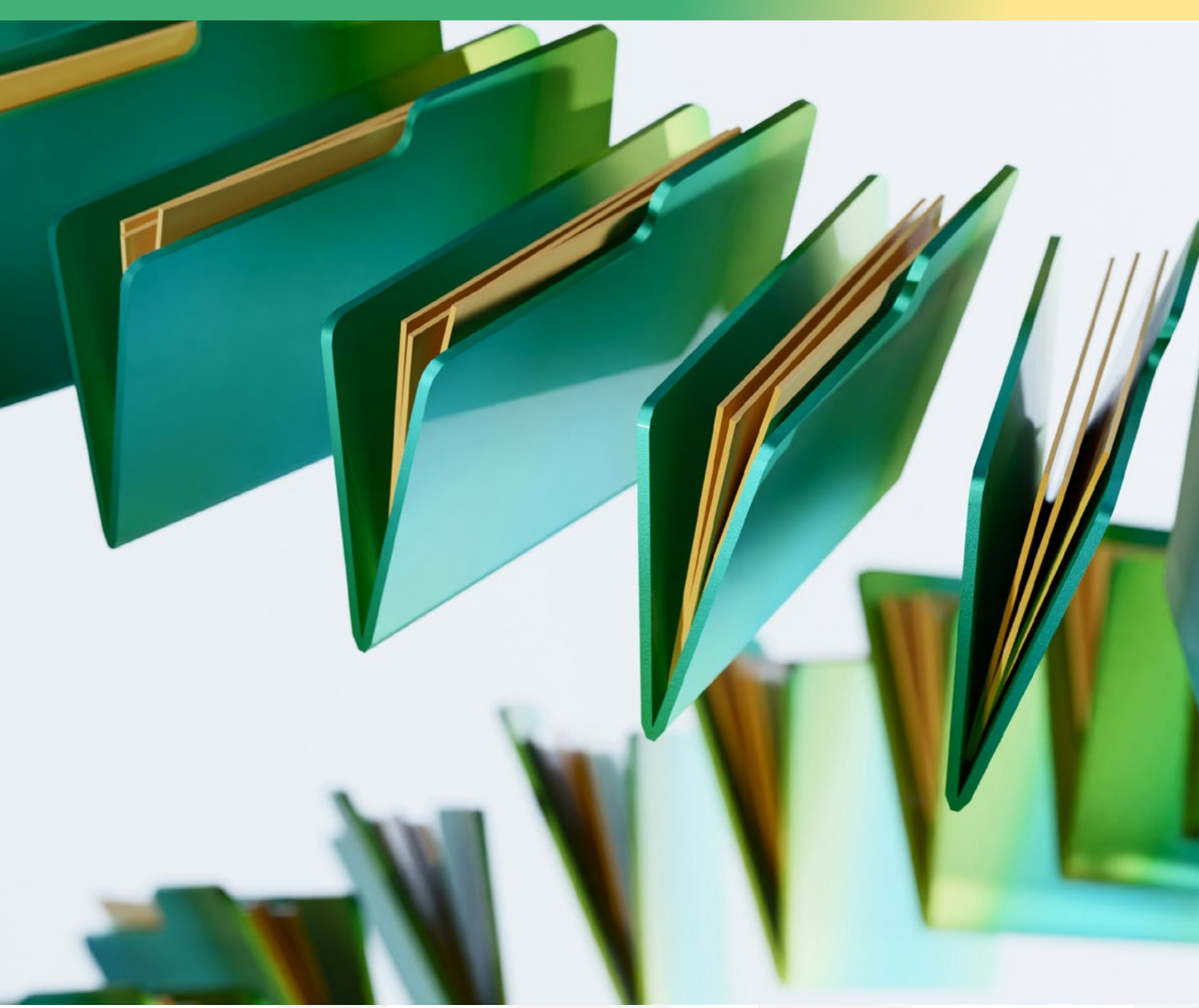

Kişisel Verileri Koruma Kurulu Kararlarında Öne Çıkanlar:

Veri İhlalinden Açık Rızaya 47 Karar Özeti

Av. Sevgi Ünsal Özden
Av. Ozan Akman
Av. Gülnur Çakmak Ergene
Av. Elvan Galatalı
Stj. Av. Yağmur Bayiz
Stj. Av. Tuğçe Polat

ERDEM & ERDEM 40 YEARS

Lejant / İçerik Kılavuzu

Veri İhlalleri

Kişisel verilerin yetkisiz kişilerce ele geçirildiği, erişildiği veya ifşa edildiği olaylara ilişkin kararlar. Kişisel Verileri Koruma Kurulu ("Kurul") bu kararlarda veri sorumlusunun aldığı teknik ve idari tedbirlerin yeterliliğini ve ihlalin bildirim sürecini değerlendirmektedir.

Fidye ve Zararlı Yazılım: Fidye yazılımı veya Truva atı gibi zararlı yazılımlar aracılığıyla verilerin şifrelendiği, ele geçirildiği ya da sızdırıldığı olaylar.

Yetkisiz Erişim ve Oltalama: Oltalama e-postaları, ele geçirilen kullanıcı hesapları veya sistemlerdeki güvenlik açıkları üzerinden verilere yetkisiz erişim sağlanan ya da sağlandığı iddia edilen olaylar.

İnsan veya Teknik Hata: Dışarıdan bir saldırı olmaksızın, yanlış alıcıya gönderim, hatalı yapılandırma veya yazılım hatası gibi veri sorumlusunun kendi süreçlerinden kaynaklanan ihlaller.

Uyum ve Haklar

Bir güvenlik olayından bağımsız olarak, kişisel verilerin hangi hukuki sebebe dayanılarak ve nasıl işlendiğine, ilgili kişilerin taleplerinin nasıl karşılandığına ilişkin kararlar.

Açık Rıza, Pazarlama ve Ticari Elektronik İleti Gönderimi: Açık rızanın geçerliliği, hizmetin rıza şartına bağlanması, gerekmediği hâlde rıza istenmesi ve izinsiz ticari ileti gönderimine ilişkin kararlar.

İlgili Kişi Başvuruları: Kişilerin verilerine erişim, verilerinin silinmesi ve unutulma hakkı gibi taleplerinin veri sorumlusunca karşılanıp karşılanmadığına ilişkin kararlar.

Gözetim ve Özel Nitelikli Veri: Kamera ve ses kaydıyla izleme ile biyometrik, sağlık ve siyasi görüş gibi özel nitelikli verilerin işlenmesine ilişkin kararlar.

Aydınlatma Yükümlülüğü ve Kişisel Veri İşleme Şartları: Kişilerin veri işleme faaliyeti hakkında bilgilendirilip bilgilendirilmediğine ve işlemenin Kanun'daki hukuki sebeplerden birine dayanıp dayanmadığına ilişkin kararlar.

Etiketler:

Talimat Kararı: Kurul'un veri sorumlusuna verilerin imhası veya işlemenin durdurulması gibi düzeltici işlemler yapması yönünde talimat verdiği kararlar. Bazı kararlarda talimat, idari para cezasıyla birlikte verilmiştir.

İdari Para Cezası: Kurul'un veri sorumlusuna idari para cezası uyguladığı kararlar.

İşlem Yok: Kurul'un yapılacak bir işlem bulunmadığına karar verdiği kararlar.

