Kişisel Verileri Koruma Kurulu Veri İhlali Kararları

2026 yılı Ağustos ayında Kişisel Verileri Koruma Kurulu internet sitesinde bir dizi yeni karar yayımlandı. Bu kapsamda önemli gördüğümüz veri ihlallerine ilişkin kararları ve gerekçelerini sizler için derledik. İlgili kararlara bu bağlantı üzerinden ulaşabilirsiniz: Kişisel Verileri Koruma Kurulu'nun Yeni Yayınlanan Karar Özetleri.

Kanun: 'Kişisel Verileri Koruma Kanunu'
KVKK: 'Kişisel Verileri Koruma Kurulu'

ÖNE ÇIKAN KARARLAR

KARAR NO **2025/601**

Otelcilik Ve Konaklama Yönetimi Alanında Faaliyet Gösteren Veri Sorumlusunun Veri İhlal Bildirimine İstinaden Yürütülen İnceleme

KARAR ÖZETİ

Hong Kong merkezli otel işletmecisinin sistemlerine siber saldırı düzenlenmiş, tehdit unsuru rezervasyon veri tabanlarına erişip fidye talep etmiştir. 909 müşteri etkilenmiş, açığa çıkan veriler kişiye göre değişmekle birlikte ad, doğum tarihi, pasaport/kimlik no, iletişim ve bazı durumlarda ödeme kartı bilgilerini kapsamaktadır.

Şirketin Türkiye'de tüzel kişiliği, çalışanı veya altyapısı bulunmadığından ve ilgili kişiler hizmetlerden Türkiye'de faydalanmadığından KVKK, "**etki ilkesi**" gereği şirketin Kanun kapsamında veri sorumlusu sayılmadığına ve bildirim yükümlülüğü bulunmadığına karar vermiştir.

YAPTIRIM

Bu aşamada **işlem yapılmamasına** karar verilmiştir.

KARARIN GEREKÇESİ

KVKK, aşağıdaki gerekçelerle Kanun'un somut olaya uygulanmayacağı sonucuna varmıştır:

- Kanun'da yer bakımından uygulama alanına ilişkin açık bir hüküm bulunmadığından, Kurulun 24.01.2019 tarih ve 2019/10 sayılı kararında benimsediği "etki ilkesi" esas alınmıştır.
- Bu ilkeye göre, yurt dışı yerleşik bir veri sorumlusunun bildirim yükümlülüğü, ilgili kişilerin sunulan ürün/hizmetlerden Türkiye'de faydalanmasına bağlıdır.
- Somut olayda veri sorumlusunun Türkiye'de tüzel kişiliği, çalışanı, grup şirketi veya teknoloji altyapısı bulunmadığı tespit edilmiştir.
- Tüm kişisel verilerin Hong Kong'da toplanıp işlendiği belirlenmiştir.
- İlgili kişilerin, söz konusu hizmetlerden Türkiye'de faydalanmadığı tespit edilmiştir.

Bu tespitler doğrultusunda, Kanun'un somut olaya uygulanmayacağına karar verilmiştir.

KARAR NO **2024/2196**

Plastik Ev Gereçleri Ve Temizlik Ürünleri Üretimi Yapan Veri Sorumlusu Tarafından Kurula İntikal Ettirilen Veri İhlal Bildirimine İstinaden Yürütülen İnceleme

KARAR ÖZETİ

Veri sorumlusu sistemlerine fidye yazılımı saldırısı düzenlenmiş, veriler şifrelenerek fidye talep edilmiştir.

Veri sorumlusu kuruma yaptığı beyanlarda ihlalden hiç kimsenin etkilenmediğini, müşteri verilerinin kişisel veri değil ticari veri (fatura) olduğunu iddia etmiş ancak adli makamlara sunduğu dava dilekçesinde verilerin siber saldırganlarca elde edildiğini ve çalışan verilerinin ihlalden etkilendiğini açıkça kabul ettiği tespit edilmiştir.

Veri sorumlusu, talep edilen destekleyici belgeleri (doküman örnekleri, Kişisel Veri İşleme Envanteri) Kişisel Verileri Koruma Kurumu'na sunamamış, sunduğu sınırlı belgelerde ise çalışanlara ait özel nitelikli veriler dahil çok sayıda kişisel veri kategorisi tespit edilmiştir.

KARARIN GEREKÇESİ

KVKK, idari para cezasının uygulanmasını aşağıdaki gerekçelere dayanmıştır:

- Özel nitelikli veriler için güvenli şifreleme tedbirinin ancak ihlal sonrasında alınmaya başlanmış olması.
- İki faktörlü oturum doğrulamasının ihlal öncesinde değil, ihlalden sonra hayata geçirilmiş olması.
- İhlal öncesi yaptırılan güvenlik açığı testinin yetersiz kalması.
- İhlale sebep olan güvenlik açığına ilişkin bilgi/belge sunulamaması.

Aynı saldırıdan 9 şirketin etkilenmiş olmasının, ağ segmentasyonu eksikliğine işaret etmesi.

YAPTIRIM

250.000 TL idari para cezası uygulanmasına karar verilmiştir.

KARAR NO **2022/1375**

Bir Sanayi Şirketi Olan Veri Sorumlusu Tarafından Kurula İntikal Ettirilen Veri İhlal Bildirimine İstinaden Yürütülen İnceleme

KARAR ÖZETİ

Veri sorumlusunun bir çalışanının internetten indirdiği bir program aracılığıyla fidye yazılımı 797 sunucuya bulaşmış, dosyalar şifrelenmiştir.

İhlalden 4.885 çalışan, müşteri ve tedarikçi etkilenmiş olup kimlik, adres, IBAN, telefon, fotoğraf, pasaport ve kan grubu bilgileri açığa çıkmıştır.

