DL | Avukatlık Bürosu

KİŞİSEL VERİLERİ KORUMA HUKUKU
GÜNCEL GELİŞMELER
MART – NİSAN – MAYIS – HAZİRAN 2025

TÜRKİYE'DEKİ GELİŞMELER

VERİ İHLALİ BİLDİRİMLERİ

Anadolu Anonim Türk Sigorta Şirketi tarafından Kişisel Verileri Koruma Kuruluna ("KVK Kurulu") bildirilen veri ihlali, 06.03.2025 tarihinde Kişisel Verileri Koruma Kurumunun ("KVK Kurumu") internet sitesinde yayımlanmıştır.

Veri sorumlusu Anadolu Anonim Türk Sigorta Şirketi tarafından KVK Kuruluna veri ihlali ("**Veri İhlali**" veya "**İhlal**") bildirilmiştir. Bildirimde aşağıdaki hususlar belirtilmiştir:

- İhlalin 25.02.2025 - 26.02.2025 tarihleri arasında gerçekleştiği,
- İhlalin 26.02.2025 tarihinde tespit edildiği,
- Veri sorumlusu sistemlerinde; poliçelere ilişkin dokümanların poliçenin üretilmesiyle otomatik olarak iletilmesini sağlayan bir geliştirme gerçekleştirildiği ve bu geliştirmenin 25.02.2025 tarihinde canlı ortama alındığı, bu itibarla; yaklaşık 2 gün boyunca hem bireysel sağlık hem de grup sağlık ürünlerine ilişkin gönderimlerin otomatik olarak sağlandığı, ancak grup sağlık ürünü alan bazı müşterilere ait hastalık verilerinin (hastalık mektubu), poliçe kapsamı dışında tutulmasına rağmen bu müşterileri sigorta ettiren şirketlere iletilmesi neticesinde ihlalin gerçekleştiğinin anlaşıldığı,
- İhlalden etkilenen ilgili kişi grubunun müşteriler olduğu,
- İhlalden 242 kişinin etkilendiği,
- İhlalden etkilenen kişisel verilerin; ad, soyadı, sigortalı adresi, poliçe numarası ve sağlık bilgileri olduğu,
- İlgili kişilerin; veri sorumlusunun çağrı merkezi, müşteri iletişim platformu ve diğer iletişim kanalları aracılığıyla ihlal ile ilgili bilgi alabilecekleri.

İlgili karara buradan ulaşabilirsiniz.

Bilfen Eğitim Kurumları A.Ş. tarafından KVK Kuruluna bildirilen veri ihlali, 20.03.2025 tarihinde KVK Kurumu internet sitesinde yayımlanmıştır.

Veri sorumlusu Bilfen Eğitim Kurumları A.Ş. tarafından KVK Kuruluna veri ihlali bildirilmiştir. Bildirimde aşağıdaki hususlar belirtilmiştir:

- İhlalin 12.03.2025 tarihinde başladığı,
- İhlalin veri sorumlusunun Whatsapp hattına siber saldırgan/saldırganlar tarafından 12.03.2025 tarihinde gönderilen bir mesaj ile tespit edildiği,

- İhlalin veri sorumlusunun kullandığı sistemde URL üzerinden sehven erişime açık bırakılan XML dosyalarının saldırganlar tarafından ele geçirilmesiyle gerçekleştiği,
- İhlalden etkilenen ilgili kişilerin; öğrenciler, öğrenci velileri ve çalışanlar olduğu,
- İhlalden etkilenen veri kategorilerinin; kimlik, iletişim, işlem güvenliği, mesleki deneyim, görsel ve işitsel kayıtlar ile birlikte özel nitelikli kişisel verilerden sağlık bilgileri olduğu,
- İhlalden etkilenen kişi sayısının 24.061 kişi olduğu,
- İlgili kişilerin, veri sorumlusuna ait https://bilfen.com/tr internet sitesi vasıtasıyla veri ihlaline ilişkin duyurulara ulaşabileceği ve ayrıca detaylı bilgi için kvkk@bilfen.com e-posta hesabı vasıtasıyla veri ihlali hakkında bilgi alabilecekleri.

İlgili karara buradan ulaşabilirsiniz.

Turknet İletişim Hizmetleri A.Ş. tarafından KVK Kuruluna bildirilen veri ihlali, 20.03.2025 tarihinde KVK Kurumu internet sitesinde yayımlanmıştır.

Veri sorumlusu Turknet İletişim Hizmetleri A.Ş. tarafından KVK Kuruluna veri ihlali bildirilmiştir. Bildirimde aşağıdaki hususlar belirtilmiştir:

- İhlalin 26.02.2025 tarihinde başladığı,
- İhlalin 11.03.2025 tarihinde genele açık bir BTK şikayet kaydı ile tespit edildiği,
- İhlalin veri sorumlusunun servislerinden birine gerçekleştirilen SQL Injection saldırısı neticesinde gerçekleştiği,
- İhlalden etkilenen ilgili kişi grubunun Aboneler/Üyeler olduğu,
- İhlalden etkilenen kişisel verilerin; müşterilere ait ad, soyad, telefon numarası, abonelik numarası, TC kimlik numarası, TurkNet abonelik devre bilgileri, adres, statik IP bilgileri olduğu,
- İlk incelemelerde; ilgili log kayıtlarına bakıldığında 244.396 kullanıcının verilerinin sızdığının tespit edilebildiği ve bu kapsamda veri sorumlusu bünyesinde detaylı incelemenin devam ettiği,
- İlgili kişilerin 0850 288 80 80 / 0850 344 28 18 numaralı Turknet hızlı işlem hattından veya “Fulya, Büyükdere Cad. Torun Center No: 80 A Blok No: 74 A 34394 Şişli/İstanbul” posta adresinden ihlal ile ilgili bilgi alabileceği.

İlgili karara buradan ulaşabilirsiniz.

Nevşehir Hacı Bektaş Veli Üniversitesi tarafından KVK Kuruluna bildirilen veri ihlali, 28.03.2025 tarihinde KVK Kurumu internet sitesinde yayımlanmıştır.

Veri sorumlusu Nevşehir Hacı Bektaş Veli Üniversitesi tarafından KVK Kuruluna veri ihlali bildirilmiştir. Bildirimde aşağıdaki hususlar belirtilmiştir:

- İzmir Kâtip Çelebi Üniversitesi (“İKÇÜ”) tarafından geliştirilen Üniversite Bilgi Yönetim Sistemi’nin (ÜBYS) veri sorumlusu tarafından kullanıldığı ve bu kapsamdaki PingPong Üniversite Rehberi isimli mobil uygulamanın, İKÇÜ tarafından sağlanan web servisleri aracılığıyla veri sorumlusunun personel ve öğrencilerinin kişisel verilerine eriştiğinin tesadüfen tespit edildiği,
- Bir öğrencinin veri sorumlusuna, kişisel verilerine başka bir mobil uygulamadan erişebildiğini ifade etmesi üzerine durumun tespit edildiği ve mobil uygulamaya sahip firmanın verilerinin İKÇÜ tarafından elde edildiğinin tespit edildiği,

- İKÇÜ'ye durum hakkında bilgi vermesi için yazışmalar gerçekleştirildiği, verilerin İKÇÜ'nün veri sorumlusundan izinsiz olarak paylaşıldığının tespit edildiği, paylaşım yapılan firmanın kullanıcı sözleşmesi incelendiğinde ise verilerin saklandığı ve işlendiğinin değerlendirildiği,
- İhlalden etkilenen ilgili kişi gruplarının; çalışanlar ve öğrenciler olduğu,
- İhlalden etkilenen kişi sayısının tam olarak bilinmediği ancak web serviste kayıtlı 22.960 aktif öğrenci ve personelin bulunduğu.

İlgili karara buradan ulaşabilirsiniz.

Bellapais El Ayak Bakımı ve Güzellik Salonu Ticaret Limited Şirketi tarafından KVK Kurumuna bildirilen veri ihlali, 10.04.2025 tarihinde KVK Kurumu internet sitesinde yayımlanmıştır.

Veri sorumlusu Bellapais El Ayak Bakımı ve Güzellik Salonu Ticaret Limited Şirketi tarafından KVK Kuruluna veri ihlali bildirilmiştir. Bildirimde aşağıdaki hususlar belirtilmiştir:

- İhlalin 03.04.2025 tarihinde tespit edildiği,
- İhlalin, siber saldırı neticesinde veri sorumlusu sistemine yetkisiz erişim sağlandığı ve sistemdeki verilerin ele geçirilecek gerçekleştiği,
- İhlalden etkilenen ilgili kişi gruplarının; çalışanlar, kullanıcılar ve müşteriler/potansiyel müşteriler olduğu,
- İhlalden etkilenen ilgili kişi sayısının 83.070 olduğu,
- İhlalden etkilenen kişisel verilerin; ad, soyad, T.C. Kimlik numarası, doğum tarihi, cinsiyet, anne adı, baba adı, telefon numarası, adres bilgileri, müşteriyle yapılması planlanan işlemler, alınan ödeme bilgileri (tutar, işlem açıklamaları vb.) ve sağlık verilerinin (varsa beyan edilen kronik rahatsızlık bilgileri) etkilendiği,
- İlgili kişilerin, çağrı merkezi ve sosyal mecralar aracılığıyla bilgi alabilecekleri.

İlgili karara buradan ulaşabilirsiniz

Robotistan Elektronik Ticaret A.Ş tarafından KVK Kurumuna bildirilen veri ihlali, 15.04.2025 tarihinde KVK Kurumu'nun internet sitesinde yayımlanmıştır.

Veri sorumlusu Robotistan Elektronik Ticaret A.Ş tarafından KVK Kuruluna veri ihlali bildirilmiştir. Bildirimde aşağıdaki hususlar belirtilmiştir:

- İhlalin 2024 yılının Şubat ayında başladığı ve 07.04.2025 tarihinde tespit edildiği,
- Siber saldırgan/saldırganların, veri sorumlusu ile e-posta aracılığıyla iletişime geçtikleri ve veri sorumlusuna ait verileri ele geçirdiklerini belirttikleri,
- İnternet sitesi altyapı sağlayıcısı olarak T-Soft üzerinden hizmet alındığı,
- İhlalden etkilenen ilgili kişi grubunun; müşteriler/potansiyel müşteriler olduğu,
- İhlalden etkilenen ilgili kişi sayısının henüz bilinemediği,
- İhlalden etkilenen kişisel verilerin; ad, soyad, telefon numarası, adres bilgileri ve sipariş bilgilerinin ihlalden etkilendiği.