İlgili Karar	İlgili İçerik
Yurt Dışında Gerçekleşen Fidye Yazılımı Saldırısı Nedeniyle Veri İhlali 28.03.2025 tarihli ve 2025/601 sayılı Kurul Kararı	• Hong Kong merkezli bir otel yönetim şirketinin konaklama rezervasyonu veri tabanlarına yönelik fidye yazılımı saldırısı sonucunda Türkiye'de ikamet eden 909 müşteriye ait ad, iletişim ve ödeme kartı bilgileri dâhil çeşitli kişisel veriler yetkisiz erişime konu oldu. • Kurul, şirketin Türkiye'de herhangi bir tüzel kişiliği, çalışanı veya teknoloji altyapısının bulunmadığını, tüm kişisel verilerin Hong Kong'da işlendiğini ve ilgili kişilerin sunulan hizmetlerden Türkiye'de faydalanmadığını dikkate alarak "etki ilkesi" çerçevesinde şirketin KVKK kapsamında veri ihlali bildirim yükümlülüğünün bulunmadığına ve bu aşamada KVKK kapsamında yapılacak bir işlem olmadığına karar verdi.
Zararlı Yazılım Yoluyla Müşteri Verilerine Yetkisiz Erişim Nedeniyle Veri İhlali 09.01.2025 tarihli ve 2025/88 sayılı Kurul Kararı	• Bir restoran zinciri ve hızlı servis gıda şirketinde çalışan bilgi işlem yöneticisinin bilgisayarına zararlı yazılım aracılığıyla sızan saldırganlar, tarayıcıda kayıtlı kullanıcı adı ve şifreleri ele geçirerek şirket sistemine erişti ve 505.337 müşteriye ait ad-soyad, cinsiyet, e-posta, telefon ve şehir bilgilerini elde etti. • Kurul, veri sorumlusunun yetkisiz erişimi tespit edecek alarm ve izleme mekanizmalarının bulunmamasını, iki faktörlü kimlik doğrulama ile SIEM ve güvenlik duvarı gibi temel güvenlik tedbirlerinin ihlal sonrasında devreye alınmasını ve çalışanlara veri güvenliği konusunda yeterli eğitim verildiğinin gösterilememesini dikkate alarak veri güvenliğine ilişkin teknik ve idari tedbirlerin yetersiz olduğuna karar verdi. • Kurul, gerekli güvenlik tedbirlerinin alınmaması nedeniyle 800.000 TL, ilgili kişilere veri ihlalinin en kısa sürede bildirilmemesi nedeniyle ise 200.000 TL olmak üzere veri sorumlusu hakkında toplam 1.000.000 TL idari para cezası uyguladı.
Yetersiz Teknik Güvenlik Tedbirleri Nedeniyle Fidye Yazılımı Saldırısı 26.12.2024 tarihli ve 2024/2196 sayılı Kurul Kararı	• Plastik ev gereçleri ve temizlik ürünleri üreten bir şirketin sistemlerine yönelik fidye yazılımı saldırısı sonucunda çalışanlara ait maaş, banka hesabı, kimlik ve pasaport bilgileri ile özel nitelikli kişisel veriler dâhil çok sayıda kategoride kişisel veri ihlale konu oldu. Veri sorumlusu, ihlalden etkilenen kişiler ve kişisel veriler konusunda Kurul'a farklı ve çelişkili beyanlarda bulundu. • Kurul, özel nitelikli kişisel veriler için güvenli şifreleme ve kriptografik anahtar kullanımına ancak ihlal sonrasında başlanmasını, gerekli log kayıtlarına ulaşılamamasını, güvenlik açığı testlerinin yetersiz kalmasını ve iki faktörlü kimlik doğrulama ile uygun ağ segmentasyonu gibi temel tedbirlerin ihlal öncesinde yeterli düzeyde uygulanmamasını veri güvenliği bakımından eksiklik olarak değerlendirdi. • Kurul, veri güvenliğini sağlamaya yönelik gerekli teknik ve idari tedbirlerin alınmadığı sonucuna vararak veri sorumlusu hakkında 250.000 TL idari para cezası uyguladı.

İlgili Karar	İlgili İçerik
Yetersiz Sistem Takibi Nedeniyle Fidye Yazılımı Saldırısı 07.11.2024 tarihli ve 2024/1898 sayılı Kurul Kararı	• İlaç ve sağlık ürünleri alanında faaliyet gösteren bir şirketin sipariş yönetim sisteminin bulunduğu sunucusuna yönelik fidye yazılımı saldırısı sonucunda 196 mevcut çalışan, 303 eski çalışan ve 17 müşteri/iş ortağına ait kimlik, iletişim, özlük ve müşteri işlem bilgileri ihlale konu oldu. • Kurul, saldırganların sunucu üzerinde zararlı yazılım indirme, dosya ve kod çalıştırma gibi birden fazla işlem gerçekleştirebildiğini, ilk erişimin nasıl sağlandığının kesin olarak belirlenemediğini, ağ ve sunucu güvenliği ile kullanıcı yetkilendirmesine ilişkin tedbirlerin yetersiz kaldığını ve kişisel veri güvenliğinin takibinde yeterli dikkat ve özenin gösterilmediğini tespit ederek veri sorumlusu hakkında 350.000 TL idari para cezası uyguladı.
Truva Atı Saldırısı Nedeniyle Veri İhlali 09.10.2024 tarihli ve 2024/1718 sayılı Kurul Kararı	• Bir kozmetik ve kişisel bakım şirketinin ağ sunucusuna Truva atı (Trojan) virüsü bulaştırılması sonucunda Türkiye'de yaşayan yabancı kişilere ait 325 adet kimlik belgesi fotokopisi ile 107 marka elçisine ait kimlik ve iletişim bilgileri ihlale konu oldu. • Kurul, veri sorumlusunun ihlal öncesinde kötü amaçlı yazılımları tespit etmeye yönelik EDR çözümlerini ancak ihlal sonrasında devreye aldığını, sızma testi yaptırmadığını ve sistemlerin düzenli takip ve kontrolünün sağlandığını gösteren herhangi bir güvenlik taraması raporu sunamadığını tespit ederek veri sorumlusu hakkında 500.000 TL idari para cezası uyguladı.
Veri Sorumlusu Tarafından Kurum'a İntikal Ettirilen Veri İhlal Bildirimi Kapsamında Lockbit Fidye Yazılımının Türkiye'deki Sunuculara Yayılması Nedeniyle Veri İhlali 06.03.2024 tarihli ve 2024/415 sayılı Kurul Kararı	• Veri sorumlusuna ait verilerin Fransa'daki bir iş ortağı tarafından depolanan ve yönetilen sunuculara yönelik LockBit fidye yazılımı saldırısı, Fransa ile Türkiye arasındaki bağlantı üzerinden veri sorumlusunun Türkiye'de bulunan sekiz sunucusuna da yayıldı. İhlalden çalışan, müşteri ve son kullanıcı olmak üzere toplam 43 kişi ile 100.000'den fazla olabileceği belirtilen kayıt etkilendi; bu kapsamda işlem güvenliği, finans ve pazarlama kategorilerindeki kişisel veriler ihlale konu oldu. • Kurul, ağ bileşenleri arasındaki erişimin yeterli ve uygun şekilde sınırlandırılmaması veya ağın alt ağlara ayrılmaması nedeniyle zararlı yazılımın tüm ağ kaynaklarına yayıldığını değerlendirdi. Ayrıca, ihlal öncesinde sızma testi yaptırılmadığını ve sistemlerin düzenli olarak takip ve kontrol edildiğini gösteren herhangi bir güvenlik taraması raporunun sunulmadığını tespit ederek gerekli teknik ve idari tedbirleri almayan veri sorumlusu hakkında 430.000 TL idari para cezası uyguladı.

İlgili Karar	İlgili İçerik
Yurt Dışındaki Grup Şirketine Yönelik Fidye Yazılımı Saldırısı Sonucunda Çalışan Verilerinin Sızdırılması 06.03.2024 tarihli ve 2024/413 sayılı Kurul Kararı	• Tarım makineleri üretimi ve ticareti alanında faaliyet gösteren veri sorumlusunun bağlı bulunduğu yurt dışındaki grup şirketinin sistemlerine yönelik fidye yazılımı saldırısı ve verilerin karanlık ağa (dark web) sızdırılması sonucunda, veri sorumlusunun 56 çalışanına ait kimlik, iletişim, özlük ve sağlık kategorisindeki veriler ihlale konu oldu. • Kurul, ihlale sebep olan fidye yazılımı saldırısının çok faktörlü doğrulama sistemiyle engellenebilecek bir olay olduğunu ancak veri sorumlusunun çok faktörlü doğrulama ve güvenlik yamaları gibi temel güvenlik tedbirlerini ancak veri ihlali sonrasında uygulamaya aldığını, ağ bileşenleri arasında yeterli erişim sınırlandırması veya ayrıştırma yapılmadığını ve farklı veri sorumlularının ortak bir sunucu sistemi kullanmasının hem teknik hem de idari eksiklik teşkil ettiğini değerlendirerek veri sorumlusu hakkında 150.000 TL idari para cezası uyguladı.
Çalışanın İndirdiği Programla Fidye Yazılımının 797 Sunucuya Yayılması ve 4.885 Kişinin Verilerinin İhlale Konu Olması 23.12.2022 tarihli ve 2022/1375 sayılı Kurul Kararı	• Bir sanayi şirketinin ABD'deki kuruluşunda çalışan bir kişinin internetten indirdiği bir ses dosyası değiştirme programını bilgisayarına kurması sonucunda fidye yazılımı şirket ağına bulaştı. Zararlı yazılım 797 küresel sunucuya yayılarak sunuculardaki bazı dosyaları şifreledi. İhlalden çalışan, müşteri ve tedarikçilerden oluşan 4.885 ilgili kişi etkilendi; ihlale konu kişisel veriler arasında kimlik ve iletişim bilgilerinin yanı sıra IBAN, fotoğraf, pasaport ve kan grubu bilgileri de yer aldı. • Kurul, ihlal öncesindeki sızma testinde tespit edilen acil ve kritik güvenlik açıklarının giderildiğinin veri sorumlusu tarafından ortaya konulamadığını; parola ve erişim güvenliği, güncelleme, ağ segmentasyonu ve çalışan farkındalığı bakımından gerekli tedbirlerin alınmadığını tespit etti. Veri güvenliği tedbirlerinin yetersizliği nedeniyle Kanun'un 12/1'inci maddesine aykırılıktan hareketle Kanun'un 18/1-b) maddesine dayalı olarak 800.000 TL, kişisel veri ihlalinin 20 gün gecikmeli bildirilmesi nedeniyle Kanun'un 12/5'inci maddesine aykırılıktan hareketle Kanun'un 18/1-b) maddesine dayalı olarak 200.000 TL olmak üzere toplam 1.000.000 TL idari para cezası uyguladı.
Hizmet Sağlayıcı Hesabı Üzerinden Gerçekleştirilen Fidye Yazılımı Saldırısında 660 Kişinin Verilerinin Şifrelenmesi ve Sızdırılması 21.07.2022 tarihli ve 2022/711 sayılı Kurul Kararı	• Bir otomotiv güvenlik ve elektronik sistemleri üreticisinin sistemlerine, hizmet sağlayıcısına ait bir kullanıcı hesabı üzerinden sızılarak fidye yazılımı saldırısı gerçekleştirildi; müşteri ve tedarikçi temsilcileri ile mevcut ve eski çalışanlar dâhil 660 kişinin kimlik, iletişim, bordro, izin ve sağlık verileri ihlalden etkilendi ve bazı veriler yayınlandı. • Kurul, saldırı faaliyetlerinin veriler şifrelenene kadar tespit edilemediğini ve hizmet sağlayıcı hesabının güvenliği için gerekli tedbirlerin alınmadığını belirterek veri sorumlusunun bu eksikliklerden müştereken sorumlu olduğunu değerlendirdi ve Kanun'un 12/1'inci maddesine aykırılık gerekçesiyle, Kanun'un 18/1-b) maddesine dayalı olarak 500.000 TL idari para cezası uyguladı.