İhlal öncesi yapılan sızma testinde tespit edilen acil/kritik güvenlik açıklarının (basit parola, güncel olmayan işletim sistemi, sınırsız parola deneme hakkı, yanlış yapılandırılmış SNMP [Simple Network Management Protocol: ağ üzerindeki cihazların uzaktan izlenmesi ve yönetilmesini sağlayan protokol], ağ segmentasyonu eksikliği) giderildiğine dair belge sunulamamıştır.

KARARIN GEREKÇESİ

KVKK, idari para cezasının uygulanmasını aşağıdaki gerekçelere dayanmıştır:

- İhlal öncesinde yapılan sızma testinde tespit edilen ciddi güvenlik açıklarının (zayıf parola politikası, güncellenmemiş işletim sistemi, sınırsız giriş denemesi, yetersiz ağ segmentasyonu) kapatıldığına dair kanıt sunulamaması.
- Çalışana yeterli farkındalık eğitimi verilmemiş olması, ihlale yol açan uygulamanın indirilmesiyle ilişkilendirilmiştir.
- Bildirimin 23 gün gecikmeli yapılmış olması, ayrı bir yükümlülük ihlali sayılmıştır.

YAPTIRIM

1.000.000 TL idari para cezası uygulanmasına karar vermiştir.

KARAR NO **2022/711**

Otomotiv Güvenlik Ve Elektronik Sistemleri Üretimi Yapan Veri Sorumlusu Tarafından Kurula İntikal Ettirilen Veri İhlal Bildirimine İstinaden Yürütülen İnceleme

KARAR ÖZETİ

Veri sorumlusunun sunucularına bulaşan fidye yazılımıyla dosyalar şifrelenmiş, saldırganlar ele geçirdikleri verileri blogda yayınlamıştır.

İhlalin, hizmet sağlayıcıya ait 2003'ten beri kullanılan bir hesabın ele geçirilerek sızma ürünü yüklenmesiyle başladığı değerlendirilmiştir.

660 kişi etkilenmiş olup müşteri/tedarikçi iletişim bilgileri, çalışanlara ait kimlik, fotoğraf, bordro, izin bilgileri, bazı çalışanların kan grubu, Covid-19 ve 2012 tarihli doktor raporu bilgileri açığa çıkmıştır.

KARARIN GEREKÇESİ

KVKK, idari para cezasının uygulanmasını aşağıdaki gerekçelere dayanmıştır:

- Veri sorumlusunun, hizmet aldığı veri işleyenin güvenlik seviyesini yeterince denetlememiş olması nedeniyle müşterek sorumlu olduğu tespit edilmiştir.
- Saldırganların aylarca fark edilmeden sistemde hareket edebilmiş olması (sızma, yanal hareket, yetki ele geçirme), bilişim ağı taramasının ve güvenlik takibinin yetersiz kaldığının göstergesi sayılmıştır.

YAPTIRIM

500.000 TL idari para cezası uygulanmasına karar verilmiştir.

KARAR NO **2024/728**

Finans Ve Muhasebe Alanında Faaliyet Gösteren Uluslararası Bir Meslek Kuruluşu Olan Veri Sorumlusu Tarafından Kurula İntikal Ettirilen Veri İhlal Bildirimine İstinaden Yürütülen İnceleme

KARAR ÖZETİ

Sahte bir CEO e-postasıyla gerçekleştirilen oltalama saldırısı sonucu, bir çalışan doğrulama yapmadan 217 Türk üyenin ad-soyad, üyelik numarası ve bazı durumlarda e-posta bilgilerini harici adrese göndermiştir.

Güvenlik yapılandırması ve çok faktörlü doğrulama önlemleri ihlal sonrasında hayata geçirilmiştir.

KARARIN GEREKÇESİ

KVKK, idari para cezasının uygulanmasını aşağıdaki gerekçelere dayanmıştır:

- Güvenlik yapılandırmasının ancak ihlal sonrasında sıkılaştırılmış olması, risklerin önceden belirlenmediğinin göstergesi sayılmıştır.
- Çalışana eğitim verilmiş olmasına rağmen, farklı görünümdeki bir e-postanın teyit edilmeden yanıtlanmış olması, güvenlik farkındalığının benimsenmediğini ortaya koymuştur.
- 72 saatlik bildirim süresine uyulmaması, ayrı bir yükümlülük ihlali sayılmıştır.

YAPTIRIM

1.000.000 TL idari para cezası uygulanmasına karar verilmiştir

KARAR NO **2022/1407**

Moda Tekstil Faaliyeti Yürüten Veri Sorumlusunun Veri İhlal Bildirimine İstinaden Yürütülen İnceleme

KARAR ÖZETİ

Kimliği belirsiz kişiler, bir müşterinin telefon numarasını ele geçirerek dolandırıcılık amacıyla aramıştır.

Veri sorumlusu tarafında sızıntı tespit edilememiş olup suç duyurusunda bulunulmuş, aynı gün duyuru yapılmıştır.

KARARIN GEREKÇESİ

KVKK, bu aşamada yapılacak bir işlem bulunmadığına ilişkin kararını aşağıdaki gerekçelere dayandırmıştır:

- Veri sorumlusu tarafında herhangi bir sızıntı tespit edilememesi.
- Verilerin başka veri sorumlularından sızmış olabileceği ihtimalinin önemli bir unsur olarak değerlendirilmesi.
- Veri sorumlusunun mali büyüklüğü ve iştigal alanı gözetildiğinde; sızma testi, üç katmanlı kimlik doğrulama, mevcut bir ihlal müdahale planının uygulanması ve gizlilik taahhütnameleri gibi tedbirlerin makul ve yeterli olduğu kanaatine varılması.

YAPTIRIM

Bu aşamada **işlem yapılmamasına** karar verilmiştir.

