

KİŞİSEL VERİLERİ KORUMA KURULUNUN, 9 AĞUSTOS 2021 TARİHLİ KARAR ÖZETLERİ



Kişisel Verileri Koruma Kurulu (“KVK Kurulu” veya “Kurul”)’nun on bir yeni karar özeti, Kurumun internet sitesi üzerinden 09.08.2021 tarihli duyuru ile yayımlandı.

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

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

“BİR PERAKENDE GİYİM FİRMASININ VERİ İHLAL BİLDİRİMİ HAKKINDA” KİŞİSEL VERİLERİ KORUMA KURULUNUN 20/01/2020 TARİH VE 2020/50 SAYILI KARAR ÖZETİ



**VERİ SORUMLUSU:
PERAKENDE GİYİM FİRMASI**

**KARAR TARİH: 20/01/2020
KARAR SAYI : 2020/50**

**İLGİLİ İLKELER :
KİŞİSEL VERİ İŞLEME GENEL
İLKELERİ**

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

**UYGULANAN YAPTIRIM :
50.000-TL İPC**

Veri sorumlusu giyim firması tarafından yapılan veri ihlal bildiriminde ihlalin bazı müşterilerin yeni bir hesap açarken kişisel verilerinin yanlışlıkla bir URL üzerinden veri sorumlusunun iç sistemlerine ve çalıştığı bazı üçüncü taraf satıcı/sağlayıcılara aktarılması şeklinde gerçekleştiği bildirilmiştir. İhlalden aboneler/üyeler, müşteriler/potansiyel müşteriler etkilenmiş olup 44 kişinin e-posta adresi, doğum tarihi, açık metin şeklinde şifre verilerinin olduğu, ayrıca zorunlu alan olmayan ad soyad verilerinin de etkilenmiş olabileceği Kuruma bildirilmiştir. Aynı zamanda ilgili kişilere 23.07.2019 tarihinde e-posta yoluyla bildirim yapıldığı ifadelerine yer verilmiştir.



Kişisel Verileri Koruma Kurulunun 20/01/2020 tarih ve 2020/50 sayılı Kararı ile;

01.08.2018 ve 21.10.2018 tarihlerinde gerçekleşen veri ihlallerinin tespitinin yaklaşık bir yıl sonra 02.07.2019 tarihinde yapılmış olmasının, gerçekleştirilen işlemlere dair Şirketin log kaydı/takip alarm sistemlerinin bulunmadığının ya da etkin bir şekilde kullanılmadığının ve Şirket tarafından gerekli kontrollerin yapılmadığının göstergesi olduğu değerlendirilmektedir. Bununla birlikte URL üzerinden kişisel verilerin üçüncü taraf satıcı/sağlayıcılar tarafından görülmesinin web sayfası tasarım aşamasında iken yapılan testlerin yetersiz olduğunun veya gerekli testlerin yapılmadığının göstergesi olduğu kanaatine varılarak Web sayfası tasarım aşamasında iken yapılan testlerin yetersiz olması sebebiyle veri güvenliğini sağlamaya yönelik gerekli teknik ve idari tedbirleri almadığı gerekçesiyle veri sorumlusu hakkında **50.000 TL idari para cezası** uygulanmasına karar verilmiştir.

Veri ihlal bildiri veri sorumlusu şirket tarafından zamanında yapıldığı ve gerekli araştırmalar yapıldığından bu hususlarda kanunen yapılacak bir şey olmadığı kararda yer almıştır.

“BİLGİSAYAR OYUNLARI ALANINDA FAALİYET GÖSTEREN VERİ SORUMLUSUNUN VERİ İHLALİ BİLDİRİMİ HAKKINDA” KİŞİSEL VERİLERİ KORUMA KURULUNUN 05/05/2020 TARİH VE 2020/345 SAYILI KARAR ÖZETİ



**VERİ SORUMLUSU:
BİLGİSAYAR OYUNU
FAALİYETİ GÖSTEREN ŞİRKET**

**KARAR TARİH :05/05/2020
KARAR SAYI : 2020/345**

İLGİLİ İLKELER :

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

**UYGULANAN YAPTIRIM :
130.000-TL İPC**

Veri sorumlusu tarafından Kuruma yaptığı ihlal bildiriminde; ihlalin rutin güvenlik denetimi sırasında eski bir çalışan tarafından içerisinde kaynak kod ile veri dosyaları içeren bir klasörün yetkisiz olarak github.com internet sitesine yüklenmesi sonucunda gerçekleştiği belirtilmiştir. Veri sorumlusu tarafından yürütülen inceleme neticesinde klasör içerisinde yer alan birçok dosyada kullanıcıların bir alt kümesinin kimliğini belirleyebilecek bilgilerin bulunulabildiği tespit edilmiş olsa da, bu verilerin büyük bir kısmının veri sorumlusu hizmetlerinden men edilmiş sahte hesaplara ait olduğu ifade edilmiştir. İhlal bildiriminde hem gerçek kişi hem de bot hesaplarına ait verilerin ihlal edildiği, ihlalden etkilenen 62 kişi olduğu ve bunlardan az da olsa bir kısmının çocuk olduğu bilgisi verilmiştir. Bu kişilerin kimlik, doğum tarihi, e-posta adresi, internet hizmet sağlayıcı ve kullanıcı kayıt tarihi ve saati gibi bilgilerin etkilendiği ifade edilmiştir.