İlgili Karar	İlgili İçerik
Haber Bülteni Dağıtım Platformuna Yetkisiz Erişim 02.05.2025 tarihli ve 2025/833 sayılı Kurul Kararı	• Kâr amacı gütmeyen bir kuruluşa ait haber bülteni dağıtım platformuna yetkisiz erişim sağlanması sonucunda Türkiye'de ikamet eden 15 kişiye ait ad-soyad ve e-posta adresi bilgileri ihlale konu oldu. Veri sorumlusu, ihlali veri işleyenin bildirimi üzerine öğrenerek platformu geçici olarak kapattı, etkilenen kişileri bilgilendirdi ve çok faktörlü kimlik doğrulamanın etkinleştirilmesi dâhil ek güvenlik önlemleri almaya yönelik çalışmalar yürüttü. • Kurul, ihlalden etkilenen veri ve kişi sayısının sınırlı olduğunu, verilerin dolandırıcılık veya kimlik hırsızlığı gibi kötüye kullanıldığına dair herhangi bir bulgu bulunmadığını ve veri sorumlusunun ihlal sonrasında önlemler aldığını dikkate alarak bu aşamada KVKK kapsamında yapılacak bir işlem bulunmadığına karar verdi.
Pazarlama Hesabına Yetkisiz Erişim Nedeniyle Veri İhlali 07.11.2024 tarihli ve 2024/1899 sayılı Kurul Kararı	• Avrupa'daki grup şirketlerine kurumsal destek hizmetleri sağlayan bir şirketin pazarlama amacıyla kullanılan kullanıcı hesabının ele geçirilmesi sonucunda FTP sunucusunda bulunan ve bazıları "herkese açık" olarak ayarlanmış kara listede bulunan bir IP adresinden yetkisiz erişim sağlandı. İhlalden yaklaşık 70.000 kişiye ait ad-soyad, e-posta, iletişim ve adres bilgileri etkilendi. • Kurul, ihlalin gerçekleşme tarihinin tespit edilemediğini, kişisel veri içeren dosyaların herkese açık bırakıldığını, ihlal öncesinde güçlü parola politikası uygulanmadığını ve yetkisiz erişimlerin uzun süre fark edilmediğini tespit ederek veri sorumlusu hakkında 700.000 TL idari para cezası uyguladı.
Oltalama (Phishing) Saldırısı Ve Bilgi Güvenliği Zafiyetleri Nedeniyle Veri İhlali 10.09.2024 tarihli ve 2024/1523 sayılı Kurul Kararı	• Bir otel işletmesinde çalışan personelin oltalama (phishing) içerikli e-postadaki bağlantıya tıklaması sonucunda bilgisayarı yetkisiz kişilerin kontrolüne geçti ve bilgisayarda bulunan vardiya çizelgesi aracılığıyla 450 çalışana ait kimlik bilgileri ihlale konu oldu. • Kurul, ihlalin tek bir bilgisayarla sınırlı kaldığını tespit etmekle birlikte veri sorumlusunun sistemlerinde güncelleme ve konfigürasyon eksiklikleri bulunduğunu, sistemlerin spam e-postalara karşı yeterince korunmadığını, zayıf parola kullanıldığını ve sunucu odalarına girişte kimlik doğrulama mekanizmasının bulunmadığını tespit ederek veri sorumlusu hakkında 500.000 TL idari para cezası uyguladı.
Aynı Güvenlik Açığının İki Kez Kullanılması Nedeniyle Veri İhlali 08.06.2023 tarihli ve 2023/1017 sayılı Kurul Kararı	• Bir dijital oyun ve eğlence platformunun yaklaşık 69 milyon aktif ve eski kullanıcı hesabını barındıran sisteminde, uygulamadaki güvenlik açığından yararlanan saldırgan aynı açık üzerinden iki kez ihlal gerçekleştirdi. Türkiye'de ikamet eden 90.182 kişiye ait kullanıcı adı, ad, e-posta adresi, doğum tarihi, cinsiyet, ülke ve IP adresi gibi kişisel veriler de ihlalden etkilendi; etkilenen kişiler arasında çocuklar da yer aldı ve saldırgan verileri satışa çıkardı. • Kurul, veri sorumlusunun ihlali kendi güvenlik sistemleri aracılığıyla tespit edemediğini, ihlal öncesinde sızma testi yaptırmadığını ve yama yönetim politikası uygulamadığını, ayrıca aynı güvenlik açığı kullanılarak gerçekleştirilen ikinci ihlali önleyemediğini tespit ederek veri sorumlusu hakkında 1.500.000 TL idari para cezası uyguladı.

İlgili Karar	İlgili İçerik
Mobil Uygulamanın Veri Tabanına Yetkisiz Erişim ve İhlal Bildirimi Yapılmaması 16.05.2024 tarihli ve 2024/790 sayılı Kurul Kararı	• Bir yazılım ve teknoloji şirketinin 7.823 üye kaydı bulunan mobil uygulamasının veri tabanına yetkisiz erişim sağlandı. Veri tabanında ad-soyad, e-posta adresi ve telefon numarası bilgileri bulunurken, uygulamadaki bazı bilgiler değiştirildi ve yetersiz log kayıtları nedeniyle yetkisiz erişimin nasıl gerçekleştiği kesin olarak tespit edilemedi. • Kurul, veri tabanı şifresinin ele geçirilmiş olmasını, ihlal sonrasında parola politikasının değiştirilmesini ve yeterli log kaydı bulunmadığı için yetkisiz erişimin nasıl gerçekleştiğinin tespit edilememesini veri güvenliği bakımından eksiklik olarak değerlendirdi ve veri sorumlusu hakkında 250.000 TL idari para cezası uyguladı. • Veri sorumlusu, kişisel verilerin zarar görmediği ve veri bütünlüğünde değişiklik olmadığı gerekçesiyle ilgili kişilere bildirim yapmadı. Kurul, veri ihlalinin yalnızca verilerin bütünlüğünün bozulmasıyla değil, gizlilik veya erişilebilirliğin ihlaliyle de gerçekleşebileceğini belirterek bildirim yükümlülüğünün ihlali nedeniyle ayrıca 100.000 TL idari para cezası uyguladı.
Oltalama E-Postası Sonucunda Üye Bilgilerinin Saldırgana Gönderilmesi Suretiyle Gerçekleşen Veri İhlali 09.05.2024 tarihli ve 2024/728 sayılı Kurul Kararı	• Finans ve muhasebe alanında faaliyet gösteren uluslararası bir meslek kuruluşunun çalışanı, kuruluşun başkanı ve CEO'sundan gönderilmiş gibi görünen bir oltalama e-postasını gerçek zanneden çalışan, 217 Türk üyeye ait ad-soyad, üyelik numarası ve bazı üyelerin e-posta adreslerini saldırgana göndererek veri ihlaline neden oldu. • Kurul, veri sorumlusunun ihlal öncesinde oltalama saldırılarından kaynaklanabilecek riskleri yeterince gözetmediği ve gelen e-posta adreslerinin kontrolünü sağlayan güvenlik sistemini yeterince sıkı yapılandırmadığını değerlendirdi. Ayrıca çalışanlara eğitim verilmiş olmasına rağmen, şüpheli e-postanın doğruluğunun teyit edilmeden kişisel verilerin paylaşılmasının, veri güvenliği farkındalığının çalışanlar nezdinde yeterince benimsenmediğinin göstergesi olarak kabul etti. Bu nedenle, veri güvenliğine ilişkin gerekli teknik ve idari tedbirlerin alınmaması nedeniyle 750.000 TL; ihlalin öğrenilmesinden itibaren 72 saat içinde Kurul'a bildirilmemesi nedeniyle 250.000 TL olmak üzere veri sorumlusu hakkında toplam 1.000.000 TL idari para cezası uyguladı.