KARAR NO **2024/756**

Hazır Giyim Ve Tekstil Ürünlerinin Perakende Satışını Gerçekleştiren Veri Sorumlusunun Veri İhlal Bildirimine İstinaden Yürütülen İnceleme

KARAR ÖZETİ

Bir müşterinin siparişinin paketlenmesi sırasında personelin yaptığı hata sonucunda, ilgili kişiye ait kargo ve fatura başka bir müşteriye teslim edilmiştir.

Etkilenen veriler kimlik, iletişim ve sipariş bilgisinden ibaret olup ihlalden yalnızca 1 kişi etkilenmiştir. İlgili kişiye bildirimde bulunulmuştur.

KARARIN GEREKÇESİ

KVKK, bu aşamada yapılacak bir işlem bulunmadığına ilişkin kararını aşağıdaki gerekçelere dayandırmıştır:

- İhlalin, sistemsel bir güvenlik açığından değil, paketleme sürecindeki bir insan hatasından kaynaklanmış olması.
- Tek bir kişinin, sınırlı sayıda veri kategorisiyle etkilenmiş olması.
- İlgili kişiye derhal bilgilendirme yapılmış olması.

YAPTIRIM

Bu aşamada **işlem yapılmamasına** karar verilmiştir.

KARAR NO **2023/1796**

İlgili Kişinin Kişisel Verilerinin Veri Sorumlusu Giyim Mağazasına Ait İnternet Sitesinde Üçüncü Kişilerin Erişimine Açılması

KARAR ÖZETİ

Bir giyim mağazasının internet sitesinde yaşanan teknik bir sorun nedeniyle ilgili kişinin adı, soyadı, telefon numarası ve üyelik bilgileri sınırsız sayıda kişinin erişimine açık hale gelmiştir.

Sorun, şirketin CDN (Content Delivery Network: Dağıtım Ağı) hizmeti aldığı tedarikçi firmanın önbellek (cache) sistemindeki bir cihazda ortaya çıkmıştır.

Şirket, teknik ve idari tedbirleri almanın hizmet aldığı firmanın sorumluluğunda olduğunu, kendi sistemlerinde herhangi bir anormallik tespit edilmediğini ve tüm testlerin sorunsuz geçtiğini savunmuştur.

KARARIN GEREKÇESİ

KVKK, veri sorumlusu hakkında idari para cezası uygulanmasına aşağıdaki gerekçelerle karar vermiştir:

- Veri işleyenden (CDN hizmeti veren firma) hizmet alınması, veri sorumlusunun güvenlik yükümlülüğünü ortadan kaldırmaz; taraflar bu konuda müşterek sorumludur.
- Şirket, sistem güncellemesini canlıya almadan önce yeterli test yapmamıştır.

Bu nedenle, kişisel verilere hukuka aykırı erişimi önleme yükümlülüğü ihlal edilmiştir.

YAPTIRIM

200.000 TL idari para cezası uygulanmasına karar vermiştir.

KARAR NO **2024/790**

Yazılım Ve Teknoloji Odaklı Girişim Yatırımları Ve Geliştirme Faaliyetleri Yürüten Veri Sorumlusu Tarafından Kurula İntikal Ettirilen Veri İhlal Bildirimine İstinaden Yürütülen İnceleme

KARAR ÖZETİ

Veri sorumlusunun mobil uygulamasının veri tabanına yetkisiz erişim sağlanmış ve 7.823 üyeye ait isim, e-posta ve telefon bilgileri etkilenmiştir.

Yeterli log yapısı bulunmadığından erişim yöntemi tespit edilememiş veri bütünlüğü bozulmadığı gerekçesiyle bildirim yapılmamıştır.

YAPTIRIM

350.000 TL idari para cezası uygulanmasına karar vermiştir.

KARARIN GEREKÇESİ

KVKK, aşağıdaki gerekçelerle veri sorumlusunun yükümlülüklerini ihlal ettiği sonucuna varmıştır:

- Tüm veri tabanı alanlarında yeterli log yapısının bulunmaması, erişim kayıtlarının tutulup kontrol edilmesi yükümlülüğüne aykırılık olarak değerlendirilmiştir.
- İhlal sonrasında parola politikasının değiştirilmiş olması, ihlal öncesinde bu konuda yeterli önlem alınmadığının bir göstergesi sayılmıştır.

Bildirim yapılmamasına ilişkin savunma (veri bütünlüğünün bozulmadığı gerekçesi) kabul edilmemiştir. Zira KVKK, ihlalin gizlilik ve erişilebilirlik boyutunun da bulunduğunu ve bunun bildirim yükümlülüğü doğurduğunu belirtmiştir.

KARAR NO **2025/88**

Restoran Zinciri Ve Hızlı Servis Gıda Şirketi Olan Veri Sorumlusu Tarafından Kurula İntikal Ettirilen Veri İhlal

KARAR ÖZETİ

Veri sorumlusu bilgi işlem yöneticisinin mesajlaşma hesabına, kripto varlıklarının ve şirket verilerinin ele geçirildiğini iddia eden saldırganlarca mesaj gönderilmiştir.

İnceleme sonucunda saldırganların, çalışanın bilgisayarına tarayıcı üzerinden çalışan zararlı yazılımla yetkisiz erişim sağladığı ve tarayıcıda kayıtlı kullanıcı adı/şifreleri ele geçirdiği, bu bilgilerle ilgili sisteme erişilerek verilerin elde edildiği tespit edilmiştir.

İhlalden 505.337 müşteriye ait ad-soyad, cinsiyet, e-posta, telefon ve şehir bilgisi etkilenmiştir.

KARARIN GEREKÇESİ

KVKK, idari para cezasının uygulanmasını aşağıdaki gerekçelere dayanmıştır:

- Gerekli teknik ve idari tedbirlerin alınmadığı, sistemde alarm mekanizmasının bulunmadığı ve risklerin önceden belirlenmediği tespit edilmiştir.
- İhlal sonrasında devreye alınan 2FA (Two-Factor Authentication: İki Faktörlü Doğrulama) ve SIEM (Güvenlik Bilgisi ve Olay Yönetimi) gibi güvenlik önlemlerinin ihlal öncesinde mevcut olmadığı belirlenmiştir.
- Veri ihlalinden etkilenen ilgili kişilere en kısa sürede bildirim yapılmadığı anlaşılmıştır.