İlgili karara buradan ulaşabilirsiniz.

Tourama Tourism Seyahat ve Ticaret A.Ş. tarafından KVK Kurumuna bildirilen veri ihlali, 06.05.2025 tarihinde KVK Kurumunun internet sitesinde yayımlanmıştır.

Veri sorumlusu Tourama Tourism Seyahat ve Ticaret A.Ş. tarafından KVK Kuruluna veri ihlali bildirilmiştir. Bildirimde aşağıdaki hususlar belirtilmiştir:

- İhlalin 29.04.2025 tarihinde gerçekleştiği ve aynı gün tespit edildiği,
- İhlalin, veri sorumlusuna ait bir internet uygulamasındaki güvenlik açığından faydalanılması sonucu otellere bilgi amaçlı gönderilen e-postalara yetkisiz erişim sağlanarak gerçekleştiği,
- İhlalin, yetkisiz kişinin sisteme sızdığına dair veri sorumlusuna bir e-posta göndermesi üzerine tespit edildiği,
- İhlalden etkilenen ilgili kişi grubunun müşteriler olduğu,
- İhlalden etkilenen kişi ve kayıt sayısının tam olarak tespit edilemediği, ancak yapılan incelemelerde, e-posta sunucusunda bulunan dosyaların bir kısmının yetkisiz şekilde dışarı sızdırıldığının veri sorumlusu tarafından değerlendirilmiş olduğu ve e-posta sunucusunda yaklaşık 8.200 kişinin ad ve soyad bilgisinin yer aldığının tahmin edildiği,
- İhlalden etkilenen kişisel verilerin; ad ve soyad olduğu.

İlgili karara buradan ulaşabilirsiniz.

Atakaş Çelik Sanayi ve Ticaret A.Ş. ve Atakaş Liman İşletmeciliği ve Ticaret A.Ş. tarafından KVK Kurumuna bildirilen veri ihlali, 22.05.2025 tarihinde KVK Kurumunun internet sitesinde yayımlanmıştır.

Veri sorumlulukları Atakaş Çelik Sanayi ve Ticaret A.Ş. ve Atakaş Liman İşletmeciliği ve Ticaret A.Ş. tarafından KVK Kuruluna veri ihlali bildirilmiştir. Bildirimde aşağıdaki hususlar belirtilmiştir:

- Bir süre önce bir kısım çalışan ve eski çalışanın kimlik ve iletişim bilgilerini içeren tehdit ve şantaj içerikli e-postalar alınmaya başlandığı,
- Anılan e-postaların, öncelikle güvenlik duvarına takıldığı için geç fark edildiği; 08.05.2025 tarihinde gönderilen e-postada yer alan bağlantıya tıklandığında çalışanlara ait, fotoğraf, kimlik, adres, anne adı, baba adı bilgilerinin bulunduğunun görüldüğü,
- İlgili log kayıtlarından 03.05.2025 tarihinden itibaren veri sorumluları sistemlerine yetkisiz girişler olduğunun tespit edildiği,
- İhlalden etkilenen ilgili kişi grubunun; çalışanlar ve eski çalışanlar olduğu,
- İhlalden etkilenen ilgili kişi sayısının; Atakaş Çelik Sanayi ve Ticaret A.Ş. için tahmini olarak 1080, Atakaş Liman İşletmeciliği ve Ticaret A.Ş. için tahmini 135 olduğu,
- İhlalden etkilenen kişisel verilerin; ad, soyad, vesikalık fotoğraf, telefon numarası, doğum tarihi, e-posta adresi, anne adı, baba adı, adres bilgisi, medeni hal, cinsiyet, işe giriş tarihi, görev ve şirket bilgileri olduğu.

İlgili karara buradan ulaşabilirsiniz.

Christian Dior Couture SA tarafından KVK Kurumuna bildirilen veri ihlali, 22.05.2025 tarihinde KVK Kurumunun internet sitesinde yayımlanmıştır.

Veri sorumlusu Christian Dior Couture SA tarafından KVK Kuruluna veri ihlali bildirilmiştir. Bildirimde aşağıdaki hususlar belirtilmiştir:

- 26 Ocak 2025 tarihinde, veri sorumlusunun küresel CRM veritabanında tutulan aktif, pasif ve potansiyel müşterilere ait kişisel verilere yetkisiz erişim gerçekleştirildiği,

- Kötü niyetli yetkisiz kişi tarafından, veri sorumlusu sistemleri dışına aktarılan verilerin ifşa edilmekle tehdit edildiği ve bu kapsamda veri sorumlusundan fidye talep edildiği,
- İhlalden etkilenen ilgili kişi grubunun; müşteriler ve potansiyel müşteriler, satış danışmanları ve müşteri asistanları olduğu,
- İhlalden etkilenen ilgili kişi sayısının henüz tespit edilemediği,
- İhlalden etkilenen kişisel verilerin; ad, cinsiyet, doğum tarihi, yaş, posta veya e-posta adresi, sabit hat veya cep telefonu numarası, şifre, müşteri numarası, pasaport bilgileri, kimlik belgeleri, genel tercih verileri (yeme-içme, etkinlikler, hobiler vb.), satın alma geçmişi verileri (segmentler, nihai parasal tutar vb.), satın alma tercihi ve ölçü verileri (renk, beden, ölçüler vb.), meslek bilgisi, dolandırıcılık şüphesi ve uluslararası yaptırımlar kapsamındaki numaralar (yasalar gereğince tutulan), bazı ülkelerde yasal olarak talep edilen vergi numarası, imza ve hedef alınan müşteri hizmetleri personeline ait kimlik doğrulama verileri olduğu,
- CRM veritabanına yetkisiz erişim engellenmiş olmakla birlikte, verilerin uygunsuz şekilde kullanılması veya ifşa edilmesi riskinin mevcut olduğu,
- Veri sorumlusu bünyesinde ihlal ile ilgili incelemelerin devam ettiği.

İlgili karara buradan ulaşabilirsiniz.

Adidas Spor Malzemeleri Satış ve Pazarlama A.Ş. tarafından KVK Kurumuna bildirilen veri ihlali, 22.05.2025 tarihinde KVK Kurumunun internet sitesinde yayımlanmıştır.

Veri sorumlusu Adidas Spor Malzemeleri Satış ve Pazarlama A.Ş. tarafından KVK Kuruluna veri ihlali bildirilmiştir. Bildirimde aşağıdaki hususlar belirtilmiştir:

- Veri sorumlusunun, Adidas AG grup alt yapısıyla ilişkili bir siber güvenlik olayı hakkında bilgilendirilmesiyle; ihlalin, 17.05.2025 tarihinde tespit edildiği,
- İhlalin, Adidas çalışanının üçüncü bir tarafın e-postasını Adidas Siber Güvenlik Olaylarına Müdahale Ekibine iletmesinin ardından ortaya çıktığı,
- Bu e-postada üçüncü tarafın, Adidas müşteri verilerine sahip olduğunu iddia ettiği, Adidas tarafından yapılan inceleme sonucunda üçüncü şahıs tarafından paylaşılan dosyanın büyük olasılıkla Adidas müşteri verilerini içerdiğini ve Türk müşterilerinin de etkilendiği Adidas tarafından doğrulandığı,
- İhlalin kaynağı ve nasıl gerçekleştiği hakkında soruşturmanın devam ettiği,
- İhlalden etkilenen ilgili kişi sayısının 544.395 olduğu,
- İhlalden etkilenen kişisel verilerin; isim, e-posta adresi, cinsiyet, doğum tarihi ve telefon numarası olduğu, tüm müşteriler için bütün veri tiplerinin etkilenmediği.

İlgili karara buradan ulaşabilirsiniz.

Manulaş Manisa Ulaşım Hizmetleri Makina Sanayi ve Ticaret A.Ş. tarafından KVK Kurumuna bildirilen veri ihlali, 03.06.2025 tarihinde KVK Kurumunun internet sitesinde yayımlanmıştır.

Veri sorumlusu Manulaş Manisa Ulaşım Hizmetleri Makina Sanayi ve Ticaret A.Ş. tarafından KVK Kuruluna veri ihlali bildirilmiştir. Bildirimde aşağıdaki hususlar belirtilmiştir:

- İhlalin, veri sorumlusu sistemlerine gerçekleştirilen siber saldırı (fidye yazılımı saldırısı) neticesinde meydana geldiği,
- İhlalin, 25.05.2025 tarihinde gerçekleştiği ve aynı gün tespit edildiği,
- Siber saldırı neticesinde verilerin dışarıya aktarılıp aktarılmadığının henüz tespit edilemediği,

- İhlalden etkilenen ilgili kişi gruplarının; aboneler/üyeler olduğu,
- Veri ihlalinden etkilenen kişi/kayıt sayısının 1.268.222 olduğu ancak sistem içerisinde çok sayıda mükerrer kayıt bulunması sebebiyle ihlalden etkilenen gerçek kişi sayısının muhtemelen çok daha az olduğu,
- İhlalden etkilenen kişisel verilerin; ad, soyad, T.C. kimlik numarası, doğum tarihi, cinsiyet, telefon numarası, e-posta adresi, açık adres, meslek bilgisi (öğretmen/ polis/öğrenci vb.), plaka no, fotoğraf ve sağlık bilgileri (engellilik bilgisi, engellilik oranı) olduğu,
- İlgili kişilerin; veri sorumlusunun internet sitesi (https://manulas.com.tr/), telefon numarası (0 236 232 19 00) veya e-posta adresi (info@manulas.com.tr) aracılığıyla ihlal hakkında bilgi alabilecekleri.

İlgili karara buradan ulaşabilirsiniz.

Richemont İstanbul Lüks Eşya Dağıtım A.Ş. tarafından KVK Kurumuna bildirilen veri ihlali, 03.06.2025 tarihinde KVK Kurumunun internet sitesinde yayımlanmıştır.