İlgili Karar	İlgili İçerik
Veri Tabanına Yönelik Siber Saldırı Sonucunda Kullanıcı Verilerinin Silinmesi ve Ele Geçirilmesi 25.01.2024 tarihli ve 2024/133 sayılı Kurul Kararı	• Bir online yemek siparişi, restoran entegrasyonu ve teslimat/kurye hizmetleri sağlayıcısının veri tabanı sistemine gerçekleştirilen siber saldırı sonucunda veri tabanındaki veriler saldırganlar tarafından silindi ve ele geçirildi. 1.362 kullanıcıya ait kimlik (ad-soyad), iletişim (telefon, adres ve e-posta bilgileri) kategorisindeki kişisel veriler ihlale konu oldu ve ele geçirilen kişisel verilere ilişkin saldırganlar tarafından fidye talep edildi. • Kurul, yönetim paneli şifresinin tarayıcıya kaydedilmesinin veri sorumlusunun parola güvenliği konusunda gerekli dikkat ve özeni gösterilmediğini; veri tabanı yönetim yazılımında IP adresi erişiminin sınırlandırılmamasının ise yetkisiz erişime sebebiyet verdiğini ve bu konuda gerekli tedbirlerin alınmadığını gösterdiğini değerlendirdi. Bu doğrultuda, Kanun'un 12/1'inci maddesine dayalı olarak veri güvenliğinin tesisi için gerekli teknik ve idari tedbirleri almayan veri sorumlusu hakkında Kanun'un 18/1-b) maddesine dayalı olarak 250.000 TL idari para cezası uyguladı.
Bir Hosting Firmasının Kullandığı Satış ve Muhasebe Yazılımındaki Müşteri Yönetim Panelinde Bulunan Güvenlik Açığı Nedeniyle 31.179 İlgili Kişiye Ait Verilerin Almanya Merkezli Bir IP Adresine Aktarılması ve Karanlık Ağda Yayımlanması 21.03.2023 tarihli ve 2023/412 sayılı Kurul Kararı	• Bir hosting firmasının satış ve muhasebe yazılımındaki müşteri yönetim panelinde bulunan güvenlik açığından yararlanılması sonucunda ana sunucudaki veriler toplu şekilde Almanya'da bulunan bir IP adresine aktarıldı ve karanlık ağda (dark web) yayımlandı. Yaklaşık altı ay sonra tespit edilen ihlalden 31.179 müşteri, kullanıcı ve çalışan etkilendi; kimlik, iletişim, müşteri işlem ve finans kategorisindeki kişisel veriler ile bazı şifreleri içeren e-posta içerikleri, alan adı kayıt belgeleri ve kredi kartı bilgileri ihlale konu oldu. • Kurul, veri sorumlusunun ihlal öncesinde saldırı tespit ve önleme sistemi ile toplu veri indirmesini engelleyecek bir çözüm kullanmadığını; iki faktörlü kimlik doğrulama ve güçlü parola politikası uygulamadığını tespit etti. Ayrıca log kayıtlarında yer alan kredi kartı bilgilerinin maskelenmemesi ve gerekli olmayan verilerin kaydedilmesi nedeniyle veri maskeleme tedbirinin alınmadığını ve veri minimizasyonu ilkesinin gözetilmediğini değerlendirdi. Bu doğrultuda, veri güvenliğini sağlamaya yönelik gerekli teknik ve idari tedbirleri almayan veri sorumlusu hakkında 350.000 TL idari para cezası uyguladı.

İlgili Karar	İlgili İçerik
Müşteri İletişim Bilgilerinin Ele Geçirilerek Dolandırıcılık Amacıyla Kullanılması 28.12.2022 tarihli ve 2022/1407 sayılı Kurul Kararı	• Kimliği belirsiz kişiler, bir moda tekstil firmasının müşterilerine ait telefon numaralarını hukuka aykırı olarak ele geçirerek, teslim alınmayan kargolar nedeniyle icra takibi başlatılacağı iddiasıyla para transferi talep etti; olay, bir müşterinin veri sorumlusuna bildirimde bulunması üzerine tespit edildi. • Kurul, kişisel verilerin veri sorumlusunun sistemlerinden sızdığının tespit edilemediğini ve söz konusu verilerin e-ticaret platformları, kargo şirketleri veya finans kuruluşları gibi diğer veri sorumlularının sistemlerinden elde edilmiş olabileceğini değerlendirdi. Ayrıca, veri sorumlusunun sızma testi, ERP sistemine üç katmanlı kimlik doğrulamasıyla erişim, veri ihlali müdahale planı, gizlilik taahhütleri ve veri güvenliğinin tesisine ilişkin sözleşmeler dahil olmak üzere, işlenen kişisel verilerin niteliğiyle orantılı makul teknik ve idari tedbirleri aldığını değerlendirdi. Kurul, veri sorumlusunun ihlali öğrendiği gün internet sitesi ve sosyal medya hesaplarından duyuru yapmasını da gözeterek Kanun kapsamında yapılacak bir işlem bulunmadığına karar verdi.
Bir Teknoloji Şirketi Olan Veri Sorumlusu Tarafından Kurula İletilen Veri İhlal Bildirimi Kapsamında Kişisel Verilere Yetkisiz Şekilde Erişildiğine İlişkin Tehdit E-Postası Üzerine Yürütülen İnceleme 07.10.2022 tarihli ve 2022/1087 sayılı Kurul Kararı	• Kimliği belirsiz kişiler, bir teknoloji şirketine gönderdikleri e-postada şirketin veri tabanlarına eriştiklerini ve bazı bilgileri ele geçirdiklerini ileri sürerek şirketi tehdit etti. Bunun üzerine veri sorumlusu, iki bağımsız güvenlik firmasına sistemleri üzerinde ayrıntılı analiz ve sızma testleri yaptırdı. İncelemelerde herhangi bir kişisel veri ihlaline ilişkin bulguya rastlanmazken e-postada örnek olarak sunulan verilerin de şirket sistemlerinde tutulan kişisel verilerle eşleşmediği tespit edildi. • Kurul, bağımsız şirketlerce hazırlanan adli bilişim ve sızma testi raporlarında kişisel veri ihlaline yönelik herhangi bir bulgu tespit edilemediğini dikkate alarak bu aşamada Kanun kapsamında yapılacak bir işlem bulunmadığına karar verdi.
Üst Düzey Yöneticinin E-Posta Hesabının Ele Geçirilerek Müşterilere Zararlı İçerik Gönderilmesi 21.07.2022 tarihli ve 2022/714 sayılı Kurul Kararı	• Bir tarımsal emtia şirketinin üst düzey yöneticisine ait e-posta hesabı ele geçirildi; saldırganlar hesap üzerinden yaklaşık 1.000 kişiye, zararlı bir siteye yönlendiren sahte fatura görünümlü e-postalar gönderdi. Bazı müşterilerin oltalama saldırısına maruz kaldığı değerlendirilen ihlal, 2-3 gün sonra bir müşterinin uyarısıyla fark edildi. • Kurul, ihlalden etkilenen kişi sayısının belirlenememesini veri sorumlusunun kişisel veriler üzerindeki kontrolü sağlayamadığının bir göstergesi olarak değerlendirdi. Veri kaybı önleme yazılımı, gelişmiş kimlik doğrulama ve saldırı veya anormallikleri tespit edecek sistemlerin ihlal öncesinde kullanılmadığını; erişim ve log kayıtlarının düzenli olarak izlenmemesi nedeniyle ihlalin veri sorumlusu tarafından tespit edilemediğini belirtti. Ayrıca Kurul, parola yönetim politikasının aynı parolanın farklı platformlarda kullanılmasını önleyecek şekilde düzenlenmediğini ve etkin biçimde uygulanmadığını tespit etti. Bu nedenlerle, veri güvenliğinin tesisi için gerekli teknik ve idari tedbirleri almayan veri sorumlusu hakkında Kanun'un 12/1'inci maddesine aykırılık sebebiyle 200.000 TL idari para cezası uyguladı.

