmektedir. Bu kapsamda çalışanlara, yapmakta oldukları iş ve görevler ile yetki ve sorumlulukları için gerekli olduğu ölçüde erişim yetkisi tanınmalı ve … ilgili sistemlere erişim sağlanmalıdır."* tedbirlerine aykırılık teşkil ettiği,

- Veri ihlali sonrasında, başka şube müşterisinin bilgilerini sorgulamak isteyen çalışanlara erişecekleri verileri iş ihtiyacı kapsamında ve görev tanımıyla uyumlu bir şekilde kullanabileceklerine dair uyarı sisteminin geliştirildiği, veri ihlali öncesinde herhangi bir uyarı sistemi kullanılmadığı

hususları dikkate alındığında, Kanunun 12. Maddesinin 1. Fıkrası çerçevesinde veri güvenliğini sağlamaya yönelik gerekli teknik ve idari tedbirleri almayan veri sorumlusu hakkında Kanunun 18. Maddesinin 1. Fıkrasının (b) bendi uyarınca **100.000 TL idari para cezası uygulanmasına**

karar verilmiştir.

Yayım Tarihi : 05/07/2021
Karar Tarihi : 25/03/2021
Karar No : 2021/311
Konu Özeti : **Bir kozmetik şirketinin veri ihlal bildirimi hakkında karar**



Veri sorumlusunun Kurumumuza intikal eden veri ihlal bildiriminde;

- 18.05.2020 tarihinde, veri sorumlusunun internet sitesinde yer alan yeni bir kampanya sebebiyle siteye yüksek erişim sağlandığı ve uygulama sunucularının yetersiz kaldığı,
- Veri işleyen tarafından yeni uygulama sunucuları eklenirken, sitenin çalışmaması ihtimali gözetilerek sitenin mevcut halinin kopyalarının çıkarıldığı,
- Bu işlem gerçekleştirilirken; sitenin statik sayfasının kopyasının alınmasının ve yeni uygulama sunucuları eklenirken müşterilere sayfanın statik kopyasının gösterilmesinin amaçlandığı,
- Bu işlem esnasında; DDos ataklarını önlemek için kullanılan ve veri işleyenin üçüncü kişiden aldığı hizmetin içinde tanımlandığı gibi çalışmayan bir fonksiyon sebebiyle yalnızca mevcut ara yüzün değil kullanıcı profillerinin de bir kopyasının oluştuğu ve üye olarak giriş yapan kullanıcılara rastgele kopyası alınan kullanıcı profillerinin bilgilerinin görünür olduğu,
- Görüntülenen profillerde adı-soyadı, e-posta, adres gibi kişisel veriler yer aldığı, kredi kartı gibi finansal hiçbir kişisel veri bulunmadığı,
- Sitenin olağan dışı davranışlarının tüketiciler ve merkez ofis ekip tarafından veri sorumlusunun çağrı merkezine gelen bildirimlerle kısa sürede fark edildiği ve düzeltmek için yapılan çalışmalar neticesinde, saat 17.00'de sitedeki sorunların giderildiği, 17.00'de erişime kapatılan sitenin, 17.48'de tekrar normal çalışma düzenine çekildiği,
- Bu 48 dakikalık süre zarfı boyunca, sitede üye girişi yapmış müşterilerin, kendi kişisel verileri yerine kopyalama yapıldığı ana denk gelen tüketicilerin kopyası alınan profillerindeki kişisel verilerini görmüş olma ihtimali bulunduğu,
- Ancak bu süreçte alınan kopyaların herhangi bir sistemde saklanmadığı için kaç kişinin hangi üyelerin profilini görmüş olabileceği hakkında net bir sayının belirtilemediği, toplamda 24 kişinin bilgisinin farklı üyeler tarafından görünür olduğunun öngörüldüğü

ifadelerine yer verilmiştir.