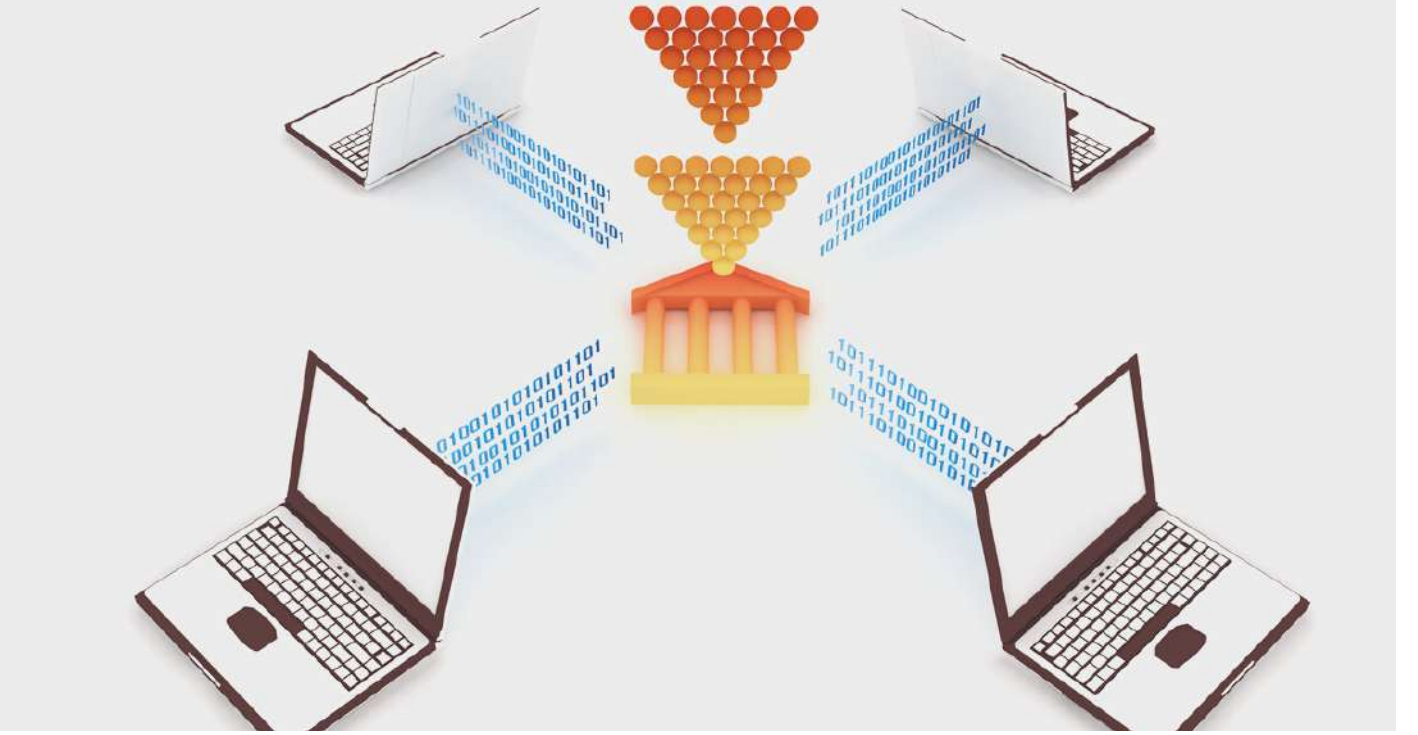


Kişisel Verileri Koruma Kurulunun 05/05/2020 tarih ve 2020/345 sayılı Kararı ile;

Veri sorumlusunun eski çalışanın veri sorumlusuna ait kaynak kodları github.com internet sitesine yüklemiş olmasının bir güvenlik açığı olduğu, bu kaynak kodların yetkisiz üçüncü kişiler tarafından analiz edilerek başka güvenlik açıklıklarına sebebiyet verebileceği dikkate alındığında veri sorumlusu tarafından gerekli teknik ve idari tedbirlerin yeterince alınmamış olduğunun göstergesi olduğu değerlendirilmiştir. Bunun yanı sıra, personele çok sayıda veri politikasının imzalatıldığına beyan edilmesine rağmen söz konusu çalışanın kişisel verileri içeren dosyaları taşınabilir belleğe depolamasının politikaların etkin şekilde uygulanmadığı ve yeterli farkındalığın oluşturulmadığı kanaatine varılmış, nitekim çalışana yönelik farkındalık çalışmaları yapılmadığı, gerekli eğitimlerin verilmediği ve güvenlik risklerinin belirlenmediği, “İzin Verilmedikçe Her Şey Yasaktır” prensibine uygun davranmadığı tespit edilmiştir. Kurul, ihlalin gerçekleşme tarihinden neredeyse iki yıl sonra ihlalin tespit edilmesinin veri sorumlusunun güvenlik kontrollerini düzenli olarak yapmadığı, dolayısıyla alması gereken teknik ve idari tedbirlerin yetersiz kaldığını değerlendirerek veri sorumlusu hakkında **100.000 TL idari para cezasına** hükmetmiştir.