İlgili Karar	İlgili İçerik
Çalışan Verilerinin Yanlışlıkla Üçüncü Taraf Uygulamayla Paylaşılması 22.05.2025 tarihli ve 2025/881 sayılı Kurul Kararı	• Bir şirket çalışanının, iş seyahati harcamalarının takibinde kullanılan uygulamada sehven farklı bir uygulamanın entegrasyonunu etkinleştirmesi sonucunda 488 çalışana ait ad-soyad, iş e-posta adresi ve iş telefonu bilgileri üçüncü taraf bir uygulama şirketiyle paylaşıldı. Veri sorumlusu, ihlali tespit etmesinin ardından senkronizasyonu derhal iptal etti ve paylaşılan verilerin silinmesini talep etti. • Kurul, ilgili çalışanlara son bir yıl içinde kişisel verilerin korunması eğitimi verildiğini, ihlal sonrasında hızlı şekilde önlem alındığını ve ihlalin ilgili kişiler üzerinde olumsuz sonuç doğurma olasılığının düşük olduğunu dikkate alarak bu aşamada KVKK kapsamında yapılacak bir işlem bulunmadığına karar verdi.
Müşteri E-Posta Adreslerinin Diğer Alıcılara Görünür Şekilde Gönderilmesi 12.03.2025 tarihli ve 2025/536 sayılı Kurul Kararı	• Bir küçük ev aletleri şirketi tarafından müşterilere gönderilen 14 bilgilendirme e-postasında alıcıların e-posta adreslerinin gizlenmemesi sonucunda müşteriler birbirlerinin e-posta adreslerini gördü. İhlalden tahmini 500 müşteri etkilendi ve veri sorumlusu durumu fark etmesinin ardından e-postaları geri çekmek için işlem başlattı. • Kurul, ihlalin fark edilmesinin ardından e-postaların geri çekildiğini, ihlalden yalnızca e-posta adreslerinin etkilendiğini ve ilgili kişiler üzerinde olumsuz sonuç doğma ihtimalinin düşük olduğunu dikkate alarak bu aşamada KVKK kapsamında yapılacak bir işlem bulunmadığına karar verdi.
Hazır Giyim Ve Tekstil Ürünlerinin Perakende Satışını Gerçekleştiren Veri Sorumlusunun Paketleme Hatası Nedeniyle Müşteri Bilgilerinin Üçüncü Kişiye Gönderilmesi 09.05.2024 tarihli ve 2024/756 sayılı Kurul Kararı	• Bir hazır giyim şirketinin deposunda paketleme personelinin yaptığı hata sonucunda bir müşteriye ait kargo ve fatura başka bir müşteriye teslim edildi. İhlalden etkilenen kişisel veriler kimlik (ad soyad), iletişim (adres, cep telefonu numarası, e-posta adresi) ve müşteri işlem (sipariş bilgileri) bilgilerinden oluşurken ihlalden yalnızca bir müşteri etkilendi. • Kurul, ilgili kişiye ihlal bildiriminde bulunulduğunu ve ihlalin ilgili kişi üzerinde olumsuz sonuç doğurma riskinin düşük olduğunu dikkate alarak bu aşamada Kanun kapsamında yapılacak bir işlem bulunmadığına karar verdi.

İlgili Karar	İlgili İçerik
İnsan Kaynakları Uygulamasındaki Menü Karışıklığı Nedeniyle Çalışan Verilerinin Toplu Gönderilmesi 28.09.2023 tarihli ve 2023/1675 sayılı Kurul Kararı	• Bir endüstriyel mutfak ekipmanları üreticisinin insan kaynakları çalışanının, adres güncelleme bildirimi sırasında bireysel gönderim menüsü yerine toplu gönderim menüsünü seçmesi sonucunda 1.522 çalışana ait ad-soyad, T.C. kimlik numarası ve adres bilgileri 1.589 çalışana gönderildi. İhlal, veri sorumlusu nezdindeki çalışanların geri bildirimleri üzerine aynı gün tespit edildi. • Kurul, benzer tasarıma sahip menüler nedeniyle söz konusu insan hatasının hayatın olağan akışı içinde anlaşılabilir olduğunu, bilgi güvenliğinin en zayıf halkasının insan faktörü olduğunu, veri sorumlusunun çalışanlarına bilgi güvenliği konularında yeterli eğitim verdiğini, gizlilik taahhütleri ve disiplin düzenlemeleri oluşturduğunu ve kişisel verilerin güvenliği için uygun düzeyde teknik tedbirler aldığını, ayrıca ihlalin personel geri bildirimi üzerine aynı gün tespit edildiğini dikkate alarak bu aşamada Kanun kapsamında yapılacak bir işlem bulunmadığına karar verdi.
Mobil Uygulamadaki Teknik Hata Nedeniyle Müşterilerin Birbirinin Profil Bilgilerini Görüntülemesi 21.07.2022 tarihli ve 2022/707 sayılı Kurul Kararı	• Veri sorumlusu sıfatını haiz bir mağazacılık firmasının mobil e-ticaret uygulamasındaki teknik hata nedeniyle bazı müşteriler, başka müşterilere ait ad-soyad, telefon, e-posta ve maskeli kredi kartı bilgilerini görüntüleyebildi; ihlal bir müşterinin bildirimi üzerine tespit edilerek kısa sürede giderildi. • Kurul, ihlale konu kişisel verilerin kamuoyuna ifşa olmadığını ve kötüye kullanılma ihtimalinin düşük olduğunu, ihlalden etkilenen kesin kişi sayısının 17 olduğunu ve en fazla 136 kişinin etkilenmiş olabileceğini, kişi başına görüntülenebilecek veri miktarı ile verilerin kötüye kullanılma ihtimalinin düşük olduğunu değerlendirdi. Ayrıca, veri sorumlusunun müşteri bildiriminden önce sistemdeki sorunun kaynağını araştırmaya başladığını, ihlalin anlaşılması üzerine sistemi kısa sürede kapatarak teknik hatayı giderdiğini ve ilgili kişilere bildirimde bulunduğunu dikkate alarak Kanun'un 12/1'inci maddesi kapsamında bu aşamada yapılacak bir işlem bulunmadığına karar verdi.
Giyim Mağazasının İnternet Sitesindeki Teknik Hata Nedeniyle Müşteri Verilerinin Erişime Açılması 19.10.2023 tarihli ve 2023/1796 sayılı Kurul Kararı	• Bir giyim mağazasının internet sitesinde, hizmet alınan veri işleyenin sunduğu CDN hizmeti kapsamındaki önbellek (cache) yapılandırmasından kaynaklanan teknik sorun nedeniyle bir müşteriye ait ad-soyad, üyelik ve telefon numarası bilgileri sınırsız bir kitlenin erişimine açık hale geldi. İlgili kişi, üçüncü kişiler tarafından aranması ve kendisine ait olmayan bir siparişe ilişkin mesaj alması üzerine hesabını kontrol ettiğinde, başka bir kişinin üyelik bilgileriyle sisteme giriş yapıldığını, adres bilgisini değiştirdiğini ve sipariş verdiğini tespit etti. • Kurul, teknik sorunun hizmet alınan veri işleyenden kaynaklanmasının veri sorumlusunun yükümlülüklerini ortadan kaldırmadığını ve veri güvenliğine yönelik gerekli teknik ve idari tedbirlerin alınması bakımından veri sorumlusu ile veri işleyenin müştereken sorumlu olduğunu belirtti. Değişiklik canlıya alınmadan önce gerekli detaylı testlerin yapılmadığını ve güncellemenin kontrol edilmediğini tespit ederek veri sorumlusu hakkında 200.000 TL idari para cezası uygulanmasına karar verdi.

İlgili Karar	İlgili İçerik
Reklam Ve Pazarlama Amacıyla İzinsiz SMS Gönderilmesi ve Arama Yapılması 10.06.2026 tarihli ve 2026/1183 sayılı Kurul Kararı	• Bir tasarruf finansman şirketi, marka elçiliği programı kapsamında müşterilerinden temin ettiği üçüncü kişilere ait telefon numaralarını kaydederek, ilgili kişileri önceden aydınlatmaksızın ve geçerli bir açık rıza temin etmeden reklam ve pazarlama amacıyla SMS gönderdi ve sesli arama gerçekleştirdi. • Kurul, ilgili kişinin telefon görüşmesi sırasında kampanya tanıtımına ilgi göstermesinin ve konuşmaya devam etmesinin geçerli bir açık rıza teşkil etmediğini ve kişisel verilerin açık rıza alınmadan önce işlenmeye başlandığını tespit ederek veri sorumlusu hakkında 1.000.000 TL idari para cezası uyguladı.
Uçak İçi İnternet Hizmetinin Açık Rıza Şartına Bağlanması 15.08.2024 tarihli ve 2024/1393 sayılı Kurul Kararı	• Uçuş sırasında sunulan internet hizmetinden yararlanmak isteyen yolcuların soyadı ile koltuk veya bilet numarası bilgileri internet servis sağlayıcısının portalı üzerinden alınarak havayolu şirketi sistemleri üzerinden doğrulandı. İnternet servis sağlayıcı, bu veri paylaşımı için yolculardan ayrıca açık rıza talep etti. • Kurul, söz konusu doğrulama işlemini kişisel veri aktarımı olarak değerlendirdi ve havayolu şirketi ile internet servis sağlayıcının bu süreç bakımından ayrı veri sorumluları olduğuna karar verdi. • Kurul, söz konusu veri işleme faaliyetinin sözleşmenin kurulması veya ifasıyla doğrudan ilgili ve gerekli olması, veri sorumlusunun hukuki yükümlülüğünü yerine getirmesi ve bir hakkın tesisi, kullanılması veya korunması için zorunlu olması şartlarına dayanabileceğini; dolayısıyla bu işlem için ayrıca açık rıza alınmasına gerek bulunmadığını tespit etti. • Buna rağmen internet servis sağlayıcının ilgili kişilerden ayrıca açık rıza talep etmesi, yanıltıcı ve yanlış yönlendirici bulunarak hukuka ve dürüstlük kurallarına uygun olma ilkesine aykırı kabul edildi. Kurul bu nedenle internet servis sağlayıcı hakkında 90.000 TL idari para cezası uygulanmasına karar verdi.