Veri sorumlusu Richemont İstanbul Lüks Eşya Dağıtım A.Ş. tarafından KVK Kuruluna veri ihlali bildirilmiştir. Bildirimde aşağıdaki hususlar belirtilmiştir:

- İhlalin, 17.01.2025-18.01.2025 tarihleri arasında gerçekleştiği ve 30.05.2025 tarihinde tespit edildiği,
- Veri sorumlusunun da dahil olduğu Richemont Group bünyesinde görev yapan bir çalışanın hesabının yetkisiz kişi/kişilerce elde edilmesi ve bu hesap kullanılarak veri sorumlusunun müşterilerine ait kişisel verilerin ele geçirilmesi neticesinde ihlalin gerçekleştiği,
- İhlalden etkilenen ilgili kişi grubunun; müşteriler/potansiyel müşteriler olduğu,
- İhlalden etkilenen ilgili kişi sayısının 25.737 olduğu,
- İhlalden etkilenen kişisel verilerin; isim, e-posta adresi, ülke bilgisi, müşteri kimliği ve doğum tarihi olduğu.

İlgili karara buradan ulaşabilirsiniz.

İstanbul Gedik Üniversitesi tarafından KVK Kurumuna bildirilen veri ihlali, 03.06.2025 tarihinde KVK Kurumunun internet sitesinde yayımlanmıştır.

Veri sorumlusu İstanbul Gedik Üniversitesi tarafından KVK Kuruluna veri ihlali bildirilmiştir. Bildirimde aşağıdaki hususlar belirtilmiştir:

- İhlalin, veri sorumlusu adına veri işleyen şirketin sistemlerine yetkisiz erişim gerçekleştirilmesi neticesinde gerçekleştiği,
- İhlalin 13.05.2025-14.05.2025 tarihleri arasında gerçekleştiği ve 14.05.2025 tarihinde tespit edildiği,
- İhlalden etkilenen ilgili kişi gruplarının; çalışanlar, kullanıcılar ve öğrenciler olduğu,
- İhlalden etkilenen ilgili kişi sayısının 23.269, kayıt sayısının ise 209.421 olduğu,
- İhlalden etkilenen kişisel verilerin; ad, soyadı, kullanıcı adı, maskelenmiş ve yalnızca son dört hanesi görünür biçimde T.C. kimlik numarası, e-posta adresi, kurum-departman bilgileri ve kullanıcının trafik verileri olduğu.

İlgili karara buradan ulaşabilirsiniz.

TCO Turkey Mücevherat Ticareti Ltd. Şti. tarafından KVK Kurumuna bildirilen veri ihlali, 10.06.2025 tarihinde KVK Kurumunun internet sitesinde yayımlanmıştır.

Veri sorumlusu TCO Turkey Mücevherat Ticareti Ltd. Şti. tarafından KVK Kuruluna veri ihlali bildirilmiştir. Bildirimde aşağıdaki hususlar belirtilmiştir:

- İhlalin veri sorumlusunun ABD merkezli bağlı şirketi Tiffany and Company şirketinin bazı sistemlerine yetkisiz bir üçüncü tarafça erişim sağlanmasıyla gerçekleştiği,
- İhlalin 12.05.2025 - 16.05.2025 tarihleri arasında gerçekleştiği ve 04.06.2025 tarihinde tespit edildiği,
- İhlalden etkilenen ilgili kişi gruplarının; veri sorumlusu çalışanları ve müşterileri olduğu,
- İhlalden etkilenen kişi ve kayıt sayısının belirlenmesi için veri sorumlusu tarafından çalışmaların sürdürüldüğü,
- İhlalden etkilenen kişisel verilerin; ad, iletişim bilgileri, unvan, yönetici bilgileri, kullanıcı adları ve karma şifreler dahil olmak üzere çalışan ve danışman şirket dizini verilerini içerdiğinin belirlendiği, ayrıca devam eden soruşturmaya dayanılarak; etkilenen kişisel verilerin müşteri adları, iletişim bilgileri, yaş, satış verileri ve cinsiyet bilgilerini de içerme ihtimalinin bulunduğu.

İlgili karara buradan ulaşabilirsiniz.

BeiGene, Ltd. tarafından KVK Kurumuna bildirilen veri ihlali, 24.06.2025 tarihinde KVK Kurumunun internet sitesinde yayımlanmıştır.

Veri sorumlusu BeiGene, Ltd. tarafından KVK Kuruluna veri ihlali bildirilmiştir. Bildirimde aşağıdaki hususlar belirtilmiştir:

- 16 Haziran 2025 tarihinde, sınırlı sayıda kurumsal dosyanın iki harici dosya paylaşım platformuna (pastebin.com ve swisstransfer.com) yüklendiğinin tespit edildiği,
- Söz konusu dosyaların, klinik çalışmaların planlanması ve takibi için kullanılan verileri içerdiği,
- İhlalden etkilenen ilgili kişi gruplarının; veri sorumlusu çalışanları ve hastalar olduğu,
- İhlalden ,Türkiye'den 17 çalışan ve 450 hasta olmak üzere 467 kişinin etkilendiği,
- İhlalden etkilenen kişisel veri kategorilerinin; kimlik, iletişim ve sağlık bilgileri olduğu.

İlgili karara buradan ulaşabilirsiniz.

GÜNCEL KARARLAR

KVK Kurulu tarafından fiziksel alışverişler kapsamında ilgili kişilere iletilen SMS doğrulama kodlarına yönelik 2025/1072 sayılı İlke Karar yayımlanmıştır.

KVK Kurulu'nun 10.06.2025 tarihli ve 2025/1072 sayılı ilke kararı 26.05.2025 tarihinde yayımlanmıştır. Karar, ürün ve hizmet sunumu sırasında ilgili kişilere SMS ile gönderilen doğrulama kodları üzerinden kişisel verilerin işlenmesine dair önemli düzenlemeler getirmekteyse de KVK Kurumu tarafından daha önceki dönemlerde benzer hususları içeren duyurular yayımlanmıştır. Kararda özetle;

- Ürün ve hizmet sunumlarına ilişkin süreçlerde (ödeme yapma, kayıt açma, üyelik oluşturma, teklif oluşturma ve benzeri işlemler esnasında) ilgili kişilerin telefonuna gönderilecek olan SMS'in amacının ne olduğu ve bu SMS ile iletilen kodun verilmesi halinde ne gibi sonuçlar doğuracağı hususunun, katmanlı aydınlatmanın bir gereği olarak ilk aşamada veri sorumlusunun görevlileri tarafından ilgili kişilere açık ve anlaşılır bir biçimde aktarılması, ayrıca aydınlatma yükümlülüğünün yerine getirilebilmesi amacıyla söz konusu SMS içeriklerinde de gerekli bilgilendirme kanallarının sağlanması,
- İlgili kişilere SMS ile doğrulama kodu gönderilerek üyelik sözleşmesinin onaylanması, kişisel verileriişleme izni alınması, ticari elektronik ileti onayı alınması vb. birbirinden farklı işleme

faaliyetlerinin tek bir eylemle gerçekleştirilmesine yönelik uygulamalara son verilmesi, açık rıza ile gerçekleştirilmesi gereken işleme faaliyetlerine yönelik seçenek sunulmak suretiyle ilgili kişilerden ayrı ayrı açık rıza alınması,

- Bunun yanı sıra, veri sorumlularınca açık rıza alınması ve aydınlatma yükümlülüğünün yerine getirilmesi işlemlerinin ayrı ayrı gerçekleştirilmesi,
- Ticari elektronik ileti gönderimi için açık rıza alınmasını teminen SMS doğrulama kodu gönderilmesine yönelik bir uygulamaya gidilmesi halinde ise söz konusu işlemde alınacak açık rızanın Kanun'da belirtilen tüm unsurları kapsaması,
- Ticari elektronik ileti gönderilmesi amacıyla kişisel verilerin işlenmesine açık rıza verilmesinin ürün ve hizmet sunumunun tamamlanabilmesi için zorunlu bir unsur şeklinde ilgili kişilere sunulmaması, aksi takdirde söz konusu uygulamanın açık rızanın unsurlarından olan "bilgilendirmeye dayanma ve özgür iradeyle açıklanma" unsurlarının zedelenmesine sebep olabileceği, bu nedenle tüm süreçlerin Kanun'a uygun şekilde gerçekleştirilmesi,
- Bu kapsamda ticari elektronik ileti gönderilmesi amacıyla kişisel verilerin işlenmesine yönelik açık rızanın, ürün ve hizmet sunumunun tamamlanmasından sonra talep edilmesi veya gerek SMS içeriklerinde gerekse veri sorumlusu tarafından fiziksel ortamda veya dijital ortamda yapılan bilgilendirmelerde söz konusu kodun görevli ile paylaşılması suretiyle verilen rızanın ürün ve hizmet sunumunun tamamlanması için zorunlu olmadığı, kodun verilmemesi halinde de her zaman ürün ve hizmet sunulabileceği, kod ile verilen izinlerin ve tercihlerin istendiği zaman değiştirilebileceği bilgisine net bir şekilde yer verilmesi yöntemlerinin tercih edilmesi ile ticari elektronik iletiiznine yönelik açık rızanın ürün ve hizmet sunumunun zorunlu bir unsuru gibi algılanmasının önüne geçilmesi,
- Bahse konu işlemlerin hukuka uygunluğunun sağlanmasını teminen veri sorumluları tarafından bu süreçlerde yer alan personele yönelik gerekli eğitim ve farkındalık çalışmalarının periyodik olarak yürütülmesi

Yukarıda hususlara aykırı davranılması halinde KVKK'nın 18. maddesi uyarınca veri sorumlularına idari para cezası düzenleneceği belirtilmiştir.

İlgili karara buradan ulaşabilirsiniz.

DUYURULAR VE HABERLER

KVK Kurumu tarafından akıllı telefonlara ilişkin bazı güvenlik önerileri yayımlanmıştır.

KVK Kurumunun LinkedIn hesabından akıllı telefonları kullanırken kişisel verilerin korunmasına özen göstermek amacıyla bazı öneriler yayımlanmıştır.