Veri ihlal bildiriminin Kurumumuzun yetki ve görev alanı çerçevesinde incelenmesi neticesinde; Kişisel Verileri Koruma Kurulunun 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,

- Fonksiyonun canlı ortama alınmadan önce teste tabi tutulmuş olmasına rağmen bu testin sınırlı sayıda kullanıcı ile yapıldığı, veri sorumlusu tarafından kampanya sebebiyle yoğunluğun yüksek olacağının öngörülerek, bu yoğunluğa uygun bir şekilde yazılımın kontrollerinin gerçekleştirilmesinin ardından uygulamaya konulması gerektiği ayrıca 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 ancak veri sorumlusunun ihlale sebebiyet veren olayda buna uymadığı, açıklanan bu durumların Kişisel Veri Güvenliği Rehberi (Teknik ve İdari Tedbirler)'nde 3.5. Bilgi Teknolojileri Sistemleri Tedariği, Geliştirme ve Bakımı başlığı altında belirtilen *"Veri sorumlusu tarafından yeni sistemlerin tedariği, 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. Uygulamalar, işlem sırasında oluşacak hataların veri bütünlüğünü bozma olasılığını asgari düzeye indirecek şekilde tasarlanmalıdır."* ifadelerine uygun düşmediği,

- Bunların yanında veri sorumlusunun kullanıcıların kişisel verilerini maskeleyerek veya şifreleyerek saklaması gerekirken Kişisel Veri Güvenliği Rehberi (Teknik ve İdari Tedbirler) 4.1. Teknik Tedbirler Özet Tablosu'nda da yer verilen "şifreleme ve veri maskeleme" önlemlerini ancak ihlalden sonra almayı planladığı

- Yukarıda sayılan gerekçelerin veri sorumlusunun Kişisel Veri Güvenliği Rehberi (Teknik ve İdari Tedbirler)'nde 2.1. Mevcut Risk ve Tehditlerin Belirlenmesi başlığı altında belirtilen *"…bu verilerin korunmasına ilişkin ortaya çıkabilecek risklerin gerçekleşme olasılığının ve gerçekleşmesi durumunda yol açacağı kayıpların doğru bir şekilde belirlenerek buna uygun tedbirlerin alınması gerekmektedir."* şeklinde belirtilen risk odaklı yaklaşım çerçevesinde ve veri sorumlusu yükümlülüklerine uygun hareket etmediğinin göstergesi olduğu,

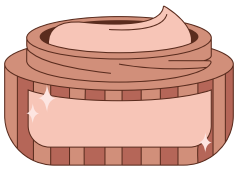
dikkate alındığında, Kanunun 12. Maddesinin 1. Fıkrası çerçevesinde veri güvenliğini sağlamaya yönelik gerekli teknik ve idari tedbirleri almayan veri sorumlusu hakkında Kanunun 18. Maddesinin 1. Fıkrasının (b) bendi uyarınca **200.000 TL idari para cezası uygulanmasına,**

- Kişisel Verileri Koruma Kurulunun 24.01.2019 tarih ve 2019/10 sayılı Kararı ile belirlenen veri ihlalinin öğrenilmesinden itibaren başlayan 72 saatlik süre içerisinde veri sorumlusunun Kuruma bildirimde bulunduğu,

- Veri sorumlusu tarafından veri ihlaline ilişkin bildirim yapılması amacıyla ilgili kişilere e-posta gönderildiği, gönderilen e-postanın Kişisel Verileri Koruma Kurulunun 18.09.2019 tarih ve 2019/271 sayılı Kararında belirtilen bildirimde bulunması gereken asgari unsurları taşıdığı

dikkate alındığında, Kanunun 12. Maddesinin 5. Fıkrası uyarınca, bu aşamada yapılacak bir işlem olmadığına

karar verilmiştir.