İlgili Karar	İlgili İçerik
Güvenlik Kamerası, Çerezler ve Reklam ve Pazarlama Amaçlı Açık Rıza Uygulamaları 08.08.2024 tarihli ve 2024/1361 sayılı Kurul Kararı	• Bir özel eğitim kurumunun güvenlik kamerası, internet sitesi çerezleri ve iletişim formundaki reklam ve pazarlama amaçlı açık rıza uygulamaları Kurul tarafından incelendi. • Kurul, güvenlik kameralarıyla ses kaydı alındığının kanıtlanamadığını ve görüntü kaydının hukuki yükümlülük kapsamında gerçekleştirildiğini belirterek bu konuda işlem yapılmasına gerek olmadığına karar verdi. • İnternet sitesinde kullanılan zorunlu olmayan analitik çerezlerin, KVKK'ya aykırı olarak kullanıcıların açık rızası alınmadan çalıştırıldığı tespit edildi. • Kurul, yalnızca kurumdan bilgi almak isteyen kişilerin iletişim bilgilerinin reklam, promosyon ve kampanya amaçlarıyla kullanılmasına ilişkin rızanın aynı seçenek altında alınmasını hukuka aykırı buldu. Bilgi alma hizmetinin reklam ve pazarlama amaçlı açık rıza şartına bağlanmasının, rızanın "belirli bir konuya ilişkin olma" ve "özgür iradeyle açıklanma" şartlarını karşılamadığına karar verdi. • Kurul ayrıca yeterli aydınlatma yapılmadığını tespit ederek veri sorumlusu hakkında hukuka aykırı veri işleme nedeniyle 250.000 TL ve aydınlatma yükümlülüğünün ihlali nedeniyle 15.000 TL olmak üzere toplam 265.000 TL idari para cezası uyguladı.
Sık Aralıklarla Pazarlama Ve Bilgilendirme SMS'i Gönderilmesi 08.08.2024 tarihli ve 2024/1350 sayılı Kurul Kararı	• Bir elektronik haberleşme işletmecisi, sözleşme süresi sona erecek bir abonesine 08.05.2023 ile 26.07.2023 tarihleri arasında aynı veya benzer içerikte 20'den fazla SMS gönderdi. İlgili kişi, kampanya ve tekliflerle ilgilenmediğini çağrı merkezi görüşmelerinde belirtmesine rağmen SMS gönderimi devam etti. • Kurul, kampanya bitişi ve uygulanacak tarife hakkına bilgilendirme yapılmasının veri sorumlusunun hukuki yükümlülüğü kapsamında olduğunu; ancak aynı içerikteki SMS'lerin kısa aralıklarla ve çok sayıda gönderilmesinin ilgili kişinin makul beklentisini aştığını ve hakkın kötüye kullanılması niteliğinde olduğunu değerlendirerek veri sorumlusu hakkında 100.000 TL idari para cezası uyguladı. • Kurul ayrıca, kişisel verilerin işlenmesine ilişkin açık rıza metninin sözleşme içerisinde yer almasının ilgili kişiler açısından yanıltıcı olabileceğini ve açık rızanın unsurlarını sakatlayabileceğini belirterek açık rıza metninin sözleşmeden ayrı olarak sunulmasının uygun olacağını veri sorumlusuna hatırlattı.

İlgili Karar	İlgili İçerik
Abonelik Sözleşmesinde Gereksiz Açık Rıza Alınması 22.02.2024 tarihli ve 2024/282 sayılı Kurul Kararı	• Bir telekomünikasyon şirketi, adres değişikliği sonrasında internet altyapısının değişmesi nedeniyle yeni abonelik sözleşmesi kurulması kapsamında ilgili kişiden yeniden kimlik belgesi talep etti. İlgili kişinin gerekli belgeleri sunmaması üzerine internet hizmeti sonlandırıldı. • Kurul, yeni sözleşmenin kurulması için kimlik bilgilerinin talep edilmesini sözleşmenin kurulması ve veri sorumlusunun hukuki yükümlülüğünü yerine getirmesi kapsamında hukuka uygun buldu. Kimlik bilgilerinin işlenmesini gerektiren sebepler devam ettiği için bu verilerin silinmesi talebi de kabul edilmedi. • Buna karşılık Kurul, kişisel verilerin aktarımı bakımından açık rıza dışında geçerli bir veri işleme şartı bulunduğu halde abonelik sözleşmesinde ayrıca açık rıza alınmasını ilgili kişileri yanıltıcı ve yanlış yönlendirici bularak hukuka ve dürüstlük kurallarına aykırı olduğuna karar verdi ve veri sorumlusu hakkında 350.000 TL idari para cezası uyguladı. • Kurul ayrıca, sözleşmedeki açık rıza niteliğindeki hükümlerin kaldırılması, açık rızanın gerektiği hallerde sözleşme ve aydınlatma metninden ayrı olarak alınması ve kişisel verilerin aktarıldığı grup şirketleri listesinin ilgili kişiyle paylaşılması yönünde veri sorumlusunu talimatlandırdı.
Canlı Maç Yayını Hizmetinin Ticari İleti Onayı Ön Şartına Bağlanması 21.09.2023 tarihli ve 2023/1610 sayılı Kurul Kararı	• Bir çevrimiçi yasal spor ve şans oyunları platformu, canlı maç yayını hizmetinden yararlanmayı ticari elektronik ileti onayı verilmesi şartına bağladı; diğer koşulları sağlayan ancak bu onayı vermeyen bir kullanıcı hizmetten yararlanamadığı gerekçesiyle Kurul'a şikâyette bulundu. • Kurul, canlı yayın hizmetinin ticari ileti onayına bağlanmasının açık rızanın "özgür iradeyle verilmesi" unsurunu zedelediğini ve gerçekleştirilen veri işleme faaliyetinin Kanun'daki herhangi bir işleme şartına dayanmadığını değerlendirdi. Bu kapsamda, hukuka aykırı veri işlemeyi önlemeye yönelik gerekli teknik ve idari tedbirleri almayan veri sorumlusu hakkında 250.000 TL idari para cezası uyguladı; söz konusu uygulamaya son verilmesine ve sonuç hakkında Kurula bilgi verilmesine karar verildi.