- Şifre, PIN veya desen kaydırma gibi ekran kilidi yöntemlerinin tercih edilmesi,
- Akıllı telefonların işletim sisteminin ve içerisindeki uygulamaların güncel tutulması,
- Kötü amaçlı yazılım ve virüslerden korunmaya yardımcı olması bakımından anti virüs ve güvenlik yazılımlarının kullanılması,
- Uygulamaları kullanırken gerekli olmayan erişim izinlerinin sınırlandırılması,
- Akıllı telefonun kaybolması veya çalınması durumunda içerisindeki verileri uzaktan silmenizi veya cihazınızı kilitlemenizi sağlayan güvenlik özelliklerinin aktif hale getirilmesi.

İlgili önerilere buradan ulaşabilirsiniz.

KVK Kurumu tarafından çevrimiçi alışverişlere ilişkin bazı öneriler yayımlanmıştır.

KVK Kurumunun LinkedIn hesabından çevrimiçi alışverişlere ilişkin bazı öneriler yayımlanmıştır.

Çevrimiçi alışverişlerde dikkat edilmesi gereken hususlar aşağıdaki şekilde belirtilmiştir:

- Alışveriş yapılacak internet sitesinin iletişim bilgilerinin, 3D güvenli ödeme yöntemi ile SSL sertifikasının bulunup bulunmadığının kontrol edilmesi,
- Kredi kartı bilgilerinin çalınması riskini minimize etmek amacıyla alışverişlerde sanal kart kullanılması,
- Alışveriş sırasında yalnızca gerekli olan bilgilerin paylaşılması, gereğinden fazla bilgi taleplerine karşı sorgulayıcı olunması,
- Alışveriş yapılan farklı platformlarda aynı şifrelerin kullanılmaması,
- Şüpheli bir durumla karşılaşılması halinde parola ve şifrelerin değiştirilmesi,
- E-posta, SMS veya sosyal medya reklamlarıyla gelen bağlantılara karşı dikkatli olunması, güvenliğinden emin olunmayan bağlantıların açılmaması,
- Aceleyle yapılan çevrim içi alışverişlerin kişisel verilerin korunmasını riske atabilmesi sebebiyle; hızlı karar verirken sahte internet sitelerini, sahte bağlantıları ve dolandırıcılık amaçlı e-postaları fark edilmesinin güçleşmesi sebebiyle acele alışveriş yapılmaması.

Fiziksel alışverişlerde dikkat edilmesi gereken hususlar aşağıdaki şekilde belirtilmiştir:

- Kişisel verilerin işlenmesine ilişkin aydınlatma metinlerinin gözden geçirilmesi, buna istinaden merak edilen bir husus olması halinde sorulması,
- Kasada işlem esnasında kart şifresi ve kart numarası gibi finansal bilgilerin diğer kişilerce görünür olmamasına özen gösterilmesi,
- Sadakat kart ve kampanyalara kayıt olunması halinde kişisel verilerin hangi amaçlarla işleneceğinin öğrenilmesi,
- Ödeme yapıldıktan sonra fiş veya faturalarınızın sizlere ait olup olmadığının kontrol edilmesi.

İlgili önerilere buradan ulaşabilirsiniz.

KVK Kurumu tarafından yapay zeka alanında kişisel verilerin korunmasına dair 10 önemli tavsiye paylaşılmıştır.

KVK Kurumu tarafından yapay zekâ teknolojilerinin gelişimi karşısında bireylerin temel hak ve özgürlüklerinin korunmasına dikkat çekerek, kişisel verilerin korunmasına dair 10 önemli tavsiye KVK Kurumunun LinkedIn hesabında paylaşılmıştır. Tavsiyelerde aşağıdaki husular belirtilmiştir:

- Yapay zekâ sistemleri, insan merkezli bir yaklaşımla tasarlanması,
- Tüm algoritmalar, veri koruma hukukuna uygunluk bakımından hesap verebilir olması,
- Uygulamalardan etkilenmesi muhtemel birey ve grupların katılımına dayalı risk değerlendirmesi yapılması,
- Kararlarda otomatik işlemeye dayalı olarak bireylerin mağdur edilmesi önlenmesi,
- Verilerin işlenmesinde mümkünse anonimleştirme tercih edilmesi,
- Yapay zeka çalışmalarında tüm sistemler tasarımdan itibaren veri koruma ilkesine göre geliştirilmesi,
- İnsan müdahalesinin rolü tesis edilmelidir. Bireylerin yapay zeka uygulamaları ile sunulan önerilerin sonucuna güvenmeme özgürlüğü korunması,
- Kişisel verilerin kullanımı, asgari düzeyde tutulmalı; veri kalitesi ve doğruluk izlenmesi,

- Mahremiyet etki değerlendirmesi ile yüksek riskli veri işleme faaliyetleri kontrol altına alınması,
- Veri mahremiyeti odaklı eğitim ve farkındalık çalışmaları desteklenmesi.

İlgili önerilere buradan ulaşabilirsiniz.

KVK Kurumu tarafından 13.03.2025 tarihinde bir taahhütname duyurusu yayımlanmıştır.

KVK Kurumunun internet sitesinde yayımlanan duyuru kapsamda; VF Ege Giyim San. ve Tic. Ltd. Şti. tarafından KVK Kurumuna üç adet Taahhütname başvurusu gerçekleştirildiği, bu kapsamda KVK Kurulu tarafından işbu başvuruların 6698 sayılı Kişisel Verilerin Korunması Kanunu'nun ("**KVKK**") 9 uncu maddesinin 4 üncü fıkrasının (ç) bendi kapsamında değerlendirilerek ve usul ve esasa dair herhangi bir eksikliğin bulunmadığı kanaatinde varılarak 12.03.2025 tarihinde Kurul tarafından söz konusu veri aktarımlarına izin verildiği paylaşılmıştır.

İlgili duyuruya buradan ulaşabilirsiniz.

KVK Kurumu tarafından Biyometrik Verilerin İşlenmesine İlişkin Rehber güncellenerek 25.03.2025 tarihinde yayımlanmıştır.

KVK Kurumu tarafından biyometrik verilerin işlenmesi süreçleri bakımından dikkat edilmesi gereken hususlara ilişkin Rehber güncellenerek KVK Kurumunun internet sitesinde yayımlanmıştır. Güncellenen Rehber'de, biyometrik verilerin özel nitelikli kişisel veri olduğu hatırlatılarak, aşağıdaki hususlar belirtilmiştir:

- AB Genel Veri Koruma Tüzüğüne ("GDPR") atfen, bir verinin biyometrik veri olabilmesi için, (i) Kişinin fizyolojik, fiziksel veya davranışsal özellikleri gibi ayırt edici özellikleri veri işleme sonucunda ortaya çıkarması gerektiği (ii) Ortaya çıkarılan özellikler kişinin kimliğini tanımlamaya yarayan ya da kişinin kimliğini doğrulayan kişisel veriler olması gerektiği,
- Biyometrik verilerin, kişilerin unutmasının mümkün olmadığı, genelde ömür boyu değişmeyen ve herhangi bir müdahaleye gerek olmaksızın zahmetsiz bir şekilde sahip olunan veriler olduğu,
- Biyometrik verilerin kullanılması sayesinde kişilerin birbirlerinden ayırt edilmeleri çok kolay bir hale gelmekte olduğu ve birbirleriyle karıştırılma ihtimalleri neredeyse ortadan kalktığı,
- Kişinin parmak izi, retinası, avuç içi, yüzü, el şekli, irisi, yüz geometrisi, el geometrisi gibi biyometrik verileri fizyolojik nitelikli biyometrik verileri oluşturmakta olduğu; **kişinin yürüyüş biçimi, klavyeye basış biçimi, araba sürüş biçimi, akıllı telefon ve benzer cihazları kullanırken ekranı kaydırmak için sergilenen hareketler, klavyeye basış biçimi gibi biyometrik verileri ise davranışsal nitelikli biyometrik verileri oluşturduğu,**
- Biyometrik verilerin ancak belirtilen koşulların hepsinin sağlanması halinde işlenebileceği; (i) Temel hak ve özgürlüklere dokunmaması, (ii) Başvurulan yöntemin işleme amacına ulaşılabilmesi bakımından elverişli olması, veri işleme faaliyetinin ulaşılmak istenen amaç için uygun olması, (iii) Biyometrik veri işleme yönteminin ulaşılmak istenen amaç bakımından gerekli olması, (iv) Veri işlemeyle ulaşılmak istenilen amaç ve aracın arasında orantı bulunması, (v) Gerektiği süre kadar tutulması, gereklilik ortadan kalktıktan sonra söz konusu verilerin gecikmeksizin/derhal imha edilmesi, (vi) İşleme amacı doğrultusunda sınırlı olmak üzere; veri sorumlularının KVKK'nın 10 uncu maddesine uygun bir biçimde aydınlatma yükümlülüğünü yerine getirmesi, (vii) Açık rızanın gerekmesi halinde ilgili kişilerin açık rızalarının KVKK'ya uygun şekilde alınmış olması ve bu kapsamda kişinin sadece konu üzerinde değil, aynı zamanda rızasının sonuçları üzerinde de tam bir bilgi sahibi olması gerektiği,
- Yukarıda sayılan işbu koşulların sağlandığının veri sorumlusu tarafından kayıt altına alınıp belgelendirilmesi, gerekmediği takdirde, biyometrik veri alınırken genetik veri (kan, tükürük vb.) alınmaması, biyometri türünün veya türlerinin seçiminde (iris, parmak izi, elin damar ağı, vb.) tercih

edilen biyometrik veri türünün veya türlerinin diğerleri yerine neden seçildiğine dair gerekçeler ve belgelerin sunulması, KVKK'nın 4 üncü maddesinin birinci fıkrasının (d) bendinde yer alan ilgili mevzuatta öngörülen veya işlendikleri amaç için gerekli olan süre kadar muhafaza edilme ilkesi gereği, kişisel verilerin işlenmesinde azami süre belirlenmesi, bu kapsamda sürelerin belirlenmesinde mevzuattan kaynaklanan süreler olabileceği gibi, mevzuat kaynaklı olmayan ancak veri sorumlularının tayin edeceği süreler de olabileceği, bununla birlikte, biyometrik özelliğin bütün çeşitleri (ham ve türetilmiş vb. kayıtlar) gereken süre boyunca işlenmesi; söz konusu verilerin ne kadar süre boyunca tutulacağı nedenleri ile birlikte kişisel veri saklama ve imha politikasında veri sorumlusu tarafından açıklanması gerektiği ifade edilmiştir.