Karar Tarihi : 06/07/2021
Karar No : 2021/675
Konu Özeti : Cosmolog Kozmetik Sanayi ve Ticaret AŞ Veri İhlal Bildirimi

Veri sorumlusu sıfatını haiz olan Cosmolog Kozmetik Sanayi ve Ticaret AŞ tarafından Kurumumuza gönderilen veri ihlali bildiriminde özetle;

- Veri sorumlusu kayıtlarında veri ihlali olduğuna ilişkin iddiaların 2 adet internet sitesinde 17-18 Haziran 2021 tarihinde duyurulduğu, 25 Haziran 2021 tarihinde veri sorumlusuna haber verilmesiyle konu hakkında incelemelerin başlatıldığı,

- Yapılan incelemelerde veri sorumlusunun sistemde oluşturduğu raporların, rapor isimlerinin/URL isimlerinin herhangi bir kişi tarafından bilinmesi durumunda söz konusu raporlara erişim yetkisi verilmeyen 3. kişilerce erişilebileceğinin tespit edildiği,

- İhlalin 02.07.2021 tarihinde sona erdiği,

- İhlalinden etkilenen kişi sayısının 36.116 kişi olduğu,

- İhlalden etkilenen ilgili kişi gruplarının müşteriler olduğu,

- İhlalden etkilenen kişisel verilerin kimlik (ad-soyad), iletişim (e-posta ve adres) bilgileri olduğu,

- İlgili kişilerin veri ihlali ile ilgili guvenlik@cosmolog.com.tr e-posta adresinden bilgi alabileceği

ifade edilmiştir.

Veri ihlal bildiriminin Kurumumuzun yetki ve görev alanı çerçevesinde incelenmesi neticesinde; Kişisel Verileri Koruma Kurulunun 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,

- Fonksiyonun canlı ortama alınmadan önce teste tabi tutulmuş olmasına rağmen bu testin sınırlı sayıda kullanıcı ile yapıldığı, veri sorumlusu tarafından kampanya sebebiyle yoğunluğun yüksek olacağının öngörülerek, bu yoğunluğa uygun bir şekilde yazılımın kontrollerinin gerçekleştirilmesinin ardından uygulamaya konulması gerektiği ayrıca 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 ancak veri sorumlusunun ihlale sebebiyet veren olayda buna uymadığı, açıklanan bu durumların Kişisel Veri Güvenliği Rehberi (Teknik ve İdari Tedbirler)'nde 3.5. Bilgi Teknolojileri Sistemleri Tedariği, Geliştirme ve Bakımı başlığı altında belirtilen "Veri sorumlusu tarafından yeni sistemlerin tedariği, 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. Uygulamalar, işlem sırasında oluşacak hataların veri bütünlüğünü bozma olasılığını asgari düzeye indirecek şekilde tasarlanmalıdır." ifadelerine uygun düşmediği,

- Bunların yanında veri sorumlusunun kullanıcıların kişisel verilerini maskeleyerek veya şifreleyerek saklaması gerekirken Kişisel Veri Güvenliği Rehberi (Teknik ve İdari Tedbirler) 4.1. Teknik Tedbirler Özet Tablosu'nda da yer verilen "şifreleme ve veri maskeleme" önlemlerini ancak ihlalden sonra almayı planladığı

- Yukarıda sayılan gerekçelerin veri sorumlusunun Kişisel Veri Güvenliği Rehberi (Teknik ve İdari Tedbirler)'nde 2.1. Mevcut Risk ve Tehditlerin Belirlenmesi başlığı altında belirtilen "…bu verilerin korunmasına ilişkin ortaya çıkabilecek risklerin gerçekleşme olasılığının ve gerçekleşmesi durumunda yol açacağı kayıpların doğru bir şekilde belirlenerek buna uygun tedbirlerin alınması gerekmektedir." şeklinde belirtilen risk odaklı yaklaşım çerçevesinde ve veri sorumlusu yükümlülüklerine uygun hareket etmediğinin göstergesi olduğu,

dikkate alındığında, Kanunun 12. Maddesinin 1. Fıkrası çerçevesinde veri güvenliğini sağlamaya yönelik gerekli teknik ve idari tedbirleri almayan veri sorumlusu hakkında Kanunun 18. Maddesinin 1. Fıkrasının (b) bendi uyarınca 200.000 TL idari para cezası uygulanmasına,