Veri sorumlusunun ihlal öncesi döneme ait çalışan eğitimi sunamaması, farkındalık çalışmalarında özensizlik göstergesi olarak değerlendirilmiştir.

YAPTIRIM

1.000.000 TL idari para cezası uygulanmasına karar verilmiştir.

KARAR NO **2024/1899**

Avrupa'da Bulunan Grup Şirketlerine Kurumsal Destek Hizmetleri Sağlayan Veri Sorumlusu Tarafından Kurula İntikal Ettirilen Veri İhlal Bildirimine İstinaden Yürütülen İnceleme

KARAR ÖZETİ

Grup şirketlerine kurumsal destek hizmeti veren veri sorumlusunun bir kullanıcı hesabına, Beliz merkezli kara listede bulunan bir IP adresinden yetkisiz erişim sağlanmış, pazarlama amaçlı bu hesap kullanılarak "herkese açık" ayarlanmış klasörlere ve bu klasörlerin bulunduğu FTP (File Transfer Protocol: Dosya Aktarım Protokolü) sunucusuna erişilmiştir.

İhlalden yaklaşık 70.000 kişi etkilenmiştir. Açığa çıkan veriler ad, soyad, e-posta, iletişim ve adres bilgisidir. Kredi kartı veya özel nitelikli veri etkilenmemiştir.

İhlalin başlangıç tarihi tespit edilememiş, uzun süre fark edilmemiştir.

KARARIN GEREKÇESİ

KVKK, idari para cezasının uygulanmasını aşağıdaki gerekçelere dayanmıştır:

- İhlalin defaten yetkisiz erişim şeklinde gerçekleşmesine rağmen uzun süre fark edilememesi, yetersiz takip/kontrolün göstergesi sayılmıştır.
- Kişisel veri içeren klasörlerin "herkese açık" bırakılması, erişim yetkilerinin sınırlandırılması ilkesine aykırı bulunmuştur.
- İhlal sonrası oluşturulan yeni hesapların güçlü parola politikasıyla kurulmuş olması, ihlal öncesinde bu özenin gösterilmediğini ortaya koymuştur.

YAPTIRIM

700.000 TL idari para cezası uygulanmasına karar verilmiştir.

KARAR NO **2025/881**

Telekomünikasyon Teknolojileri Geliştirme Alanında Faaliyet Gösteren Veri Sorumlusunun Veri İhlal Bildirimine İstinaden Yürütülen İnceleme

KARAR ÖZETİ

Bir çalışanın sehven yaptığı işlem sonucunda farklı bir uygulamanın entegrasyonu etkinleşmiş, 488 çalışanın adı, soy adı, iş e-postası ve iş telefonu bilgileri bu uygulama şirketiyle paylaşılmıştır.

İhlal, otomatik e-posta bildirimiyle fark edilmiş, senkronizasyon derhal iptal edilip verilerin silinmesi talep edilmiştir

YAPTIRIM

Bu aşamada **işlem yapılmamasına** karar verilmiştir.

KARARIN GEREKÇESİ

KVKK, veri ihlali hakkında bu aşamada işlem yapılmasına gerek olmadığına aşağıdaki hususları dikkate alarak karar vermiştir:

- İhlalin, kasıt içermeyen bir insan hatasından (uygulamayı yöneten çalışanın sehven yaptığı bir işlem) kaynaklanmış olması.
- Veri sorumlusunun ihlali tespit eder etmez hızlı müdahalede bulunması (senkronizasyon işleminin derhal iptal edilmesi ve verilerin paylaşıldığı şirketten silinmesinin talep edilmesi).
- İlgili çalışanlara son bir yıl içinde kişisel verilerin korunması konusunda eğitim verilmiş olması.
- İhlalin ilgili kişiler üzerinde olumsuz sonuç doğurma olasılığının düşük görülmesi.

KARAR NO **2025/833**

Bilimin İlerlemesini Destekleyen Kâr Amacı Gütmeyen Bir Kuruluş Olarak Faaliyet Gösteren Veri Sorumlusunun Veri İhlal Bildirimine İstinaden Yürütülen İnceleme

KARAR ÖZETİ

Veri sorumlusunun haber bülteni dağıtım platformuna yetkisiz erişim sağlanmış, Türkiye'de ikamet eden 15 kişinin ad, soyad ve e-posta bilgileri etkilenmiştir. İhlal veri işleyenin bildirimiyle öğrenilmiş, platform geçici olarak kapatılmıştır.

Kötüye kullanım bulgusuna rastlanmamış, ilgili kişilere bildirim yapılmıştır.

YAPTIRIM

Bu aşamada **işlem yapılmamasına** verilmiş ve ayrıca veri sorumlusuna gelecekteki bildirimlerde **"Kişisel Veri İhlal Bildirim Formu" kullanılması** gerektiği hatırlatılmıştır.

KARARIN GEREKÇESİ

KVKK, aşağıdaki hususlara dayanarak olayı düşük riskli olarak değerlendirmiştir:

- Etkilenen veri kategorisinin sınırlı olması.
- Kötüye kullanıma ilişkin herhangi bir bulgu bulunmaması.
- İlgili kişilere bildirim yapılmış olması.
- MFA (Multi-Factor Authentication: Çok Faktörlü Kimlik Doğrulama) dahil ek güvenlik tedbirlerinin alınmış olması.

Ayrıca KVKK, veri sorumlusuna, ileride yapılacak bildirimlerde standart bildirim formunun kullanılması gerektiğini hatırlatmıştır.