- Rehber'in son bölümünde biyometrik veriler bakımından alınması gereken idari ve teknik tedbirler detaylı olarak paylaşılmıştır.

İlgili güncellenen Rehber'e buradan ulaşabilirsiniz.

Siber Güvenlik Kanunu 19 Mart 2025 tarihinde Resmî Gazetede yayımlanarak yürürlüğe girmiştir.

Siber Güvenlik Kanunu 19 Mart 2025 tarihinde Resmi Gazete'de yayımlanarak yürürlüğe girmiş olup 7545 sayılı Siber Güvenlik Kanunu; siber saldırılar, veri sızıntıları ve dijital güvenliğe ilişkin kapsamlı yaptırımlar öngörmektedir. Siber Güvenlik Kanunu uyarınca; siber uzayda kişisel veya kurumsal verilerin yetkisiz paylaşımı, kritik altyapıların korunmaması, yükümlülüklere uyulmaması gibi birçok fiile ilişkin hapis cezaları ve idari yaptırımlar düzenlenmiştir. Söz konusu Kanun kapsamında; öngörülen izin ve onaylar alınmaksızın faaliyette bulunanlar hakkında 2 ila 4 yıl arasında hapis cezası ve 1000 ila 2000 gün adli para cezası uygulanabileceği belirtilmiştir. Ayrıca, kamu kurumlarına bildirimi yapılmayan güvenlik açıkları ve siber olaylara karşı da 1.000.000 TL'den 10.000.000 TL'ye kadar idari para cezaları öngörülmektedir.

İlgili Siber Güvenlik Kanunu metnine buradan ulaşabilirsiniz.

KVK Kurumu tarafından Ödeme ve Elektronik Para Sektöründe Kişisel Verilerin Korunmasına İlişkin İyi Uygulamalar Rehberi yayımlanmıştır.

Bireylerin para havalesi hizmetleri, POS hizmetleri, fatura aracılık hizmetleri ve mobil ödeme hizmetleri gibi hizmetlerden yararlanırken kişisel verilerinin korunması ve başta elektronik para kuruluşları, POS hizmeti veren kuruluşlar, mobil ödeme hizmeti sunan kuruluşlar, fatura ödemeye aracılık eden kuruluşlar ve para havalesine aracılık eden kuruluşlar olmak üzere sektörde faaliyet gösteren veri sorumlularına yol gösterilmesi amacıyla KVK Kurumu ve Türkiye Ödeme ve Elektronik Para Kuruluşları Birliği ile yapılan ortak çalışmalar neticesinde Ödeme ve Elektronik Para Sektöründe Kişisel Verilerin Korunmasına İlişkin İyi Uygulamalar Rehberi **("Rehber")** yayımlanmıştır. Bu Rehber'de şu hususlar dikkat çekmektedir:

İlgili duyuruya buradan ulaşabilirsiniz.

KVK Kurumu tarafından iş yerinde kişisel verileri korumaya yönelik bazı öneriler yayımlanmıştır.

KVK Kurumunun LinkedIn hesabından iş yerinde kişisel verilerin korunmasına özen göstermek amacıyla bazı öneriler yayımlanmıştır.

- Güvenlik açıklarının tespit edilmesi,
- Mevcut politika ve prosedürlerin gözden geçirilmesi,
- Tüm cihazların şifrelenmesi,
- Yetkilendirme kurallarının belirlenmesi, bu kapsamda çalışanların yalnızca ihtiyacı bulunan dosyalara erişim sağlaması,

- Yazılım ve işletim sistemlerinin güncel tutulması,
- Her biri için ayrı parola kullanarak ayrı wi-fi ağları oluşturulması,
- Güçlü parolalar kullanılmalı,
- Çalışanlara KVKK ve siber güvenlik eğitimi verilmesi,
- Sistem dışında bir sistem yedeklemesi yapılması ve bu yedeklemeye yalnızca sistem yöneticisinin ulaşması.

İlgili önerilere buradan ulaşabilirsiniz.

KVK Kurumu tarafından aktif rıza yöntemine yönelik bazı bilgiler yayımlanmıştır.

KVK Kurumunun LinkedIn hesabından aktif rıza yöntemine ilişkin bazı bilgiler yayımlanmıştır. Bunlar;

- "Aktif rıza yöntemi" (opt-in) seçeneği sunulmayıp sadece "pasif rıza yöntemi" (opt-out) seçeneği sunularak, ilgili kişinin kişisel verilerinin işlenmesi durumunda hukuka uygun bir işlemeden bahsedilmektedir.
- Opt-in; önceden seçili olarak sunulmayan ve ilgili kişinin aktif bir hareketi ile onay vermesini gerektiren bir rıza yöntemi iken, opt-out; ilgili kişinin aktif bir hareketi olmaksızın, önceden seçili olarak sunulan ve bu doğrultuda kişisel verilerinin işlendiğini gösteren bir rıza yöntemidir.
- Örneğin; "Kampanyalardan haberdar olmak ister misiniz?" sorusuna ilişkin kutucuğun seçili olmaksızın ilgili kişiye sunulması ve "Evet" kutucuğunun ilgili kişi tarafından işaretlenmesi halinde opt-in yöntemi, bu kutucuğun seçili olarak ilgili kişiye sunulması ve "Evet" kutucuğunda yer alan işaretlemenin ilgili kişi tarafından kaldırılması halinde opt-out yöntemi kullanılmış olmaktadır.
- Geçerli bir açık rızadan bahsedebilmek için aktif rıza yöntemi, yani opt-in şeklinde bir seçim sunulması gerektiğinden, opt-out seçeneği sunularak kişisel verilerin işlenmesi halinde, hukuka uygun bir kişisel veri işleme faaliyetinden bahsedilemeyecektir.

İlgili yazıya buradan ulaşabilirsiniz.

KVK Kurumu tarafından sahte internet sitelerine yönelik bazı önlemler yayımlanmıştır.

KVK Kurumunun LinkedIn hesabından sahte internet sitelerine yönelik bazı önlemler ve dikkat edilmesi gereken hususlar yayımlanmıştır. Bunlar;

- Gerçek mağazalar veya satıcılar gibi görünmek üzere tasarlanmış sahte internet sayfalarına karşı dikkatli olunması gerekmektedir.
- Bazen tek bir harf yanlışlığı bile sizi kötü amaçlı internet sitelerine yönlendirebilmektedir. İnternet sitesinin doğruluğundan ve güvenli bağlantılar kullanıldığından emin olunması gerekmektedir.
- İşleminizle ilgisi bulunmayan bilgi taleplerine (parola, kart şifresi vb.) yanıt verilmemesi gerekmektedir.
- Çeşitli kurum ve kuruluşların logolarını kullanarak ödül veya hediye vaadiyle kaynağı belirsiz bağlantı ve uygulamalara yönlendiren şüpheli bağlantılara dikkat edilmesi gerekmektedir.
- Akıllı cihazınıza uzaktan erişim sağlanması için gelen yönlendirmelere müsaade edilmemesi gerekmektedir.
- Alışveriş işlemlerinizden sonra hesap ve kart hareketlerinizi incelenmesi gerekmektedir.

İlgili yazıya buradan ulaşabilirsiniz.

KVK Kurumu tarafından fiziksel alışverişe yönelik bazı önlemler yayımlanmıştır.

KVK Kurumunun LinkedIn hesabından fiziksel alışverişe yönelik bazı önlemler ve dikkat edilmesi gereken hususlar yayımlanmıştır. Bunlar;

- Gereğinden fazla bilgi paylaşımından kaçınılmalıdır.
- Sadakat kart programına dahil olmanın veya olmamanın tamamen kendi tercihinize bağlı olduğunu ve her iki durumda da alışveriş yapma imkanınızın ortadan kaldırılamayacağını unutmamanız önerilmektedir.
- Size bir form sunuluyorsa, kabul etmeden önce içeriğini okuyunuz. Anlam veremediğiniz bir husus var ise sorgulanması önerilmektedir.
- Banka kartınız sizden uzak bir yere götürülmek isteniyorsa, buna müsaade edilmemelidir.
- Üzerinde isim, adres, telefon numarası veya buna benzer bilgilerinizin yer aldığı belgeleri (fatura, fiş vb.) başkalarının erişemeyeceği şekilde muhafaza edilmelidir.

İlgili yazıya buradan ulaşabilirsiniz.

KVK Kurumu tarafından seyahat ve konaklama süreçlerinde kişisel verilerin korunmasına yönelik bazı önlemler yayımlanmıştır.

KVK Kurumunun LinkedIn hesabından seyahat ve konaklama süreçlerinde kişisel verilerin korunmasına yönelik bazı önlemler yayımlanmıştır. Bunlar;

- E-postalar ve mesajlarla gelen sahte rezervasyon veya promosyon bildirimlerine karşı dikkatli olunmalıdır *(Bu tür mesajlar kimlik avı amacı taşıyabilmektedir. Doğrudan ilgili firmanın resmi internet sitesinden veya diğer resmi iletişim kanallarından olup olmadığını kontrol ediniz.).*
- Üzerinde T.C. kimlik numarası, PNR kodu ve benzeri bilgiler bulunan biniş kartınızın veya biletinizin görüntüsünü sosyal medyada paylaşılmamalıdır *(Bu tür belgelerde yer alan bilgiler kötü niyetli kişiler tarafından kullanılabilir.).*
- Rutin işlemler esnasında kişisel bilgilerinizi paylaşırken aydınlatma metinlerine göz atılmalıdır. Gerek görmeniz durumunda detaylı bilgi ve açıklama talep edilmelidir.
- Sosyal medya paylaşımlarında zamanlama ve içerik açısından dikkatli olunmalıdır *(Tatil süresince evde olmadığınızın anlaşılacağı paylaşımlar güvenliğinizi riske atabilir.).*
- Bankacılık ve sağlıkla ilgili işlemleriniz söz konusu ise bu tür işlemlerinizi güvenliğinden emin olduğunuz bağlantı ve cihazlar üzerinden gerçekleştirmelidir *(Şüpheli internet bağlantıları üzerinden yapılan hassas işlemler, kişisel verilerinizin ele geçirilmesine sebep olabilir.).*
- Akıllı cihazlarınızın güvenlik parolalarını gözden geçirerek güçlü parolalar belirlenmelidir *(Zayıf parolalar, cihazınızdaki kişisel verilere yetkisiz erişim riskini artırır. Harf, rakam ve semboller içeren güçlü parolalar kullanmanız güvenlik düzeyini artıracaktır.).*
- Kaybolan ya da unutulan cihazlar için uzaktan silme veya kilitleme özelliklerini aktif hale getirilmelidir *(Özellikle mobil cihazlarda "Cihazımı Bul" veya benzeri güvenlik özelliklerini kullanmanız faydalı olabilir.)*

İlgili yazıya buradan ulaşabilirsiniz.