Bunun yanı sıra; veri ihlalinin 09.01.2019 tarihinde tespit edilmesine rağmen Kuruma 28.02.2019 tarihinde bildirim yapıldığı gözetilerek, veri sorumlusunun “en kısa sürede” bildirimde bulunma yükümlülüğüne aykırılık teşkil etmesi nedeniyle 30.000 TL ek olmak üzere toplam 130.000 TL idari para cezası uygulanmasına karar verilmiştir.

“BİR BANKANIN VERİ İHLALİ BİLDİRİMİ HAKKINDA” KİŞİSEL VERİLERİ KORUMA KURULUNUN 07/05/2020 TARİH VE 2020/359 SAYILI KARAR ÖZETİ



**VERİ SORUMLUSU:
BANKA**

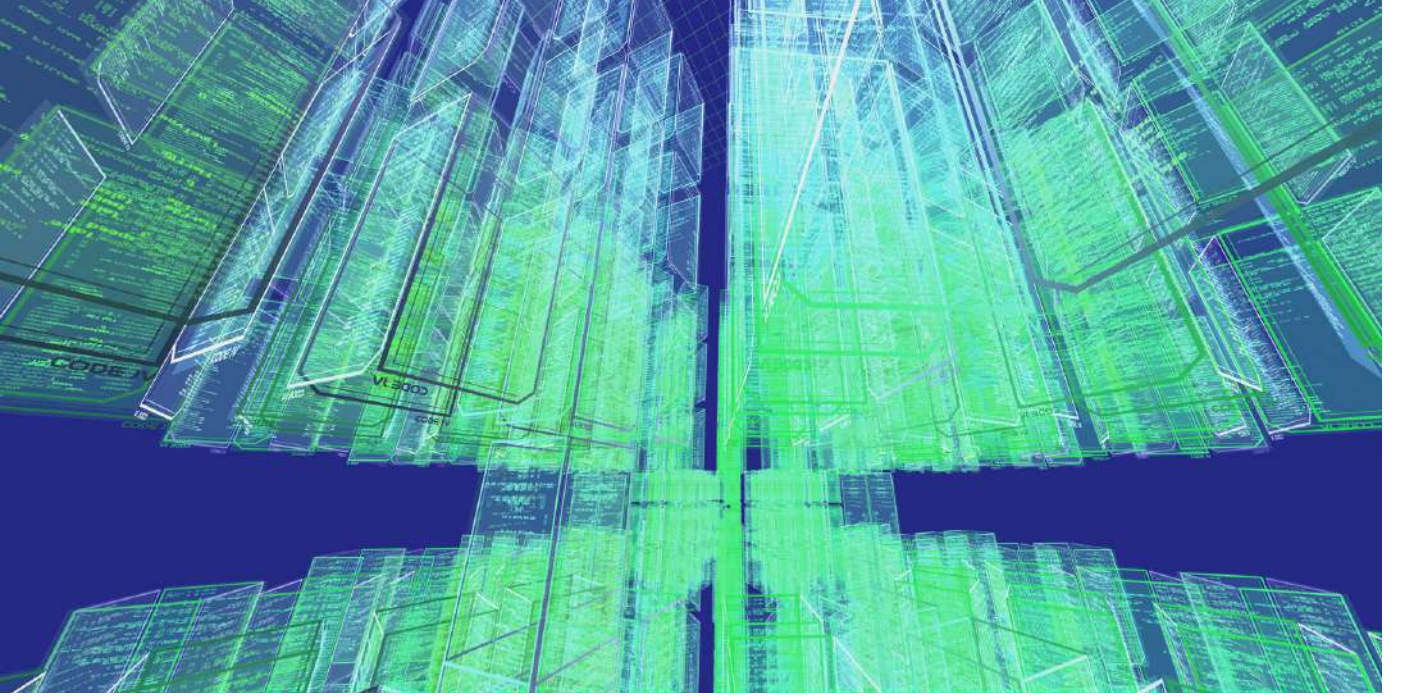
**KARAR TARİH:07/05/2020
KARAR SAYI : 2020/359**

İLGİLİ İLKELER :

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

**UYGULANAN YAPTIRIM :
450.000-TL İPC**

Veri sorumlusunun Kuruma intikal eden veri ihlali bildiriminde; ihlalin, KKB ekranında, Veri Sorumlusu Banka'nın eski çalışanın için gereğinden fazla adette sorgulama yapması sonucu gerçekleştiği belirtilmiştir. Çalışanın ifadesinde; T.C. kimlik numaraları Banka dışından 3. şahıs tarafından iletilip kişilerin kredi skorlarının öğrenilmek istendiği bilgisi verilmiştir. İlgili bildirimde ihlalin Temmuz 2018 ile Mayıs 2019 tarihleri arasında gerçekleştiği, ihlalden veri sorumlusunun müşterisi olan ve müşterisi olmayan toplam 5695 kişinin etkilendiği bilgileri verilmiştir. İhlalden etkilenen kişisel verilerin ise şahısların bankalardan kullanmış oldukları tüm kredili ürünlere ilişkin geçmişleri, ödeme performansları ve borç rakamları, adres, telefon bilgileri olduğu ifadelerine yer verilmiştir.