İlgili Karar	İlgili İçerik
Telefon Görüşmesi Kayıtlarına Erişim Talebinin Reddedilmesi 18.04.2024 tarihli ve 2024/592 sayılı Kurul Kararı	• Bir banka çalışanı, banka müşterisiyle gerçekleştirdiği ve hakaret içerdiğini ileri sürdüğü telefon görüşmesinin kaydına yasal yollara başvurabilmek amacıyla erişim talep etti. Banka, görüşmenin müşteri sırrı niteliğinde bilgiler içerdiğini gerekçe göstererek talebi reddetti. • Kurul, kişisel verilere ilişkin bilgi talep etme hakkının verilere erişim hakkını da kapsadığını ve çalışanın talebinin müşteri sırlarına değil, kendisine ait kişisel verilerin yer aldığı görüşme kaydına yönelik olduğunu değerlendirdi. Bu kapsamda, üçüncü kişiye ait müşteri sırrı niteliğindeki bankacılık işlem verilerinin maskelenmesi suretiyle görüşme kaydının yazılı döküm ve dijital ortamda ilgili kişiye verilmesi konusunda bankayı talimatlandırdı.
Kapatılan Borç Bilgisinin Risk Raporundan Silinmesi Talebi 14.03.2024 tarihli ve 2024/444 sayılı Kurul Kararı	• İlgili kişi, 2017 yılında ödeyerek kapattığı borca ilişkin bilgilerin Findeks Risk Raporu'ndan silinmesini talep etti. Kredi Kayıt Bürosu AŞ ise Findeks raporlarının Türkiye Bankalar Birliği Risk Merkezi'ndeki (Risk Merkezi) kayıtlarla paralel oluşturulduğunu belirterek talebi reddetti. • Kurul, Kredi Kayıt Bürosu AŞ'nin Findeks hizmeti bakımından veri sorumlusu olduğunu; kapatılan borca ilişkin bilgilerin Risk Merkezi tarafından "kanunlarda açıkça öngörülmesi" şartına dayanılarak işlendiğini ve borcun kapandığı tarihten itibaren 10 yıl süreyle tutulduğunu tespit etti. • İlgili kişinin borcu 2017 yılında kapatılmış olduğundan verinin 2027 yılına kadar işlenmeye ve Risk Merkezi üyeleriyle paylaşılmaya devam edilebileceğini değerlendiren Kurul, bu konuda KVKK kapsamında yapılacak bir işlem bulunmadığına karar verdi.
Kredi Kayıt Bürosu AŞ Tarafından Kişisel Verilerin İşlenmesi ve Silme Talebi 22.02.2024 tarihli ve 2024/292 sayılı Kurul Kararı	• İlgili kişi, kişisel verilerinin Kredi Kayıt Bürosu AŞ tarafından hukuka aykırı şekilde işlendiğini, üçüncü kişilerle paylaşıldığını ve ticari amaçla kullanıldığını ve silme talebinin reddedildiğini ileri sürdü. • Kurul, bankalar ve finansal kuruluşlar arasındaki veri paylaşımının mevzuata dayandığı ve Findeks platformu üzerinden işlenen verilerin üyeliğin sona ermesinden itibaren 10 yıl süreyle saklanacağına ilişkin veri sorumlusu tarafından verilen cevabın açık ve yeterli olduğunu değerlendirerek KVKK kapsamında yapılacak bir işlem bulunmadığına karar verdi.

İlgili Karar	İlgili İçerik
Eski Çalışana Ait Kişisel Verilerin İşlenmesi Ve Erişim Talebi 22.02.2024 tarihli ve 2024/284 sayılı Kurul Kararı	• Bir kamu kurumu iştirakinin eski çalışanı, işten ayrılmasının ardından kurumsal e-posta hesabı, Personel Yönetim Sistemi'nde tutulan çalışan ve sağlık verileri, veri aktarımları ve aydınlatma uygulamaları kapsamında kişisel verilerinin hukuka aykırı işlendiği iddiasıyla Kurul'a başvurdu. • Kurul, iş ilişkisinin sona ermesinden sonra çalışanın e-posta hesabına doğrudan erişilmediğini tespit ederek bu konuda işlem yapılmasına gerek olmadığına karar verdi. Kurul ayrıca, eski çalışana ait e-posta içeriklerinin olası hukuki uyuşmazlıklarda savunma amacıyla saklanabileceğini; ancak bu veri işleme faaliyetine ilişkin bilginin aydınlatma metninde yer almasını eksiklik olarak değerlendirdi ve aydınlatma metninin güncellenmesine karar verdi. • İşten ayrıldıktan sonra Personel Yönetim Sistemi hesabının pasife alınmasının kişisel verilerin silindiği anlamına gelmediğini belirten Kurul, sistemde saklanmaya devam eden kişisel verilere ilişkin erişim talebinin karşılanması konusunda veri sorumlusunu talimatlandırdı. • Kurul ayrıca, çalışanların sağlık verilerine yalnızca görevleri gereği erişmesi gereken kişilerin erişebilmesi gerektiğini belirterek genel müdür gibi görevleri bakımından bu bilgilere erişmesi gerekli olmayan kişilerin yetkilerinin sınırlandırılması gerektiğini hatırlattı.
İlgili Kişiler Hakkında Bir Gazetede Yayımlanan Ve Halen Söz Konusu Gazetenin Arşiv Kayıtlarında Yer Alan Bir Habere İlişkin Gerçekleştirilen Kişisel Verilerin Silinmesi Ve Unutulma Hakkı Kapsamındaki Şikâyet 28.12.2023 tarihli ve 2023/2185 sayılı Kurul Kararı	• İlgili kişiler, 2001 yılında bir gazetede yayımlanan ve gazetenin internet arşivinde hâlen erişilebilir olan haberin aradan geçen uzun süreye rağmen ad ve soyadlarıyla yapılan aramalarda üst sıralarda görüntülendiğini belirterek haberin ve kişisel verilerinin arşivden kaldırılmasını talep etti. Ancak veri sorumlusu, başvuruyu kanuni süresi içinde cevaplandırmadı. • Kurul, haberde kişisel verilere yer verilmesinin basın özgürlüğü kapsamında Kanun'un 28/1-(c) maddesi uyarınca istisna teşkil ettiğini ve verilerin gazete arşivinden silinmesi talebi hakkında Kanun kapsamında yapılacak bir işlem bulunmadığını değerlendirdi. Arama motorlarında görüntülenmeye son verilmesine yönelik talebin ise unutulma hakkı kapsamında öncelikle arama motorlarına Kanun'un 13 ve 14'üncü maddeleri kapsamında yöneltilmesi gerektiğine karar vererek veri sorumlusuna ilgili kişi başvurularını süresi içinde cevaplandırması gerektiğini hatırlattı.

İlgili Karar	İlgili İçerik
Ceza İnfaz Kurumundaki Hükümlünün Kişisel Verilerine Erişim Talebinin Kanun İstisnası Kapsamında Değerlendirilmesi 20.10.2022 tarihli ve 2022/1152 sayılı Kurul Kararı	• Bir ceza infaz kurumunda bulunan hükümlü, dosyasına ve kişisel verilerine erişim ve bunların düzeltilmesi taleplerinin karşılanmadığını, ayrıca Kurum tarafından kapalı zarfla gönderilen yazıların açılarak gecikmeli teslim edildiğini ve kişisel verilerinin rızası dışında diğer kurum ve kuruluşlarla paylaşıldığını belirterek Kurul'a şikâyette bulundu. • Kurul, dosyaya ve kişisel verilere erişim ile kapalı zarfın açılmasına ilişkin veri işleme faaliyetlerinin, infaz işlemleri kapsamında gerçekleştirilmesi nedeniyle Kanun'un 28. Maddesinin birinci fıkrasının (d) bendi uyarınca istisna kapsamında olduğunu değerlendirdi. Yazının gecikmeli teslim edilmesine ilişkin iddianın Kanun kapsamında değerlendirilmeyeceğine; kişisel verilerin diğer kurum ve kuruluşlarla rıza dışında paylaşıldığı iddiasının ise tevsik edici belgeler sunulmaması nedeniyle esas yönünden değerlendirilmeyeceğine karar verdi.
İşyerinin Güvenlik Kameralarıyla İzlenmesi 28.03.2024 tarihli ve 2024/540 sayılı Kurul Kararı	• Bir şirket, daha önce hırsızlık vakalarının yaşandığı ve çalışanların kişisel eşyalarını muhafaza ettiği alana güvenlik kameraları yerleştirdi, çalışanları bu konuda bilgilendirdi ve görüntü kayıtlarını 60 gün süreyle sakladı. • Kurul, kamera kullanımının iş yerinde güvenliğin sağlanmasına yönelik meşru menfaat kapsamında hukuka uygun olduğunu ve görüntülerin 60 gün süreyle saklanmasının KVKK'da öngörülen ilkelere aykırılık teşkil etmediğini değerlendirdi. • Bununla birlikte Kurul, aydınlatma metninde işleme şartının somut olarak belirtilmemesi ve aydınlatma ile açık rıza süreçlerinin ayrıştırılmaması nedeniyle veri sorumlusuna ilgili metinleri yeniden düzenlemesi yönünde talimat verdi. • Kurul ayrıca, KVKK kapsamında vekil aracılığıyla yapılan başvurularda vekaletnamede özel yetki bulunmasının zorunlu olmadığını belirterek veri sorumlusunu bu konuda uyardı.
Seçim Anketi Verilerinin Yetersiz Anonimleştirilerek Yayımlanması 22.02.2024 tarihli ve 2024/275 sayılı Kurul Kararı	• Yerel bir basın organının seçim anketi kapsamında katılımcıların kimlik ve iletişim bilgileri ile oy tercihleri toplanmış; anket sonuçları, katılımcıların ad ve soyadlarının baş harfleri, kısmen maskelenmiş telefon numaraları ve bazı kayıtlarda mahalle bilgileriyle birlikte internet sitesinde yayımlanmıştır. Veri sorumlusu, verilerin maskelendiğini ve katılımcılardan açık rıza alındığını ileri sürmüştür. • Kurul, seçim anketi sonuçlarının ilgili kişileri belirlenebilir kılan verilerle birlikte herkese açık şekilde yayımlanması sonucunda özel nitelikli kişisel veri niteliğindeki siyasi düşünce bilgilerinin işlendiğini; ilgili kişilere iletilen metnin geçerli açık rızanın unsurlarını taşımaması nedeniyle bu veri işleme faaliyetinin Kanun'un 6. maddesi kapsamında hukuki dayanağının bulunmadığını tespit ederek veri sorumlusu hakkında Kanun'un 12/1'inci maddesine dayalı olarak 40.179 TL idari para cezası uyguladı.