KVK Kurumu tarafından idari para cezalarının tebliğinde hazine ve maliye bakanlığı gelir idaresi başkanlığının e-tebligat uygulamasının kullanılması hakkında kamuoyu duyurusu yayımlanmıştır.

KVK Kurumunun resmi internet sitesinde yayımlanan duyuru doğrultusunda, idari para cezaları muhatabı veri sorumlularına Hazine ve Maliye Bakanlığı Gelir İdaresi Başkanlığının E-Tebligat uygulamasına ait altyapı kullanılarak tebliğ edilecektir. Ancak E-tebligat sistemi üzerinde vergi mükellefiyet kaydı bulunmayan veya kaydı

silinen veri sorumluları açısından tebliğ işlemleri 7201 sayılı Tebligat Kanunu hükümlerine göre yürütülmeye devam edecektir.

İlgili duyuruya buradan ulaşabilirsiniz.

KVK Kurumu tarafından çocukların çevrimiçi ortamda kişisel verilerin korunmasına yönelik bazı önlemler yayımlanmıştır.

KVK Kurumunun LinkedIn hesabından çocukların çevrimiçi ortamda kişisel verilerin korunmasına yönelik bazı önlemler yayımlanmıştır. Bunlar;

- Çevrimiçi ortamlarda çocukların kişisel verilerinin ve mahremiyetlerinin korunması, ebeveynlerin bilinçli yönlendirmesiyle şekillenen bir farkındalık ve rehberlik sürecidir.
- Kişisel veri, mahremiyet, istenmeyen e-posta ve çevrimiçi güvenlik gibi konulara ilişkin olarak çocuklarını yaşlarına uygun şekilde bilgilendirmeleri,
- Çocuklara yönelik kişisel veri işleyen ürün ve hizmetlerin bilgilendirici metinlerini dikkatli bir şekilde incelemeleri,
- Çocuklarının kişisel verilerini (özellikle; fotoğraf, video, konum bilgisi vb.) çevrimiçi ortamlarda herkese açık şekilde paylaşmaktan kaçınmaları,
- Güçlü ve tahmin edilmesi zor parolalar kullanmaları, çocuklarını da güçlü parola oluşturma ve parola güvenliği konusunda bilinçlendirmeleri,
- Çocuklarının kullandığı bilgisayar, cep telefonu, tablet veya oyun konsollarında internet filtreleme, ebeveyn denetimi ve güvenlik duvarı gibi koruyucu teknolojilerden yararlanmaları,
- Çocuklarının sosyal medya kullanımını yaşlarına uygun şekilde denetlemeleri ve gizlilik ayarlarını birlikte gözden geçirmeleri,
- Tanımadıkları kişilerle iletişime geçmemeleri ve bu kişilerden gelen mesaj, bağlantı ya da talepler karşısında temkinli olmaları gerektiği konusunda çocuklarını bilgilendirmeleri,
- Siber zorbalık ve dijital şiddet gibi riskler hakkında çocuklarına bilgi vermeleri ve bu tür durumlarla karşılaştıklarında güvenle kendilerine başvurabilecekleri bir iletişim ortamı oluşturmaları.

İlgili yazıya buradan ulaşabilirsiniz.

KVK Kurumu tarafından idari para cezalarının tebliğinde hazine ve maliye bakanlığı gelir idaresi başkanlığının e-tebligat uygulamasının kullanılması hakkında kamuoyu duyurusu yayımlanmıştır.

KVK Kurumunun resmi internet sitesinde yayımlanan duyuru doğrultusunda, idari para cezaları muhatabı veri sorumlularına Hazine ve Maliye Bakanlığı Gelir İdaresi Başkanlığının E-Tebligat uygulamasına ait altyapı kullanılarak tebliğ edilecektir. Ancak E-tebligat sistemi üzerinde vergi mükellefiyet kaydı bulunmayan veya kaydı silinen veri sorumluları açısından tebliğ işlemleri 7201 sayılı Tebligat Kanunu hükümlerine göre yürütülmeye devam edecektir.

İlgili duyuruya buradan ulaşabilirsiniz.

KVK Kurumu tarafından Kamu Kurumlarına Yönelik Kurumsal Sosyal Medya Kullanım Rehberi yayımlanmıştır.

KVK Kurumunun resmi internet sitesinde yayımlanan Rehber doğrultusunda aşağıdaki hususlar belirtilmiştir;

- Sosyal medya hesaplarının güvenliği için gerekli önlemler alınmalı, şüpheli hesaplardan ve bağlantılardan uzak durulmalı, tanınmayan kişilerden gelen istekler kabul edilmemelidir.

- Sosyal medyada yüzde yüz güvenlik söz konusu değildir. Bu nedenle nüfus cüzdanınızın fotoğrafı, kimlik numaranız, annenizin evlenmeden önceki soyadı gibi kişisel bilgilerinizi mesajlaşma ve sosyal medya uygulamaları aracılığıyla kesinlikle paylaşılmamalıdır.
- Kişisel verilerin korunması ve gizliliğine özen gösterilmeli, ilgili mevzuata uygun hareket edilmelidir.
- Kamu kurumları, sosyal medya paylaşımlarında hukuki sorumluluklarını bilmeli ve bu doğrultuda hareket etmelidir. Özellikle telif hakları, kişilik hakları ve kamu güvenliği gibi konularda dikkatli olunmalıdır. Sosyal medya hesaplarının kullanımı, etkileşimi ve paylaşımları hususlarında özellikle; 6698 Sayılı Kişisel Verilerin Korunması Kanunu, 5846 Sayılı Fikir ve Sanat Eserleri Kanunu, İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun, Türk Ceza Kanunu, Kamu Görevlileri Etik Davranış İlkeleri ile Başvuru Usul ve Esasları Hakkında Yönetmelik, 2019/12 Sayılı Cumhurbaşkanlığı Bilgi ve İletişim Güvenliği Tedbirleri Genelgesi başta olmak üzere kanun ve diğer mevzuat hükümlerine uyulması gerekmektedir.
- Kişisel verilere ilişkin mevzuata uygun hareket edilmeli, özel hayatın gizliliği korunmalıdır.

İlgili Rehbere buradan ulaşabilirsiniz.

KVK Kurumu tarafından yayımlanan birçok eski rehber güncellenmiştir.

KVK Kurumunun resmi internet sitesinde yayımlanan Rehber doğrultusunda aşağıdaki rehberler güncellenmiştir;

- Seçim Faaliyetlerinde Kişisel Verilerin Korunması Rehberi
- Türkiye Cumhuriyeti Kimlik Numaralarının İşlenmesi Hakkında Rehber
- Kişisel Verilerin Korunmasına İlişkin Bankacılık Sektörü İyi Uygulamalar Rehberi
- Unutulma Hakkı (Unutulma Hakkının Arama Motorları Özelinde Değerlendirilmesi)
- Yapay Zekâ Alanında Kişisel Verilerin Korunmasına Dair Tavsiyeler
- Kişisel Veri İşleme Envanteri Hazırlama Rehberi
- Aydınlatma Yükümlülüğünün Yerine Getirilmesi Rehberi
- 100 Soruda Kişisel Verilerin Korunması Kanunu
- Kişisel Verilerin Korunması Kanununa İlişkin Uygulama Rehberi
- Kişisel Veri Güvenliği Rehberi (Teknik Ve İdari Tedbirler)
- Kişisel Verilerin Silinmesi, Yok Edilmesi Veya Anonim Hale Getirilmesi Rehberi
- Kişisel Verilerin Korunması Kanunu Hakkında Sıkça Sorulan Sorular

İlgili Rehberlere buradan ulaşabilirsiniz.

KVK Kurumu tarafından yayımlanan yapay zeka teknolojilerine ilişkin akademik bakış ismiyle bir e-kitap yayımlanmıştır.

KVK Kurumunun resmi internet sitesinde yayımlanan e-kitap doğrultusunda yapay zeka teknolojileri KVKK perspektifinden çeşitli akademisyenler tarafından incelenmiştir.

İlgili e-kitaba buradan ulaşabilirsiniz.

KVK Kurumu tarafından yayımlanan kişisel verilerin korunması terimler sözlüğü yayımlanmıştır.

KVK Kurumunun resmi internet sitesinde yayımlanan sözlük doğrultusunda KVKK uyarınca kullanılan pek çok terim açıklaması eklenmiştir. Terimler açıklanırken; AB 2019/1024 sayılı Açık Veri Direktifi, 6698 sayılı Kişisel Verilerin Korunması Kanunu, T.C. Cumhurbaşkanlığı Dijital Dönüşüm Ofisi – Blok zincir Sözlüğü, KVK Kurumu tarafından yayımlanan çeşitli dokümanlar ve rehberler, Veri Sorumluları Sicili Hakkında Yönetmelik, AB

2015/1535 sayılı Direktif, AB 2023/2854 sayılı Tüzük, GDPR, EDPS Glossary, IAPP AI Governance Center – Key Terms for AI Governance, ISO/EIC 22989:2022, NIST Glossary, AB Yapay Zeka Yasası, T.C. Cumhurbaşkanlığı Dijital Dönüşüm Ofisi – Bilgi ve İletişim Güvenliği Rehberi, OECD – Dark Commercial Patterns, Avrupa Konseyi – AI Glossary, EDPS TechSonar:Metaverse, FTC – IOT: Privacy & Security in a Connected World, NIST – Small Business Cybersecurity Fact Sheet:Phishing, OECD – Glossary of Statistical Terms, NIST – Guide to IPsec VPNs, Siberay Sözlük, UNICEF – Siber Zorbalık: Nedir ve Nasıl Önlenir vb. çeşitli kaynaklardaki terimler doğrudan çevrilmiştir.