Kişisel Verileri Koruma Kurulunun 07/05/2020 tarih ve 2020/359 sayılı Kararı ile;

İhlalin neredeyse bir seneye yakın sürmesi sebebiyle veri sorumlusu tarafından kişisel verilerin korunmasına ilişkin kişisel veri güvenliği takibinin uygun zaman aralıklarıyla yapılmadığının ve ihlal öncesinde yapılması gereken çalışanlarının log kayıtlarında kullanıcı bazında yetki sınırlaması, ekranlara erişimlerin kısıtlanması, kişisel verilerin korunmasına ilişkin uyarılara yer verilmesi gibi kullanıcı yetki ve rollerine yönelik kontrol ve düzenlemeler ile teknik ve idari tedbirleri ihlal öncesinde almadığının göstergesi olduğunu değerlendirmiştir.

Kurul kararına göre, veri ihlalinden önce sorgulanabilecek kişi sayısının sınırlandırılmamış olması ve ancak ihlalin gerçekleşmesinden sonra 250 üzerinde sorgulama yapan

kullanıcıların kamera kayıtları incelenerek veri ihlali oluşturacak bir durum olup olmadığının kontrol edilmesi de, ihlal öncesinde olası risklerin ve tehditlerin tespit edilmediğinin göstergesi kabul edilmiştir. Ek olarak, çalışanlara Kişisel Verilerin Korunması Kanunu konusunda belli aralıklarla eğitim ve farkındalık çalışmalarının yapıldığının belgeler ile kanıtlanamadığı için Kanun'a uygun olarak çalışanlara eğitim verilmediğini tespit etmiştir. Sayılan tüm bu sebeplerle veri güvenliğini sağlamaya yönelik gerekli teknik ve idari tedbirleri almadığı gerekçesiyle veri sorumlusu Banka'ya 400.000 TL idari para cezası verilmiştir.

Ayrıca ihlal tespit edildikten sonra geçerli bir sebep olmaksızın Kurula en kısa sürede bildirilmediği için bildirimde bulunma yükümlülüğüne aykırı davranmaktan veri sorumlusu hakkında 50.000 TL de ek olmak üzere toplam **450.000 TL idari para cezası** uygulanmasına karar vermiştir.

“KİŞİSEL BAKIM SEKTÖRÜNDE FAALİYET YÜRÜTEN BİR VERİ SORUMLUSUNUN VERİ İHLALİ BİLDİRİMİ HAKKINDA” KİŞİSEL VERİLERİ KORUMA KURULUNUN 22/05/2020 TARİH VE 2020/421 SAYILI KARAR ÖZETİ



Veri sorumlusunun Kuruma intikal eden veri ihlali bildiriminde; ihlalin, 06.03.2020 tarihinde veri sorumlusu e-posta adresine kimliği belirsiz bir şahıstan web sitesi üyelerinin e-posta adresini/şifrelerini ele geçirdiğine dair bir mesaj gelmesi sonucunda yapılan incelemelerde, veri sorumlusu ile herhangi bir ilişkisi olmayan üçüncü kişilerin veri sorumlusunun kullanımındaki veri tabanlarından herhangi bir sızıntı olmaksızın dış kaynaklardan elde ettikleri elektronik posta adresleri/şifreler ile veri sorumlusuna ait internet sitesine giriş yapmaya çalışmaları sonucunda gerçekleştiği belirtilmiştir. Bu yolla 2092 site kullanıcısının hesaplarının şifrelerini doğruladıklarının tespit edildiği, ihlalden etkilenen kişisel verilerin müşterilere ait ad, soyad, cep telefonu numarası, e-posta adresi, cinsiyet, doğum günü, teslimat/fatura adresleri ve sipariş geçmişi bilgileri olduğu ifadelerine yer verilmiştir.

**VERİ SORUMLUSU:
KİŞİSEL BAKIM SEKTÖRÜNDE
FAALİYET GÖSTEREN ŞİRKET**

**KARAR TARİH: 22/05/2020
KARAR SAYI : 2020/421**

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

**UYGULANAN YAPTIRIM :
210.000-TL İPC**

Kişisel Verileri Koruma Kurulunun 22/05/2020 tarih ve 2020/421 sayılı Kararı ile;

Veri sorumlusunun kendi olağan trafiğine ek bu trafiğin veri sorumlusunca fark edilmediği ve ihlali gerçekleştiren kimliği belirsiz kişilerce gönderilen e-posta sonucunda ihlalin tespit edilebildiği gözetilerek, veri sorumlusunun sistemin hem içeriden hem de dışarıdan gelen saldırılar ve siber suçlara veya kötü amaçlı yazılımlara maruz kaldığı, çeşitli belirtilere rağmen bu durumun uzun süre fark edilmediği ve müdahale için geç kalındığı değerlendirilmiş; hesabına giriş yapılan 2092 kullanıcı dışında başarısız denemelerin sayısının fazlalığının veri sorumlusu tarafından fark edilememesinin bilişim ağlarının izlenmesi ve olmaması gereken durumların fark edilmesi hususunda teknik bir eksiklik olduğu tespit edilmiştir.

Veri güvenliğini sağlamaya yönelik gerekli teknik ve idari tedbirleri almadığı gerekçesiyle veri sorumlusu hakkında **210.000 TL idari para cezası** uygulanmasına karar verilmiştir.