- Kişisel Verileri Koruma Kurulunun 24.01.2019 tarih ve 2019/10 sayılı Kararı ile belirlenen veri ihlalinin öğrenilmesinden itibaren başlayan 72 saatlik süre içerisinde veri sorumlusunun Kuruma bildirimde bulunduğu,

- Veri sorumlusu tarafından veri ihlaline ilişkin bildirim yapılması amacıyla ilgili kişilere e-posta gönderildiği, gönderilen e-postanın Kişisel Verileri Koruma Kurulunun 18.09.2019 tarih ve 2019/271 sayılı Kararında belirtilen bildirimde bulunması gereken asgari unsurları taşıdığı dikkate alındığında, Kanunun 12. Maddesinin 5. Fıkrası uyarınca, bu aşamada yapılacak bir işlem olmadığına

karar verilmiştir.

Karar Tarihi : 06.07.2021
Karar No : 2021/677
Konu Özeti : T. Garanti Bankası AŞ Veri İhlal Bildirimi

Veri sorumlusu sıfatını haiz olan T. Garanti Bankası AŞ tarafından Kuruma gönderilen 2 adet veri ihlali bildiriminde özetle;

- Banka sistemi üzerinden Kredi Kayıt Bürosu (KKB) ekranlarına yönelik yapılan görüntülemelere ilişkin Teftiş Kurulu Başkanlığı tarafından 01.04.2020 - 15.03.2021 dönemi için uzaktan gerçekleştirilen incelemelerde, 2 farklı banka şubesinde görev alan 2 çalışanın gerçekleştirdiği görüntülemelerin dikkat çekici bulunması üzerine incelemelerin genişletildiği,

- Veri sorumlusu tarafından yapılan değerlendirme sonucu çalışanların sorgulamalara istinaden elde etmiş oldukları muhtelif müşterilere ait bilgileri 3. şahıslar ile paylaşmış olabilecekleri konusunda güçlü kanaate varıldığı,

- Bir şube çalışanının, %85'i şube müşterisi olmayan ve % 90'ı farklı müşteri segmentlerinden 3277 farklı kişiye ait KKB (Kredi Kayıt Bürosu) kaydını görüntülediği, Akyazı şubesinde bir çalışanın ise %90'ının şube müşterisi olmayan ve %70'i farklı bir şehirde ikamet eden müşterilerden 5079 farklı kişiye ait KKB (Kredi Kayıt Bürosu) kaydı görüntülemesi yaptığı,

- İhlalden etkilenen kişisel veri kategorisinin finans bilgileri olduğu,

- İlgili kişilerin veri ihlali ile ilgili www.garantibbva.com.tr, banka şubeleri ile bankanın çağrı merkezinden bilgi alabileceği

ifade edilmiştir.

Konuya ilişkin inceleme devam etmektedir.

Karar Tarihi : 13.07.2021
Karar No : 2021/725
Konu Özeti : Webhosting Bilişim Teknolojileri AŞ Veri İhlal Bildirimi

Veri sorumlusu sıfatını haiz olan Webhosting Bilişim Teknolojileri AŞ tarafından Kuruma gönderilen kişisel veri ihlali bildiriminde özetle;

- 09.07.2021 tarihinde yurtdışı kaynaklı bir sitede 2020 yılı aralık ayına ait verilerin olduğu düşünülen kayıtların paylaşıldığı ve konuya ilişkin veri sorumlusu tarafından araştırma yapıldığı,

- Yapılan kontroller neticesinde 27.12.2020 tarihinde bir sızıntı olduğunun, log kayıtlarında ilgili tarihte müşteri verilerinin toplu olarak yurtdışında bir IP adresine gönderildiğinin ve veri sızıntısının bir kez gerçekleştiğinin tespit edildiği,