KARAR NO **2025/536**

Küçük Ev Aletleri Üretimi Ve Satışı Yapan Veri Sorumlusunun Veri İhlal Bildirimine İstinaden Yürütülen İnceleme

KARAR ÖZETİ

Müşterilere gönderilen toplam 14 bilgilendirme e-postasında alıcı adresleri sehven gizlenmeden iletilmiş, bu nedenle e-posta adresleri sehven üçüncü kişilerle paylaşılmıştır.

Her e-posta en az 29, en çok 65 kişiye iletilmiş, ihlal, ilgili çalışan tarafından gönderim sonrası hemen fark edilerek e-postaların geri çekilmesi için aksiyon alınmıştır. Bu nedenle bazı alıcılara e-posta iletilmişken bazılarına iletilmemiştir.

İhlalden tahmini 500 müşteri etkilenmiş, açığa çıkan veri yalnızca e-posta adresinden ibarettir. İlgili kişilere e-posta ve çağrı merkezi yoluyla bildirim yapılacağı belirtilmiştir.

KARARIN GEREKÇESİ

KVKK, aşağıdaki hususları birlikte değerlendirerek işlem tesis edilmesine gerek olmadığına karar vermiştir:

- İhlal fark edilir edilmez e-postaların geri çekilmesi yoluyla anlık müdahalede bulunulması.
- Açığa çıkan verinin yalnızca e-posta adresiyle sınırlı olması.
- Bu sınırlılık nedeniyle, ilgili kişiler üzerinde olumsuz sonuç doğurma riskinin düşük görülmesi.

Bu üç unsurun birlikte gerçekleşmesi nedeniyle KVKK, herhangi bir işlem yapılmasına gerek görmemiştir.

YAPTIRIM

Bu aşamada **yapılacak bir işlem bulunmadığına** karar verilmiştir.

KARAR NO **2023/1017**

Dijital Oyun Ve Eğlence Platformları Sunan Veri Sorumlusu Tarafından Kurula İntikal Ettirilen Veri İhlal Bildirimine İstinaden Yürütülen İnceleme

KARAR ÖZETİ

Saldırgan, bir güvenlik açığını kullanarak iki kez ihlal gerçekleştirmiştir. Veri tabanına erişip verileri dışarı aktarmış ve forumda satışa çıkarmıştır.

Türkiye'de 90.182 kişinin kullanıcı adı, isim, e-posta, doğum tarihi ve site bilgileri etkilenmiş, şifreler ele geçirilmemiştir.

Etkilenenler arasında çocukların bulunması nedeniyle risk yüksek bulunmuştur.

YAPTIRIM

1.500.000 TL idari para cezası uygulanmasına karar verilmiştir.

KARARIN GEREKÇESİ

KVKK, idari para cezasının uygulanmasını aşağıdaki gerekçelere dayanmıştır:

- İhlalin veri sorumlusunca değil, bir forum paylaşımıyla fark edilmiş olması esas alınmıştır.
- Log kayıtlar takibi eksikliği.
- Sızma testi (pentest; sistemlere yetkili şekilde simüle edilmiş saldırılar düzenlenerek güvenlik açıklarının tespit edildiği test) eksikliği.
- Aynı güvenlik açığının iki kez kullanılabilmiş olması, hızlı raporlama düzeninin bulunmadığını göstermiştir.
- Yama (sistemdeki güvenlik açıklarını kapatmak için üretici tarafından yayımlanan güncelleme) yönetiminin ancak ihlal sonrasında uygulamaya alınması, güvenlik tedbirlerinin düzenli kontrol edilmediğini göstermiştir.

KARAR NO **2024/413**

Tarım Makineleri, Traktör Ve Tarımsal Ekipman Üretimi İle Ticareti Alanında Faaliyet Gösteren Veri Sorumlusu Tarafından Kurula İntikal Ettirilen Veri İhlal Bildirimine İstinaden Yürütülen İnceleme

KARAR ÖZETİ

Veri sorumlusunun bağlı olduğu yurtdışı şirketin sistemleri fidye yazılımıyla şifrelenmiş, bu ihlal Türkiye'deki veri sorumlusunu da etkilemiştir.

Saldırganlar verileri çaldıklarını belirterek fidye talep etmiş, örnek verileri darkweb'de (normal arama motorlarınca indekslenmeyen ve Tor gibi özel tarayıcılarla erişilen, internetin gizli bir bölümü) yayınlamıştır.

İhlalden 56 çalışan etkilenmiş olup kimlik, iletişim, özlük bilgileri ile bazı çalışanların kaza raporu ve sağlık bilgileri açığa çıkmış ve dışarıya sızdırılmıştır.

YAPTIRIM

150.000 TL idari para cezası uygulanmasına karar verilmiştir.

KARARIN GEREKÇESİ

KVKK, idari para cezasının uygulanmasını aşağıdaki gerekçelere dayanmıştır:

- İhlal sonucu verilerin dışarıya sızdırılmış olması, sızma/anormal hareket takibinde eksikliğin göstergesi sayılmıştır.
- Fidye yazılımı saldırısının çok faktörlü kimlik doğrulama ile engellenebilecek olmasına rağmen bu mekanizmanın ancak ihlal sonrasında etkinleştirilmesi.
- Bilinen açıklara yönelik yama çalışmalarının ancak ihlal sonrasında yapılmış olması.
- Ortak sunucu sistemi kullanımı nedeniyle ihlalin birden çok veri sorumlusuna yayılabilmiş olması; bunun hem ağ segmentasyonu eksikliği (teknik), hem sistemin bu şekilde kurgulanmış olması (idari) bakımından eksiklik sayılması.