“İLAÇ SEKTÖRÜNDE FAALİYET YÜRÜTEN BİR VERİ SORUMLUSUNUN VERİ İHLALİ BİLDİRİMİ HAKKINDA” KİŞİSEL VERİLERİ KORUMA KURULUNUN 16/06/2020 TARİH VE 2020/463 SAYILI KARAR ÖZETİ



**VERİ SORUMLUSU:
İLAÇ SEKTÖRÜNDE FAALİYET
GÖSTEREN BİR ŞİRKET**

**KARAR TARİHİ: 16/06/2020
KARAR SAYI : 2020/463**

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

**UYGULANAN YAPTIRIM :
125.000-TL İPC**

Veri sorumlusunun Kuruma intikal eden veri ihlali bildiriminde; ihlalin veri sorumlusu şirketin sistemlerine karşı gerçekleştirilen fide yazılımından kaynaklı bir siber saldırı sonucunda, yetkili kullanıcı şifresi ele geçirilerek sistemlere erişimin engellenmesi şeklinde gerçekleştiği ve saldırının çalışanların sistemlere erişememesi sonucu tespit edildiği belirtilmiştir. Saldırının veri sorumlusunun siber güvenlik desteği almakta olduğu firmaya ait IP adresi üzerinden ve aynı zamanda veri sorumlusunun eski çalışanı da olan firma çalışanı tarafından gerçekleştirildiği tespit edilmiş ve şüpheliler aleyhine İstanbul Cumhuriyet Başsavcılığına şikâyette bulunulduğu ifade edilmiştir.



Veri sorumlusunun faaliyetlerini sürdürmesi için gerekli verilerinin ve yedek dosyalarının depolandığı Data Domain Sunucusu verilerinin silindiği, ihlalden etkilenen yaklaşık 1000 kişi olduğunun tahmin edildiği, bunlardan 297 kişinin şirket çalışanı olduğu, diğerlerinin ise tedarikçi, müşteri ve taşeronlar olduğu ve ihlalden özel nitelikli kişisel verilerinde etkilenmiş olabileceği Kuruma bildirilmiştir.

Kişisel Verileri Koruma Kurulunun 16/06/2020 tarih ve 2020/463 sayılı Kararı ile;

Saldırının şirket çalışanlarının sistemlere erişememesi sonucu tespit edildiği ve özel nitelikli kişisel veriler üzerinde çalışan çok uluslu bir şirketin, bu tip saldırılar için sızma testleri ve risk analizleri yapıp tehditleri belirlemesi ve güvenlik açıklarını kapatması ve log kaydı takibi ile veri güvenliğini sağlayacak önlemler alması gerektiği belirtilerek bu durumun Kişisel Veri Güvenliği Rehberi 3.2. maddesi “Kişisel Veri Güvenliğinin Takibi” başlığına aykırılık teşkil ettiği kanaatine varılmıştır. Ayrıca, veri sorumlusunun sunucularının yedek dosyalarının depolandığı Data Domain sunucusunda yer alan verilerinin de silinmesinin, Kişisel Veri Güvenliği Rehberi 3.6. maddesinde; “Kişisel Verilerin Yedeklenmesi” başlığı altında düzenlenen “yedeklenen kişisel veriler sadece sistem yöneticisi tarafından erişilebilir olmalı, veri seti yedekleri mutlaka ağ dışında tutulmalıdır.” ifadesine aykırılık teşkil ettiği tespit edilmiştir.

Veri güvenliğini sağlamaya yönelik gerekli teknik ve idari tedbirleri almadığı gerekçesiyle veri sorumlusu hakkında **125.000 TL idari para cezası** uygulanmasına karar verilmiştir.

“KURUMSAL YAZILIM HİZMETİ SUNAN BİR VERİ SORUMLUSUNUN VERİ İHLALİ BİLDİRİMİ HAKKINDA” KİŞİSEL VERİLERİ KORUMA KURULUNUN 16/06/2020 TARİH VE 2020/465 SAYILI KARAR ÖZETİ



**VERİ SORUMLUSU:
YAZILIM ŞİRKETİ**

**KARAR TARİH: 16/06/2020
KARAR SAYI : 2020/465**

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

**UYGULANAN YAPTIRIM :
125.000-TL İPC**

Veri sorumlusunun Kuruma intikal eden veri ihlali bildiriminde; ihlalin siber suçlularının “parola püskürtme” saldırısı ile veri sorumlusunun bilgi sistemleri iç ağına erişmeleri sonucunda gerçekleştiği belirtilmiştir. İhlal, 6 Mart 2019 tarihinde emniyet birimlerinin siber güvenlik uzmanları tarafından veri sorumlusuna bildirilmiştir. Saldırganların Ekim 2018'den Mart 2019'a kadar altı ayı durumda, Dosya Aktarım Protokolü (FTP) ve Güvenli Dosya Aktarım Protokolü'nü (SFTP) kullanarak verileri dışarı sızdırdığı, veri sorumlusu soruşturma sırasında 6 terabayttan fazla verinin muhtemelen sistemlerinden dışarı sızdığını öğrendiği ve ihalden 22 gerçek kişiye ait kimlik (ad soyad, TCKN), özlük (iş beyanları, müşteri bağlılık belgeleri) ve finans (satış kayıtları, pazarlama materyalleri, bordro) verilerinin etkilendiği ifade edilmiştir.



06.03.2019 tarihinde tespit edilen veri ihlali, 29.04.2020 tarihinde Kuruma bildirildiği ve ihlalden etkilenen 18 çalışanına (7 eski çalışan, 11 halihazırda çalışıyor olan) ihlal sonrası posta yolu ile 29 Nisan 2019 tarihinde bildirim yapıldığı, fakat Türkiye’de ikamet ettikleri düşünülen 4 kişinin ise iletişim bilgileri kendilerinde mevcut olmadığı için bildirim yapamadıkları bilgisi Kuruma verilmiştir.