- Bir yazılım açığı sebebiyle sızıntının oluştuğunun tahmin edildiği ancak detaylı incelemenin devam ettiği,

- İhlalden etkilenen kişisel veri kategorilerinin kimlik, iletişim, müşteri işlem, finans ve diğer *(Müşterilerin hizmetlere ait detaylar, hizmetlere ilişkin bazı şifreleri içeren e-posta içerikleri, .tr uzantılı alan adı kayıtlarına ilişkin kimlik, şirket belgeleri, imza sirküleri, vergi levhası gibi belgeler. 15 Kasım 2020 ile 27 Aralık 2020 tarihleri arasında log kayıtlarının sehven açık bırakılması nedeniyle oluşan 3027 adet kredi kartı bilgisi)* olduğu,

- Kredi kartı verisinin önemi nedeniyle ilk aşamada kart numaralarının tespit edildiği ve ödeme kuruluşuna bildirildiği,

- İhlalden etkilenen kişi sayısının henüz tespit edilemediği,

- İhlalden etkilenen kişi gruplarının çalışanlar, kullanıcılar ve müşteriler/potansiyel müşteriler olduğu

ifade edilmiştir.

Konuya ilişkin inceleme devam etmektedir.

Karar Tarihi : 13.07.2021
Karar No : 2021/728
Konu Özeti : Düzen Biyolojik Bilimler Araştırma Geliştirme ve Üretim A.Ş. Veri İhlal Bildirimi

Veri sorumlusu sıfatını haiz olan Düzen Biyolojik Bilimler Araştırma Geliştirme ve Üretim A.Ş. tarafından Kuruma gönderilen veri ihlal bildiriminde özetle;

- Veri işleyen konumundaki Fransa'daki Cerba Laboratuvarında yer alan kişisel verilerin yetkisi olmayan kişiler tarafından ulaşılabilir hale geldiğinin veri sorumlusuna bildirildiği,
- İhlalin 09.06.2021 tarihinde başladığı ve 24.06.2021 tarihinde sona erdiği,
- Bu tarihler arasında veri sorumlusunun Cerba Laboratuvarına 991 adet numune ilettiği, ancak belirtilen tarihler arasındaki kayıtların ne kadarına ulaşıldığı veya ulaşılıp ulaşılmadığının bilinmediği,
- İhlalden etkilenen kişisel verilerin ad, soyad, doğum tarihi, cinsiyet, istenen tetkik bilgileriyle birlikte tetkik sonucu olduğu,
- İhlalden etkilenen kişi gruplarının hastalar olduğu,
- İlgili kişilerin veri sorumlusunun çağrı merkezinden bilgi alabileceği

ifade edilmiştir.

Konuya ilişkin inceleme devam etmektedir.

Karar Tarihi : 19.07.2021
Karar No : 2021/729
Konu Özeti : Özel Dentapoint Diş Sağlığı Polikliniği Veri İhlal Bildirimi

Veri sorumlusu sıfatını haiz olan Özel Dentapoint Diş Sağlığı Polikliniği (İzmir) tarafından Kurumumuza gönderilen veri ihlali bildiriminde özetle;

- 12.07.2021 tarihinde yapılan siber saldırı sonucu hasta bilgilerini barındıran bilgisayarların şifrelenerek erişimin engellendiği,
- İhlalden etkilenen ilgili kişi gruplarının hastalar, müşteriler ve potansiyel müşteriler olduğu,
- İhlalden etkilenen kişisel verilerin kimlik, iletişim, lokasyon, müşteri işlem, işlem güvenliği, finans, görsel ve işitsel kayıtlar olduğu, ihlalden etkilenen özel nitelikli kişisel verilerin ise ırk ve etnik köken bilgisi ile sağlık bilgileri olduğu,
- İhlalden etkilenen kişi sayısının tahmini 14.000 olduğu

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