KARAR NO **2024/1523**

Turizm, Otelcilik Ve Konaklama İşletmeciliği Yapan Veri Sorumlusu Tarafından Kurula İntikal Ettirilen Veri İhlal Bildirimine İstinaden Yürütülen İnceleme

KARAR ÖZETİ

Veri sorumlusu bünyesindeki bir personele gönderilen phishing e-postasındaki bağlantının açılması sonucu bilgisayarı yetkisiz üçüncü kişilerce kontrol edilmiştir.

Personelin bilgisayarı açamadığını bildirmesiyle ihlal tespit edilmiş, bilgisayar aynı gün ağdan izole edilmiştir.

Etkilenen tek dosya, ön büro personelinin ad, soyad bilgilerini içeren vardiya çizelgesi olup ihlalden 450 çalışan etkilenmiştir, verilerin dışarı çıkarıldığına dair anormal trafik tespit edilmemiştir.

YAPTIRIM

500.000 TL idari para cezası uygulanmasına karar verilmiştir.

KARARIN GEREKÇESİ

KVKK, idari para cezasının uygulanmasını aşağıdaki gerekçelere dayanmıştır:

- İhlalin tek bilgisayarla sınırlı kalmasına rağmen, bilgi güvenliği denetim raporundaki sistemik eksiklikler esas alınmıştır.
- Güncel olmayan sunucu/veritabanı sistemlerinin kullanılması.
- Zayıf parola kullanımı.
- SSL (Secure Sockets Layer: Güvenli Yuva Katmanı) ve web uygulama zayıflıkları.
- Spam korumasının yetersiz olması.
- Sunucu odalarına fiziksel erişimde kimlik doğrulama bulunmaması.

.

KARAR NO **2023/1675**

Endüstriyel Mutfak Ekipmanları Üretimi Yapan Veri Sorumlusunun Veri İhlal Bildirimine İstinaden Yürütülen İnceleme

KARAR ÖZETİ

İnsan kaynakları uygulamasında bireysel gönderim yerine sehven toplu gönderim yapılması sonucu 1522 çalışanın ad-soyad, T.C. kimlik no ve adres bilgisi 1589 çalışana gönderilmiştir. İhlal, personel geri bildirimiyle aynı gün tespit edilmiştir.

YAPTIRIM

Bu aşamada **işlem yapılmamasına** karar verilmiştir.

KARARIN GEREKÇESİ

KVKK, bu aşamada yapılacak bir işlem bulunmadığına ilişkin kararını aşağıdaki gerekçelere dayandırmıştır

- Menü karışıklığından kaynaklanan hatanın, yazılım geliştirme aşamasında öngörülmesinin mümkün olmaması.
- Veri sorumlusunun ihlal sonrasında derhal düzeltme talebinde bulunmuş olması.
- Düzenli eğitim verilmesi ile VLAN (Virtual Local Area Network: anal Yerel Alan Ağı), VPN (Virtual Private Network: Sanal Özel Ağ) ve PAM (Privileged Access Management: Ayrıcalıklı Erişim Yönetimi) gibi teknik tedbirler ile sızma testinin mevcut olması.
- İhlalin aynı gün tespit edilmiş olması, güvenlik takibinin yapıldığının kanıtı sayılmıştır.

KARAR NO **2024/133**

Online Yemek Siparişi, Restoran Entegrasyonu Ve Teslimat/Kurye Hizmetleri Veren Veri Sorumlusu Tarafından Kurula İntikal Ettirilen Veri İhlal Bildirimine İstinaden Yürütülen İnceleme

KARAR ÖZETİ

Siber saldırganlar veri sorumlusunun veri tabanına saldırarak verileri silmiş, ele geçirmiş ve fidye talep etmiştir.

İhlalden 1.362 kullanıcının ad-soyad, telefon, adres ve e-posta bilgileri etkilenmiştir.

Ulusal Siber Olaylara Müdahale Merkezi yapılan bildirimde saldırının hizmet reddi şeklinde olduğu, sebep olarak da yönetim paneli şifresinin tarayıcıya kaydedilmesi ve IP adres erişiminin sınırlandırılmamış olması gösterilmiştir.

YAPTIRIM

250.000 TL idari para cezası uygulanmasına karar verilmiştir.

KARARIN GEREKÇESİ

KVKK, idari para cezasının uygulanmasını aşağıdaki gerekçelere dayanmıştır:

- Yönetim paneli şifresinin tarayıcıya kaydedilmiş olması, parola güvenliğinde gerekli özenin gösterilmediğinin göstergesi sayılmıştır.
- Veri tabanı yönetim yazılımında IP (Internet Protocol: İnternet Protokolü) adres erişiminin sınırlandırılmamış olması, yetkisiz erişime imkân tanıyan bir eksiklik olarak değerlendirilmiştir.
- KVKK, bu tür tedbirlerin yüksek maliyet gerektirmeyen, düşük maliyetli veya sistemde zaten mevcut olabilecek önlemler olduğunu vurgulayarak, alınmamış olmalarını gerekli özenin gösterilmediğinin kanıtı saymıştır.

KARAR NO **20223/1787**

İlgili Kişinin Covid-19 Test Sonucunun Veri Sorumlusu Tarafından Veri Kayıt Sisteminde Bulunan Eski Cep Telefonu Numarasına Gönderilmesine İlişkin Şikâyet

KARAR ÖZETİ

İlgili kişi, Covid-19 test sonucunun kendi belirttiği güncel telefon numarası yerine sistemde kayıtlı eski (dayısına ait) telefon numarasına gönderildiğini, sağlık bilgisinin bu şekilde üçüncü bir kişiyle paylaşıldığını şikayet etmiştir.

Veri sorumlusu, 2011 yılında verilen rızayla kayıtlı numaranın kullanıldığını, rızanın hukuka uygunluk sebebi olduğunu ve kamu sağlığı gerekçesiyle hareket edildiğini savunmuştur.

YAPTIRIM

30.000 TL idari para cezası uygulanmasına ve güncel numaranın sisteme işlenmesi ve **eski numaranın imha edilmesi yönünde talimat** verilmesine karar verilmiştir.