İlgili Karar	İlgili İçerik
Bir Üniversite Tarafından Gerçekleştirilen Ders Yoklamasında Parmak İzi Verilerinin İşlenmesi Suretiyle Devamsızlık Takibi Uygulanması 08.02.2024 tarihli ve 2024/197 sayılı Kurul Kararı	• Bir üniversite, öğrencilerin derslere devam durumunu takip etmek amacıyla özel nitelikli kişisel veri niteliğindeki parmak izi verilerini işledi. Hukuk fakültesinde parmak izi vermek istemeyen öğrencilerin devam takibi manuel yoklama yöntemiyle yapılırken, Tıp fakültesinde parmak iziyle yoklama uygulandı. • Kurul, açık rıza bulunsa dahi ders yoklaması amacıyla biyometrik veri niteliğindeki parmak izinin işlenmesinin ölçülülük ilkesine aykırı olduğunu ve geçerli bir işleme şartına dayanmadığını değerlendirerek, ilgili kişiden alınan açık rızanın ölçüsüz biçimde kişisel veri işlenmesini meşru hale getirmeyeceğini vurguladı. Bu kapsamda Kurul, parmak iziyle yoklama uygulamasının durdurulmasına, mevcut işlenen parmak izi verilerinin imha edilmesine ve Kanun'un 12/1'inci maddesine uygun olarak gerekli teknik ve idari tedbirleri almaktan sorumlu kişiler hakkında Kanun'un 18/3'üncü maddesine dayalı olarak disiplin hükümleri çerçevesinde işlem yapılmasına karar verdi.
İşyerinde Güvenlik Kamerasıyla Hukuki Dayanak Olmaksızın Ses Kaydı Alınması 30.11.2023 tarihli ve 2023/2007 sayılı Kurul Kararı	• Bir çalışanın, işyerindeki güvenlik kamerasıyla ses kaydının alındığını dava sürecinde öğrenmesi üzerine yapılan incelemede Kurul, görüntü kaydının fiziksel güvenliğin sağlanması için yeterli olduğunu ve ayrıca ses kaydı alınmasının zorunlu olmadığını değerlendirdi. • Kurul, ses kaydının Kanun'da öngörülen herhangi bir veri işleme şartına dayanmadığını tespit ederek veri sorumlusuna Kanun'un 12/1'inci maddesine aykırılık sebebiyle Kanun'un 18/1-b) maddesine dayalı olarak 125.000 TL idari para cezası uyguladı ve hukuka aykırı işlenen ses verilerinin imha edilerek Kurul'a bilgi verilmesine karar verdi.
Covid-19 Test Sonucunun Güncel Olmayan Telefon Numarasına Gönderilmesi 19.10.2023 tarihli ve 2023/1787 sayılı Kurul Kararı	• İlgili kişi, okul etkinliği kapsamında üniversite kampüsünde bir sağlık şirketi tarafından açılan stantta Covid-19 testi yaptırarak test sonucunun gönderilmesi için güncel telefon numarasını form aracılığıyla bildirdi. Ancak test sonucu, bu numara yerine veri sorumlusunun sisteminde 2011 yılından beri kayıtlı bulunan ve ilgili kişinin dayısına ait olan eski telefon numarasına SMS yoluyla gönderildi. • Kurul, ilgili kişi tarafından güncel numara bildirilmesine rağmen Covid-19 test sonucunun sistemde kayıtlı eski numaraya gönderilmesinin "doğru ve gerektiğinde güncel olma" ilkesine aykırı olduğunu tespit ederek veri sorumlusuna 30.000 TL idari para cezası uyguladı. Ayrıca, güncel numaranın sisteme kaydedilmesine, ilgili kişinin dayısına ait eski numaranın imha edilerek kayıtlardan çıkarılmasına ve sonuç hakkında Kurula bilgi verilmesine karar verildi.

İlgili Karar	İlgili İçerik
Ceza İnfaz Kurumu Tarafından İnfaz İşlemleri Kapsamında Kişisel Veri İşlenmesi 19.12.2024 tarihli ve 2024/2158 sayılı Kurul Kararı	• Bir ceza infaz kurumu tarafından hükümlü ve tutuklular için düzenlenen tahsilat ve reddiyat makbuzlarında ad-soyad, T.C. kimlik numarası, cezaevi kayıt bilgileri ve para yatıran kişiye ait bilgiler gibi kişisel verilere yer verildi. • Kurul, söz konusu veri işleme faaliyetinin infaz işlemleri kapsamında bir infaz mercii tarafından gerçekleştirildiğini tespit ederek KVKK m. 28/1(d) ile düzenlenen istisna uyarınca KVKK hükümlerinin uygulanmayacağına ve yapılacak bir işlem bulunmadığına karar verdi.
Banka Hesap Bilgilerinin Sigorta Şirketi Tarafından Elde Edilmesi ve Kullanılması 08.08.2024 tarihli ve 2024/1359 sayılı Kurul Kararı	• Bir sigorta şirketi, trafik kazası sonrasında yapılan hasar bildirimi sırasında ilgili kişiye ait IBAN bilgisini kazaya karışan poliçe sahibinden temin ederek, aynı kazaya ilişkin değer kaybı başvurusu kapsamında yapılacak ödemede de bu IBAN bilgisini kullandı. • Kurul, IBAN bilgisinin hasar bildirimi sırasında hukuka uygun olarak elde edildiğini ve aynı kazaya ilişkin değer kaybı ödemesinde kullanılmasının bir hakkın tesisi, kullanılması veya korunması için veri işlemenin zorunlu olması işleme şartına dayandığını belirterek bu konuda yapılacak bir işlem bulunmadığına karar verdi.
Kütüphane Üyeliği Kapsamında İşlenen Kişisel Verilerin Hukuki Sebebi ve Aydınlatma Yükümlülüğüne İlişkin Şikâyet 02.11.2023 tarihli ve 2023/1863 sayılı Kurul Kararı	• Bir belediye kütüphanesinden yararlanmak isteyen kişi, üyelik sırasında kendisinden üyelik süreci için gerekli olmadığı kanaatinde olduğu kişisel verilerin herhangi bir aydınlatma yapılmaksızın talep edildiğini öne sürerek Kurul'a şikâyette bulundu. • Kurul, şikâyete konu olay kapsamında kişisel verilerinin açık rızaya değil, sözleşmenin kurulması veya ifası ve bir hakkın tesisi, kullanılması veya korunması hukuki sebeplerine dayanılarak işlendiğini, aydınlatma yükümlülüğünün kütüphane görevlisi tarafından sözlü olarak, mevcut üyelik sistemlerinde ise internet sitesi ve e-Devlet üzerindeki aydınlatma metni bağlantıları aracılığıyla yerine getirildiğini değerlendirdi. İlgili kişinin verilerinin de mevzuata uygun olarak imha edildiğini dikkate alarak veri sorumlusu hakkında Kanun kapsamında yapılacak bir işlem bulunmadığına karar verdi.
Çağrı Merkezi Görüşmelerinin Kaydedilmesinde Aydınlatma Yükümlülüğünün İhlali 26.10.2023 tarihli ve 2023/1818 sayılı Kurul Kararı	• Alarm ve görüntüleme hizmeti sunan bir şirketin müşterisi, telefon görüşmelerinin aydınlatma yapılmadan ve rızası alınmadan kaydedildiği gerekçesiyle Kurula şikâyette bulundu. • Kurul, görüşmelerin bir hakkın tesisi, kullanılması veya korunması ile veri sorumlusunun meşru menfaati kapsamında hukuka uygun olarak kaydedildiğini; ancak kayıt yapıldığına ilişkin bilgilendirmenin aydınlatma yükümlülüğünün asgari unsurlarını karşılamadığını tespit ederek veri sorumlusuna 15.000 TL idari para cezası uyguladı ve aydınlatma yükümlülüğünün usulüne uygun şekilde yerine getirilmesi talimatını verdi.

İlgili Kişiler

Sevgi Ünsal Özden, LL.M. CIPP/E
Yönetici Avukat ve Arabulucu

sevgiunsal@erdem-erdem.com

Tilbe Birengel, LL.M. CIPP/E
Yönetici Avukat

tilbebirengel@erdem-erdem.nl

Ozan Akman, LL.M. CIPP/E
Kıdemli Avukat

ozanakman@erdem-erdem.av.tr