Kişisel Verileri Koruma Kurulunun 16/06/2020 tarih ve 2020/465 sayılı Kararı ile;

Kurul, veri sorumlusunun veri ihlali, gerçekleşme tarihinden yaklaşık 5 ay sonra tespit ettiği ve bu durumun Kişisel Veri Güvenliği Rehberi’nde yayınlanan güvenlik kontrol ve denetimlerinin zamanında yapılmadığını gösterdiği ifade etmiştir. Buna göre, parola püskürtme saldırıları şeklinde gerçekleşen ihlalin; Kurum tarafından yayınlanan ilgili rehberde düzenlenen Çalışanların Eğitilmesi ve Farkındalık Çalışmaları ilkesine aykırı olarak veri sorumlusunun son kullanıcıları tarafından parola güvenliği farkındalığının tam olarak oluşmamasından kaynaklandığının göstergesi olduğu belirtilmiştir.

Bir paylaşım sürücüsünde bulunan 6 TB’tan fazla verinin çalınması veri sorumlusu tarafından mevcut risk ve tehditlerin belirlenmesi ilkesine uyulmamasından kaynaklanmış olduğu ve bu gibi saldırılara karşı veri kaybı riskini azaltmaya yönelik gerekli idari tedbirlerin alınmadığını belirten Kurul, veri güvenliğini sağlamaya yönelik gerekli teknik ve idari tedbirleri almadığı gerekçesiyle veri sorumlusu hakkında 75.000 TL idari para cezası uygulanmasına karar vermiştir.

Bunun yanı sıra; 06.03.2019 tarihinde tespit edilen veri ihlali, veri sorumlusu tarafından 29.04.2019 tarihinde Kuruma bildirilerek 55 günlük geç bildirimde bulunulması, veri sorumlusunun ihlalden etkilenen ilgili kişilere ihlal tespit edildikten 55 gün sonra bildirim yapmış olması sebepleriyle veri sorumlusu hakkında 50.000 TL ek olmak üzere **toplam 125.000 TL idari para cezası** uygulanmasına karar verilmiştir.

“BİR SİGORTA ŞİRKETİNİN VERİ İHLAL BİLDİRİMİ HAKKINDA” KİŞİSEL VERİLERİ KORUMA KURULUNUN 09/07/2020 TARİH VE 2020/532 SAYILI KARAR ÖZETİ



**VERİ SORUMLUSU:
SİGORTA ŞİRKETİ**

**KARAR TARİH: 09/07/2020
KARAR SAYI : 2020/532**

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

**UYGULANAN YAPTIRIM :
30.000-TL İPC**

Veri sorumlusunun Kuruma intikal eden veri ihlal bildiriminde; ihlalin veri sorumlusunun bilgi sistem destek hizmeti aldığı hizmet sağlayıcısında meydana gelen sistemsel bir hata sonucu Otomatik Katılım Sistemi (OKS) kapsamında kendisine bağlı 61 şirketin müşterisi olan 367 ilgili kişinin kişisel verilerini içeren dosyaların yanlış alıcılara gönderilmesiyle gerçekleştiği bilgisi verilmiştir. İhlalden 367 gerçek kişiye ait kimlik (TCKN, ad soyad, doğum tarihi, SGK numarası), iletişim (telefon numarası, e-posta adresi), özlük (işe başlama tarihi) ve finans (IBAN numarası, katkı payı tutarı) verilerinin etkilendiği, ihlale uğrayanlara gerekli bildirimlerin yapıldığını ifade etmiştir.



Yanlış kişisel veri dosyasının gönderildiği 854 firmaya yapılan bildirim aramaları ve e-posta gönderimleri sonunda: 543 firmanın, verileri sildiklerine dair açık teyit verdiği, irtibat bilgilerindeki sorunlar nedeniyle ulaşılamayan bütün firmalara da ayrıca posta yoluyla yazılı olarak bildirim yapılmış ve yanlış bilgilerin kaydedilmiş ise silindiğine dair teyitlerinin beklendiği beyan ettikleri ifadelerine yer verilmiştir.

Kişisel Verileri Koruma Kurulunun 09/07/2020 tarih ve 2020/531 sayılı Kararı ile;

Veri ihlaline sebep olan sistemsel hatanın 2011 yılından itibaren kullanılmaya başlanan uygulama yazılımından kaynaklanması sebebiyle, Kişisel Veri Güvenliği Rehberi nezdinde düzenlenen Bilgi Teknolojileri Sistemleri Tedariği, Geliştirme ve Bakımı ilkesine aykırı olarak veri sorumlusu tarafından yeni sistemlerin tedariki, geliştirilmesi veya mevcut sistemlerin iyileştirilmesi ile ilgili ihtiyaçlar belirlenirken güvenlik gereksinimleri göz önüne alınması gerekirken,

veri ihlaline sebep olan yazılımdaki sistemsel hatanın veri güvenliğinin sağlanması amacıyla sürekli olarak takibinin gerektiği belirtilmiştir.