KARARIN GEREKÇESİ

KVKK, idari para cezasının uygulanmasını aşağıdaki gerekçelere dayanmıştır:

- İlgili kişinin açıkça yeni bir telefon numarası bildirmiş olmasına rağmen, veri sorumlusunun sistemdeki eski kaydı esas almış olması.
- Bu durumun, kişisel verilerin doğru ve güncel tutulması yükümlülüğüne aykırılık teşkil etmesi.
- Veri sorumlusunun 2011 tarihli rıza ve kamu sağlığı savunmalarının, ilgili kişinin sonradan bildirdiği güncel iletişim tercihini geçersiz kılmamış olması.

KARAR NO **2024/415**

Otomotiv Sektöründe Faaliyet Gösteren Bir Yan Sanayi Üretim Firması Olan Veri Sorumlusu Tarafından Kurula İntikal Ettirilen Veri İhlal Bildirimine İstinaden Yürütülen İnceleme

KARAR ÖZETİ

Veri sorumlusunun Fransa'daki iş ortağı sunucularına Lockbit (Tehlikeli ve veri şifreleyen küresel fidye yazılım türü) fidye yazılımıyla saldırı düzenlenmiş, Metro Ethernet bağlantısı üzerinden Türkiye'deki 8 sunucuya da bulaşmıştır.

İhlalden çalışan, müşteri ve kullanıcı olmak üzere 43 kişi etkilenmiş, kayıt sayısının 100.000'i aşabileceği belirtilmiştir, işlem güvenliği, finans ve pazarlama verileri açığa çıkmıştır. İlgili kişilere e-posta ile bildirim yapılmıştır.

YAPTIRIM

430.000 TL idari para cezası uygulanmasına karar verilmiştir.

KARARIN GEREKÇESİ

KVKK, idari para cezasının uygulanmasını aşağıdaki gerekçelere dayanmıştır:

- Fransa'da başlayan saldırının Türkiye'deki 8 sunucuya da yayılmış olması, ağ segmentasyonunun yeterli yapılmadığının göstergesi sayılmıştır.
- Sızma testi (pentest; sistemlere yetkili şekilde simüle edilmiş saldırılar düzenlenerek güvenlik açıklarının tespit edildiği test) yaptırılmamış olması.
- Sistemin düzenli takip/kontrolüne ilişkin herhangi bir rapor sunulamaması.

Bu hususlar, güvenlik açıklarının önceden tespit edilip önlenemediğini ortaya koymuştur.

KARAR NO **2023/412**

Bir Hosting Firması Tarafından Kurula İntikal Ettirilen Veri İhlal Bildirimine İstinaden Yürütülen İnceleme

KARAR ÖZETİ

Hosting firmasının yazılımındaki güvenlik açığı nedeniyle sunucudaki veriler yetkisiz erişimle Almanya'daki bir IP'ye aktarılmış, dark web'de yayınlanmıştır.

İhlal 6 ay sonra tespit edilmiş olup 31.179 kişinin kimlik, iletişim, finans bilgileri ve 3.027 kredi kartı verisi etkilenmiştir.

YAPTIRIM

350.000 TL idari para cezası uygulanmasına karar verilmiştir.

KARARIN GEREKÇESİ

KVKK, idari para cezasının uygulanmasını aşağıdaki gerekçelere dayanmıştır:

- Sızıntının 6 ay sonra fark edilmiş olması, ciddi bir takip eksikliği sayılmıştır.
- Toplu veri indirme korumasının ihlal öncesinde bulunmayıp ancak ihlal sonrasında alınmış olması.
- Saldırı tespit sisteminin ihlal öncesinde bulunmayıp ancak ihlal sonrasında alınmış olması.
- İki faktörlü kimlik doğrulamanın ihlal öncesinde bulunmayıp ancak ihlal sonrasında alınmış olması.
- Veri maskeleme/minimizasyon ilkesinin benimsenmemiş olması.

KARAR NO **2022/707**

Mağazacılık Hizmeti Veren Veri Sorumlusu Tarafından Kurula İntikal Ettirilen Veri İhlal Bildirimine İstinaden Yürütülen İnceleme

KARAR ÖZETİ

Veri işleyende yaşanan teknik bir hata nedeniyle bazı mobil e-ticaret müşterileri, üyelik sayfalarına girdiklerinde başka üyelere ait bilgileri (ad-soyad, telefon, e-posta, maskeli kredi kartı numarası) görüntülemiştir.

İhlal, bir müşterinin çağrı merkezine bildirimi üzerine tespit edilmiş, sistem kısa süreliğine kapatılarak hata giderilmiştir

Kesin olarak 17, en fazla 136 kişinin etkilendiği tahmin edilmiştir. İlgili kişilere bildirim yapılmıştır.

YAPTIRIM

Bu aşamada **yapılacak bir işlem bulunmadığına** karar verilmiştir.

KARARIN GEREKÇESİ

KVKK, bu aşamada yapılacak bir işlem bulunmadığına ilişkin kararını aşağıdaki gerekçelere dayandırmıştır:

- Verilerin kamuya ifşa olmaması ve ihlalin kısa sürede tespit edilip müdahale edilmiş olması, kötüye kullanılma ihtimalinin düşük olduğunun göstergesi sayılmıştır.
- Kesin kişi sayısının tespit edilememesinin, tedarikçinin uluslararası bilgi güvenliği standartlarına uygun veri sınırlandırması yapmasından kaynaklandığı değerlendirilmiştir.
- Sistemin derhal kapatılıp hatanın giderilmiş olması, etkin bir güvenlik takibinin göstergesi olarak değerlendirilmiştir.