İlgili sözlüğe buradan ulaşabilirsiniz.

DÜNYADAKİ GELİŞMELER

DUYURULAR VE HABERLER

ABD Ulusal Standartlar ve Teknoloji Enstitüsü ("NIST") tarafından diferansiyel mahremiyet hakkında rehber yayımlamıştır.

NIST, bu rehber kapsamında verilerin bir bütün halinde tutulması ile mahremiyete ilişkin sorunlara dikkat çekerek her türlü geçmişe sahip uygulayıcıların farklı özel yazılım çözümleri ile diferansiyel mahremiyet hakkında bilgi sahibi olmasına destek olmayı amaçlamakta olduğu belirtilmiştir.

İlgili rehbere buradan ulaşabilirsiniz.

EPRS tarafından Birleşik Krallık yeterlilik kararının 27 Haziran 2025 tarihinde sonlanmasına ilişkin bildiri yayımlanmıştır.

EPRS, Avrupa Komisyonunun 27 Haziran 2025'e kadar yenilemesi gereken AB-Birleşik Krallık veri aktarımı yeterlilik kararına ilişkin bir değerlendirme raporu yayımlanmıştır.

Raporda, Birleşik Krallık'ın yürürlükteki ve planlanan yasal düzenlemelerinin – özellikle Veri Kullanımı ve Erişimi Yasa Tasarısı ile 2024 tarihli Gözetim Yetkileri Değişiklik Yasası'nın – kişisel verilerin güvenli aktarımına ilişkin AB standartlarıyla uyumunu zedeleyebileceği vurgulandı. Bu reformların, özellikle yapay zekâ, otomatik karar verme ve kamu yetkililerinin veri erişim yetkileri alanlarında şeffaflık ve hesap verebilirlik ilkelerini zayıflatabileceği kaydedildi. Yeterlilik kararının yenilenmemesi hâlinde, AB'den Birleşik Krallık'a yapılan veri transferlerinin ciddi ölçüde zorlaşabileceği ve şirketlerin daha maliyetli alternatif aktarma mekanizmalarına yönelmek zorunda kalabileceği ifade edilmektedir.

İlgili bildirime buradan ulaşabilirsiniz.

Avrupa Veri Koruma Kurulu ("EDPB") tarafından, yolcu kayıt verilerinin kullanımına ilişkin Avrupa Birliği Adalet Divanı'nın ("ABAD") kararının değerlendirmesi yayımlanmıştır.

EDPB, ABAD'ın 21 Haziran 2022 tarihli kararının ardından, yolcu kayıt verilerinin (PNR) işlenmesine ilişkin olarak üye devletlerce atılması gereken adımlara dair ayrıntılı bir değerlendirme yayımlanmıştır. ABAD kararında, PNR Direktifi'nin geçerliliği korunmakla birlikte, bireylerin özel hayatına saygı ve kişisel verilerin korunması haklarına yönelik ciddi müdahaleler yaratabileceği belirtilmiş ve bu nedenle PNR verilerinin işlenmesine yalnızca sıkı koşullar altında izin verilmesi gerektiği vurgulanmıştır.

EDPB açıklamasında, PNR verilerinin yalnızca terör suçları ve ciddi suçlarla doğrudan veya dolaylı bir bağlantısı olan durumlarda işlenebileceği, sıradan suçlar için sistemin kullanılamayacağı ve her bir veri işleme faaliyetinde "nesnel bir bağlantı"nın kanıtlanmasının zorunlu olduğu ifade edilmiştir. Ayrıca intra-AB uçuşlar gibi durumlarda

da, veri işlemenin yalnızca mevcut, ciddi ve somut bir tehdit bulunması hâlinde ve sınırlı bir süre için geçerli olabileceği belirtilmiştir.

EDPB ayrıca, veri işleme sürelerine, otomatik değerlendirme sistemlerine getirilen sınırlamalara ve bağımsız ön denetim mekanizmalarına dikkat çekerek, üye devletlerin hem ulusal mevzuatlarını hem de uygulamalarını ABAD kararı doğrultusunda acilen güncellemeleri gerektiğini ifade etmiştir.

İlgili açıklamaya buradan ulaşabilirsiniz.

Uluslararası Gizlilik Uzmanları Birliği ("IAPP") tarafından fidye yazılımı saldırılarına karşı eylem rehberi yayımlanmıştır.

IAPP, kuruluşların fidye yazılımı saldırılarına maruz kaldıklarında izlemeleri gereken adımlara ilişkin on maddelik bir eylem rehberi yayımlamıştır. Rehber, olay müdahalesinden veri yedeklerinin güvenliğine, iletişim stratejilerinden yasal yükümlülüklere kadar geniş bir yelpazede yönlendirme sağlamaktadır.

Rehberde öne çıkan temel adımlar arasında etkilenen sistemlerin ağdan izole edilmesi, yedekleme altyapısının korunması, iç ve dış paydaşlarla koordinasyon sağlanması, olayın iş sürekliliği üzerindeki etkisinin değerlendirilmesi, kolluk kuvvetleriyle iş birliği yapılması ve iyileşme stratejisinin devreye alınması yer almaktadır.

Rehber ayrıca, ihlal sonrası bildirim yükümlülükleri ve hukuki değerlendirmeler konusunda da yol gösterici nitelikte olup, olayın belgelenmesi ve sonraki süreçler için öğrenilen derslerin kurumsallaştırılmasına dikkat çekmektedir.

İlgili rehbere buradan ulaşabilirsiniz.

Fransa Veri Koruma ve Rekabet Otoriteleri tarafından, Kişisel Veri ve Rekabet Hukuku arasındaki etkileşime dair ortak çalışma yayımlanmıştır.

Fransa Veri Koruma Otoritesi ("**CNIL**") ile Rekabet Otoritesi, kişisel verilerin korunması ile rekabet hukuku arasındaki kesişim alanını daha iyi anlamak ve bu iki alan arasında uyumlu bir iş birliği geliştirmek amacıyla ortak bir rapor yayımladı. Raporda, CNIL'in eski başkanı ve mevcut üyesi Bruno Lasserre tarafından yürütülen özel misyonun sonuçlarına yer verilmiştir.

Rapor, veri koruma ve rekabetin dijital ekonomide artık ayrı alanlar olarak ele alınamayacağına işaret ederken; bu iki düzenleyici çerçevenin kavramsal yakınlığını ortaya koymakta ve düzenleyici kurumların birlikte çalışmasının hem bireylerin hakları hem de piyasa özgürlüğü açısından önemine vurgu yapmaktadır. CNIL'in düzenleyici uygulamalarına yönelik 15 somut öneri sunulmuş ve ekonomik analizlerin daha etkin biçimde veri koruma kararlarına entegre edilmesi çağrısında bulunulmuştur.

Ayrıca, CNIL ve Rekabet Otoritesi arasında kavramsal ve operasyonel iş birliğinin artırılması, ortak pazar analizleri yapılması, ekonomik aktörlere yönelik daha net yönlendirmelerin geliştirilmesi ve Avrupa düzeyinde koordinasyonun güçlendirilmesi önerilmiştir.

İlgili çalışmaya buradan ulaşabilirsiniz.

Çin, yüz tanıma teknolojisine ilişkin yeni güvenlik kurallarını açıklamıştır.

Çin Siber Uzay İdaresi, yüz tanıma teknolojilerinin kullanımına yönelik yeni güvenlik düzenlemelerini kamuoyuna sunmuştur. 1 Haziran 2025'te yürürlüğe girecek kurallar kapsamında, bireylerin açıkça bilgilendirilmesi, rızalarının alınması ve veri koruma etki değerlendirmesi yapılması zorunlu hale getirildi. Düzenlemeler, yüz tanıma uygulamalarının daha şeffaf ve denetlenebilir olmasını amaçlamaktadır.

İlgili düzenlemelere buradan ulaşabilirsiniz.

Norveç, AB Yapay Zekâ Tüzüğü kapsamında AI Norway adlı ulusal denetim otoritesi kurduğunu açıklamıştır.

Norveç Hükümeti, Avrupa Birliği'nin Yapay Zekâ Tüzüğü'nün (AI Act) uygulanmasına hazırlanmak amacıyla ulusal düzeyde yeni bir yönetişim yapısı kurmaktadır. Bu kapsamda, "AI Norway" adlı bir ulusal yapay zekâ merkezi, yenilikçi ve sorumlu yapay zekâ kullanımını teşvik etmek üzere Norveç Dijitalleşme Ajansı (Digdir) bünyesinde faaliyete geçirilecektir.

Dijitalleşme ve Kamu Yönetimi Bakanı Karianne Tung tarafından duyurulan yeni yapılanma, kamu, özel sektör ve akademi arasında işbirliğini teşvik etmeyi, etik yapay zekâ çözümlerinin geliştirilmesini desteklemeyi ve AB ile eşgüdüm içinde düzenlemelerin uygulanmasını sağlamayı amaçlıyor. AI Norway aynı zamanda şirketler için "AI Sandbox" ortamı sunarak, yapay zekâ sistemlerinin güvenli biçimde test edilmesini ve geliştirilmesini mümkün kılacaktır.

Yapay Zekâ Tüzüğü kapsamındaki denetim ve gözetim görevleri ise Norveç İletişim Kurumu'na (Nkom) verildi. Nkom, Norveç'te yapay zekâ sistemlerinin güvenli ve sorumlu şekilde kullanıldığından emin olmakla yükümlü olacak ve AB kurumlarıyla temas noktası olarak hareket edecektir.

Ayrıca, AB düzenlemeleri uyarınca sistem sertifikasyon ve akreditasyon süreçlerinden sorumlu kurum olarak Norveç Akreditasyon Kurumu (Norsk akkreditering) görevlendirilmiştir.

İlgili habere buradan ulaşabilirsiniz.

Avrupa Veri Koruma Kurulu ("EDPB") 2024 Yıllık Raporunu yayınlamıştır.