İhlale konu olayın gerçekleşme tarihi 01.01.2020 ile tespit tarihi 06.01.2020 arasında 5 günlük bir gecikmenin bulunduğu durumun veri sorumlusunun gerekli kontrol ve denetimleri zamanında yapmadığının göstergesi olduğu değerlendirilerek, ihlale sebep olan hatanın istisnai bir durum olması ve uygulamanın ana fonksiyonları ile doğrudan ilişkili olmamasına karşın sigortacılık işlemi yürüten bir kuruluşun bilgi sistemleri güvenliğinde daha dikkatli olması ve veri ihlaline sebep olan sistemsel hatanın işlem yayına alınmadan evvel düzeltilmesi gerektiği ifade edilmiştir. Veri güvenliğini sağlamaya yönelik gerekli teknik ve idari tedbirleri almadığı gerekçesiyle veri sorumlusu hakkında **30.000 TL idari para cezasının** uygulanmasına karar verilmiştir.

“İTERNETTEN MARKET ALIŞVERİŞ HİZMETİ VEREN VERİ SORUMLUSUNUN VERİ İHLAL BİLDİRİMİ HAKKINDA” KİŞİSEL VERİLERİ KORUMA KURULUNUN 01.10.2020 TARİH VE 2020/763 SAYILI KARAR ÖZETİ



Veri sorumlusunun Kuruma intikal eden veri ihlal bildiriminde; ihlalin 400 kişilik bir alıcı grubuna e-posta gönderimi yapılması sırasında alıcı e-posta adreslerinin gizliliğinin korunması amacıyla tüm alıcıların ilgili toplu e-postanın BCC kısmına eklenmesiyle gerçekleştiği bilgisi verilmiştir. E-postanın konu kısmında e-posta adresi yer alan 43 alıcı bilgisinin, e-posta gönderimi yapılan 400 kişilik alıcı grubu ile paylaşıldığı, ilgili kişilere ihlalin gerçekleşmesini takiben 48 saat içerisinde ilgili kişiler ile doğrudan e-posta adresleri üzerinden iletişime geçilerek 29.09.2020 tarihinde bildirim yapıldığı ifade edilmiştir. İhlalden müşterilere ait e-posta adresi bilgilerinin etkilendiği, e-posta adreslerinin kişinin adı-soyadını da içerebildiği, bu nedenle ihlalden kimlik ve iletişim verilerinin etkilendiği belirtilmiştir.

Kişisel Verileri Koruma Kurulunun 01.10.2020 tarih ve 2020/763 sayılı Kararı ile;

İhlalden az sayıda kişi etkilendiği dikkate alınarak, sadece müşterilere ait e-posta adresleri ve adreslerde kullanılan ad soyad bilgisi ihlalden etkilendiği ve ihlalin olumsuz sonuç doğurma riskinin düşük olduğu ifade edilmiş, hatalı e-posta gönderimi yapılan 400 müşteriden ihlale konu e-postanın imha edilmesinin talep edilmiş olması ve veri sorumlusunun Kuruma bildirim yükümlülüğünü zamanında yerine getirmesi gibi sebepler gözetilerek Kanunun 12 nci maddesi kapsamında yapılacak bir işlem olmadığına Kurul tarafından karar verilmiştir.