KARAR NO **2024/1718**

Kozmetik Ve Kişisel Bakım Şirketi Olan Veri Sorumlusu Tarafından Kurula İntikal Ettirilen Veri İhlal Bildirimine İstinaden Yürütülen İnceleme

KARAR ÖZETİ

Veri sorumlusunun ağ sunucusuna trojan virüsü bulaştırılarak siber saldırganlarca bazı kişisel verilere erişilmiş, 45 Bitcoin fidye talep edilmiştir.

İhlalden Türkiye'den 432 müşteri/iş ortağı etkilenmiştir. 325 kişinin nüfus cüzdanı/ikamet belgesi ile 107 marka elçisinin kimlik ve iletişim bilgileri açığa çıkmıştır.

YAPTIRIM

500.000 TL idari para cezası uygulanmasına karar verilmiştir.

KARARIN GEREKÇESİ

KVKK, idari para cezasının uygulanmasını aşağıdaki gerekçelere dayanmıştır:

- EDR (Endpoint Detection and Response: Uç Nokta Tespiti ve Yanıtı) çözümünün ihlal öncesinde değil, ancak ihlal sonrasında devreye alınmış olması, güvenlik takibi konusundaki eksikliğin göstergesi sayılmıştır.
- Sistemde düzenli tarama/tehdit tespiti yapan bir ürünün bulunmaması, aynı eksikliğin bir diğer göstergesi olarak değerlendirilmiştir.
- İhlal öncesinde sızma testi (pentest; sistemlere yetkili şekilde simüle edilmiş saldırılar düzenlenerek güvenlik açıklarının tespit edildiği test) yaptırılmamış olması, risk analizi ve önlem planlama sürecinde yeterli özen gösterilmediği sonucuna dayanak oluşturmuştur.
- Bu hususa dair herhangi bir güvenlik taraması raporu sunulamaması, aynı sonucu destekleyen bir unsur olarak değerlendirilmiştir.

KARAR NO **2022/714**

Tarımsal Emtia Ticareti Alanında Faaliyet Gösteren Veri Sorumlusu Tarafından Kurula İntikal Ettirilen Veri İhlal Bildirimine İstinaden Yürütülen İnceleme

KARAR ÖZETİ

Üst düzey yöneticinin e-posta hesabı ele geçirilerek yaklaşık 1.000 kişiye oltalama e-postası gönderilmiş olup müşteri, tedarikçi ve çalışanlara ait ad, soyad, e-posta ve unvan bilgileri etkilenmiştir.

İhlal bir müşteri bildirimiyle fark edilmiş, saldırgan 2-3 gün erişim sağlamıştır.

YAPTIRIM

200.000 TL idari para cezası uygulanmasına karar verilmiştir.

KARARIN GEREKÇESİ

KVKK, idari para cezasının uygulanmasını aşağıdaki gerekçelere dayanmıştır:

- Gelişmiş kimlik doğrulama ve saldırı tespit sistemlerinin ihlal öncesinde değil, ancak ihlal sonrasında devreye alınmış olması, güvenlik takibindeki eksikliğin göstergesi sayılmıştır.
- İhlalin veri sorumlusunca değil, bir müşteri bildirimiyle fark edilmiş olması.
- Saldırganın günlerce erişim sağlayabilmiş olması, log kayıtlarının düzenli kontrol edilmediğini ortaya koymuştur.
- Güçlü ve tekrarsız parola kullanımına ilişkin bir politikanın etkin şekilde uygulanmamış olması, ayrı bir eksiklik olarak değerlendirilmiştir.

KARAR NO **2024/1898**

İlaç Ve Sağlık Ürünleri Alanında Faaliyet Gösteren Veri Sorumlusu Tarafından Kurula İntikal Ettirilen Veri İhlal Bildirimine İstinaden Yürütülen İnceleme

KARAR ÖZETİ

Veri sorumlusunun sunucusu Ransomware (fidye yazılımı) virüsüyle şifrelenmiş, saldırgan zararlı yazılım indirip çalıştırarak verileri şifrelemiştir. İlk erişim yöntemi kesin tespit edilememiş, RDP (Remote Desktop Protocol: Uzak Masaüstü Protokolü) veya veri tabanı servisi üzerinden parola denemesiyle sağlanmış olabileceği değerlendirilmiştir.

İhlalden 520 kişi (196 mevcut çalışan, 303 eski çalışan, 17 müşteri/iş ortağı) etkilenmiştir. Kimlik, iletişim, özlük ve müşteri işlem bilgileri açığa çıkmıştır.

Verilerin sızdırıldığına dair kanıt bulunamamıştır

YAPTIRIM

350.000 TL idari para cezası uygulanmasına karar verilmiştir.

KARARIN GEREKÇESİ

KVKK, idari para cezasının uygulanmasını aşağıdaki gerekçelere dayanmıştır:

- Saldırganın sunucu üzerinde zararlı yazılım indirme, çalıştırma ve kod çalıştırma gibi çok aşamalı işlemler gerçekleştirebilmiş olması, güvenlik takibindeki özensizliğin göstergesi sayılmıştır.
- İhlal sonrası hazırlanan Siber Olay Müdahale Raporu'nda önerilen ağ, sunucu, kullanıcı güvenliği ve test/denetim tedbirlerinin ihlal öncesinde yetersiz kaldığı tespit edilmiştir.
- Saldırganın olası giriş yöntemlerinin RDP kaba kuvvet saldırısı veya veri tabanı parola denemesi olabileceği belirlenmiştir.
- Log kayıtlarının silinmiş olması, bu tespiti destekleyen bir unsur olarak değerlendirilmiştir.
- Saldırganın yetki yükselterek kalıcılık sağlaması, bu tespiti destekleyen bir diğer unsur olarak değerlendirilmiştir.

Bora Yazıcıoğlu
bora@yazicioglulegal.com

Şerife Âmine Mümin
serife@yazicioglulegal.com

Ezgi Girenay
ezgi@yazicioglulegal.com