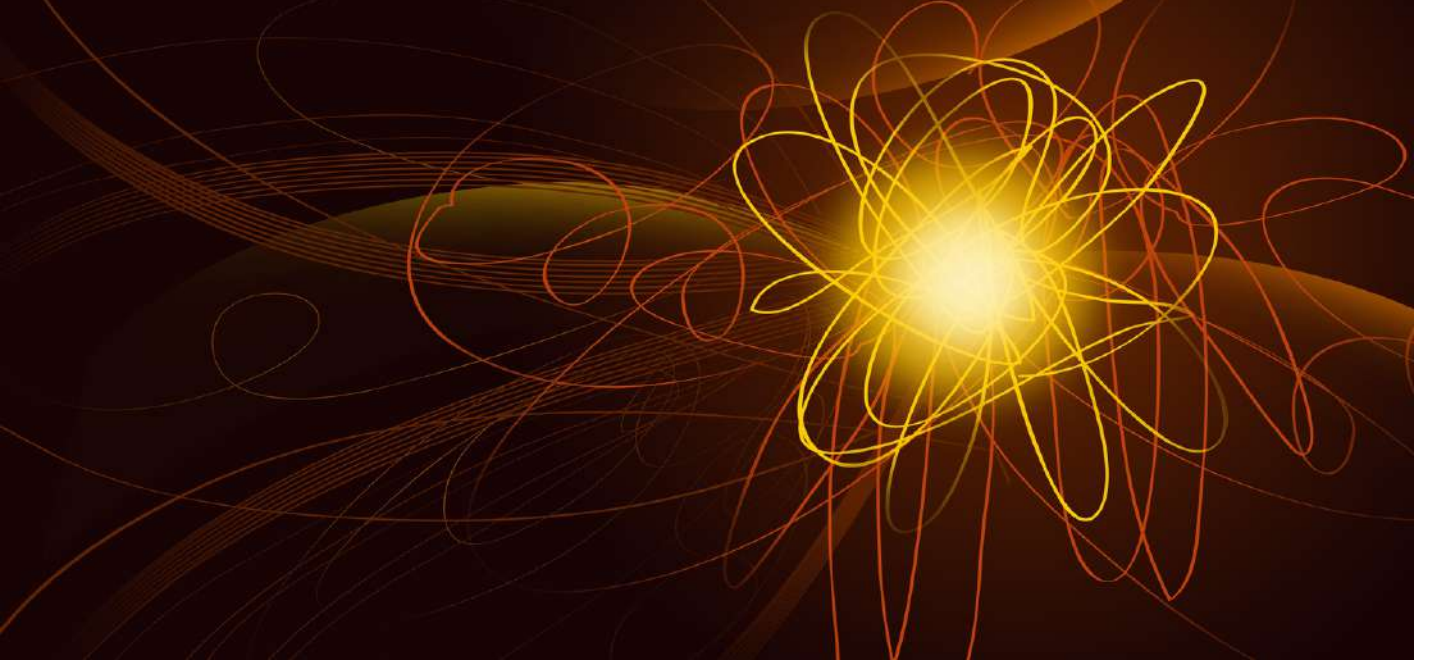
**VERİ SORUMLUSU:
E- TİCARET ŞİRKETİ**

**KARAR TARİHİ: 01/10/2020
KARAR SAYI : 2020/763**

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

**UYGULANAN YAPTIRIM :
YAPILACAK BİR İŞLEM
OLMADIĞINA DAİR KARAR**

“ENERJİ SEKTÖRÜNDE FAALİYET GÖSTEREN VERİ SORUMLUSUNUN VERİ İHLALİ BİLDİRİMİ HAKKINDA” KİŞİSEL VERİLERİ KORUMA KURULUNUN 08/12/2020 TARİH VE 2020/934 SAYILI KARAR ÖZETİ



**VERİ SORUMLUSU:
ENERJİ ŞİRKETİ**

**KARAR TARİH: 08/12/2020
KARAR SAYI. : 2020/934**

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

**UYGULANAN YAPTIRIM:
YAPILACAK BİR İŞLEM
OLMADIĞINA DAİR KARAR**

Veri sorumlusunun Kuruma intikal eden veri ihlali bildiriminde; veri sorumlusunun kurumsal internet sitelerinde yayınlama amacıyla çeşitli tanıtım belgelerinin yer aldığı bir kurum içi arşiv platformuna, yönetim tarafından kendisine verilen yetki kapsamında platform kullanıcılarına eğitim vermek amacıyla erişen bir çalışanın platforma istinaden hazırlanan kullanıcı listesini yetkili üst düzey kullanıcıları tarafından erişim sağlanabilen bir ortak klasörde sakladığı belirtilmiş, kullanıcılardan biri tarafından irtibat listesi ararken kullanıcı listesinde sehven şifre bilgilerinin de bulunduğunu fark etmesi ve durumu raporlaması üzerine veri ihlali gerçekleştiğinin tespit edildiği bildirilmiştir. Söz konusu listede, sehven, kurum içi platformun kullanıcılarının şifrelerinin açık bir şekilde, kullanıcı adı, isim, profesyonel e-posta adresi gibi tanımlayıcılarla birlikte yer aldığı ve ihlalden etkilenen kişi ve kayıt sayısının 2 olduğu ifade edilmiştir.



Kişisel Verileri Koruma Kurulunun 05/05/2020 tarih ve 2020/345 sayılı Kararı ile;

İhlalden Türkiye'den sadece iki kullanıcının etkilenmiş olduğu, ihlale ilişkin dosyanın yalnızca sekiz kullanıcı tarafından erişilmiş olabileceği ve ihlale konu olan verilerin niteliği gereği olumsuz etki doğurma olasılığının düşük olduğu gözetilerek, söz konusu sekiz kullanıcı ile görüşüldüğü ve tamamının gizlilik yükümlüklerini anladığını ve kabul ettiğini ve herhangi bir şifre bilgisini kullanmayacaklarını veya paylaşmayacaklarının teyit edildiği belirtilmiştir.

Veri sorumlusunun ihlalden sonra ilgili platformdaki şifrelerin teknik ve idari tedbirlere uygun olarak maskelenmesinin sağlandığı ve tespit edilen dosyanın ivedilikle ortadan kaldırıldığı gözetilerek, ihlalden etkilenen platform kullanıcılarının şifrelerinin yenilendiği ve ilgili kullanıcılara şifrelerini değiştirmeleri için bir uyarı e-postası gönderildiği tespit edilmiş, bu çerçevede

Kanununun 12. maddesinin (1) numaralı fıkrası kapsamında yapılacak bir işlem bulunmadığına Kurul tarafından karar verilmiştir.

Öte yandan, ihlalin 02.09.2019 ile 16.09.2019 arası gerçekleştiği, 16.09.2019 tarihinde tespit edildiği ve 24.10.2019 tarihinde Kuruma 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 veri sorumlusunun bildirimde bulunmadığı anlaşılmıştır. Bununla birlikte veri sorumlusunun çok uluslu bir yapısı olduğu ve etkilenen ilgili kişilerin bulunduğu ülkelerin tespit edilmesi ve ilgili ülkelerin bildirim yükümlülüklerinin tespit edilmesi ve değerlendirilmesi için gerekli süre göz önüne alındığında makul kabul edilebileceğine bu sebeple Kişisel Verileri Koruma Kurulunun 18.09.2019 tarih ve 2019/271 sayılı Kararına uygun olarak bildirimde bulunması hususunda daha dikkatli olunması yönünde talimatlandırılmasına karar verilmiştir.