Rapor, EDPB'nin 2024'te yürüttüğü çalışmalara genel bir bakış sunmuştur. EDPB tarafından yayımlanan söz konusu rapor kapsamına 2024 yılında yapılan çalışmalara değinilmiştir.

Bu yıllık raporda; EDPB'nin 2024 yılında gerçekleştirdiği çalışmalara genel bir bakış, 2024-2027 stratejisinin kabulü, 64(2). Madde kapsamındaki görüşlerin artışı ile rehberlik ve hukuki danışmanlık sağlama yönündeki devam eden çalışmalar gibi konu başlıklarına yer verilmektedir.

İlgili yıllık rapora buradan ulaşabilirsiniz.

Avrupa Veri Koruma Kurulu ("EDPB") Blokchain Teknolojileri Yoluyla Kişisel Verilerin İşlenmesine İlişkin bilgilendirme yazısı yayımlamıştır.

Blokchain teknolojilerinin kullanımının giderek artması nedeniyle EDPB, bu teknolojileri kullanan kuruluşlara yardımcı olması amacıyla kabul edilen yönergelere yönelik bilgilendirme yazısı yayınlanmıştır. Yönergeler kapsamında EDPB; blokzincirlerin nasıl çalıştığını açıklamakta, farklı olası mimarileri değerlendirmekte ve bunların kişisel verilerin işlenmesine etkilerini ele almaktadır. Yönergeler, veri minimizasyonuna ve kişisel verilerin işlenmesi ile saklanmasına yönelik farklı teknik örnekler sunulmaktadır.

1. Blokchainler, işlemleri doğrulayabilen ve belirli bir zamanda dijital bir varlığın (örneğin kripto para) kime ait olduğunu tespit edebilen dağıtık dijital defter sistemidir.
2. Blokchainler, verilerin bütünlüğünü ve izlenebilirliğini sağlayarak güvenli bir şekilde işlenmesini ve aktarılmasını destekleyebilir.

Ayrıca EDPB, son genel kurul toplantısında Yapay Zekâ Yasası ile AB veri koruma mevzuatı arasındaki ilişkiye dair yönergelerin hazırlanmasında Yapay Zekâ Ofisi ile yakın iş birliği yapma kararı da almıştır.

Söz konusu yönergeler, 9 Haziran 2025 tarihinde kamuoyunun da görüşünü almak için halka açılacaktır.

İlgili bilgilendirme yazısına buradan ulaşabilirsiniz.

Avrupa Parlamentosu Araştırma Servisi (“EPRS”) tarafından çevrimiçi ortamda çocukların korunmasını amaçlayan çalışma yayımlanmıştır.

Avrupa Birliği, çocukların çevrimiçi ortamda korunmasını amaçlayan çeşitli yasa ve girişimler uygulamaya koymuştur. Bu önlemler, çocukların dijital ortamı güvenli bir şekilde keşfetmesine yöneliktir.

Alınan önlemler arasında dijital hizmetler, görsel-işitsel medya hizmetleri ve veri koruma konularında düzenlemeler yer almakta; ayrıca zararlı veya yasa dışı içeriklerin bildirilmesi için yardım hatları ve ihbar hatları gibi araçlar sunulmaktadır. Ayrıca, AB güvenilir bir yaş doğrulama yöntemi sunmayı amaçlayan dijital kimlik çerçevesini hayata geçirmiştir; böylece çocukların yaşlarına uygun olmayan içeriklere erişimini önlenmeyi hedeflemektedir.

İlgili EPRS çalışmasına buradan ulaşabilirsiniz.

GÜNCEL KARARLAR

ABD Federal Ticaret Komisyonu, Avast’ın veri satışı nedeniyle mağdur kullanıcılara tazminat ödenmesine karar vermiştir.

ABD Federal Ticaret Komisyonu (FTC), antivirüs yazılımı geliştiricisi Avast’ın, kullanıcılarının çevrim içi etkinlik verilerini koruyacağı iddiasıyla pazarladığı ürünler aracılığıyla detaylı gezinme verilerini üçüncü taraflara sattığını tespit etmiştir. FTC’nin Şubat 2024 tarihli şikayeti üzerine taraflar arasında varılan uzlaşma kapsamında, Avast 16,5 milyon dolar tazminat ödemeyi kabul etti. Bu tazminat, 2014-2020 yılları arasında Avast yazılımı satın almış yaklaşık 3,7 milyon kullanıcıya iade edilmek üzere kullanılacak. Ayrıca Avast’ın, toplanan verilerin nasıl kullanıldığını yanıltıcı şekilde açıklaması ve bu verileri reklam amaçlı üçüncü taraflara satması yasaklanmıştır.

İlgili karara buradan ulaşabilirsiniz.

ABAD, otomatik karar alma sistemlerinde şeffaflık yükümlülüğüne ilişkin karar uygulamıştır.

ABAD, otomatik sistemlerle yapılan kredi değerlendirmelerine ilişkin önemli bir karar verdi. Avusturya’da bir mobil operatör, düşük kredi notu gerekçesiyle aylık 10 avroluk sözleşme talebini reddettiği bir müşteriye, bu kararın nasıl verildiğine dair yeterli bilgi sunmadı. Kararın temelini oluşturan algoritmik değerlendirme, Dun & Bradstreet Austria tarafından gerçekleştirilmiştir.

ABAD, veri sorumlusunun yalnızca algoritmayı açıklamasının yeterli olmayacağını, kullanılan kişisel verilerin nasıl işlendiği ve karar üzerindeki etkisinin veri sahibince anlaşılabilir şekilde açıklanması gerektiğini vurguladı. Mahkeme, ticari sır gerekçesiyle bilginin tamamen saklanamayacağını; böyle durumlarda ilgili bilginin denetim otoritesine veya mahkemeye sunulması gerektiğini belirtmiştir.

İlgili karara buradan ulaşabilirsiniz.

İspanya Veri Koruma Otoritesi, mobil operatör şirketine 1,2 milyon Euro ceza kararı uygulamıştır.

İspanya Veri Koruma Otoritesi (AEPD), bir mobil operatörün bayisi tarafından veri sahibinin bilgisi dışında çıkarılan yedek SIM kart sonucunda banka hesabından 9.000 Euro çalınmasına ilişkin soruşturma kapsamında operatöre toplam 1,2 milyon Euro idari para cezası uyguladı. Kararda, operatörün açık rıza olmaksızın SIM kart çoğaltarak GDPR madde 6(1)'i ihlal ettiği ve kimlik doğrulama sürecindeki eksiklikler nedeniyle GDPR madde 25 kapsamında veri koruma yükümlülüklerini yerine getirmediği belirtilmiştir.

İlgili karara buradan ulaşabilirsiniz.

İtalya Vergi Otoritesi'ne GDPR ihlali nedeniyle para cezası uygulamıştır.

İtalya Veri Koruma Otoritesi (Garante), vergi alacaklarının tahsili sürecinde, veri sahibine ait el koyma bildirimlerinin geçmişte kiracı olmuş ancak kira ilişkisi sona ermiş üçüncü kişilere iletilmesi nedeniyle vergi idaresi Agenzia delle Entrate'ye 40.000 Euro idari para cezası uygulanmıştır. Kararda, kiracılık ilişkisinin sona ermesine rağmen kişisel verilerin paylaşılmasının hem GDPR madde 5 hem de madde 6 hükümlerini ihlal ettiği ve yeterli teknik ve organizasyonel önlemlerin alınmadığı belirtilmiştir.

İlgili karara buradan ulaşabilirsiniz.

İspanya Veri Koruma Otoritesi, sağlık verisi sızıntısı ve DPIA eksikliği nedeniyle 2 milyon Euro ceza kararı uygulamıştır.

İspanya veri koruma otoritesi AEPD, IBERMUTUA adlı şirkete, bir bilgisayar hatası nedeniyle 3.395 kişinin sağlık verilerinin 354 yanlış alıcıya e-posta yoluyla gönderilmesi üzerine 1 milyon Euro idari para cezası verdi. Aynı otorite, bir başka kararında ise stadyumlara erişimde biyometrik kontrol uygulamadan önce veri koruma etki değerlendirmesi (DPIA) yapmayan LaLiga'ya da 1 milyon Euro para cezası uygulanmıştır.

İlgili karara buradan ulaşabilirsiniz.

İtalya Veri Koruma Otoritesi, Telekom şirketine izinsiz pazarlama nedeniyle ceza uygulamıştır.

İtalya Veri Koruma Otoritesi (Garante), Wind Tre isimli telekomünikasyon şirketine, kullanıcı rızası olmaksızın üçüncü taraflardan elde edilen iletişim bilgileriyle yürüttüğü pazarlama faaliyetleri, eksik veri işleme kayıtları ve yetersiz güvenlik önlemleri nedeniyle toplam 347.520 Euro idari para cezası uygulanmıştır. Kararda ayrıca, şirketin bir güvenlik açığı sonucu müşteri hesaplarının karışmasına yol açan veri ihlalini yetkili makamlara bildirmemesi de GDPR ihlali olarak değerlendirilmiştir.

İlgili karara buradan ulaşabilirsiniz.

İtalya Veri Koruma Otoritesi, eski çalışanın e-posta hesabının silinmemesi sebebiyle ceza kararı uygulamıştır.

İtalya Veri Koruma Otoritesi (Garante), işten ayrılan bir çalışanın kişisel e-posta hesabını yaklaşık dokuz ay boyunca aktif tutmaya devam eden ve silinmesi yönündeki taleplerine yanıt vermeyen Sicurnet Liguria s.r.l. şirketine 8.000 euro idari para cezası verilmiştir. Kararda, şirketin e-posta hesabını kapatmak yerine gelen iletileri başka bir kurumsal adrese yönlendirmesinin veri minimizasyonu, amaçla sınırlılık ve saklama süresi ilkelerini ihlal ettiği vurgulanmıştır.

İlgili karara buradan ulaşabilirsiniz.

İspanya Veri Koruma Otoritesi, konuklardan WhatsApp ile kimlik isteyen konaklama şirketine ceza uygulamıştır.

İspanya Veri Koruma Otoritesi (AEPD), bir konaklama şirketinin, misafirlerinden – aralarında çocukların da bulunduğu – kimlik belgelerini WhatsApp üzerinden kopya halinde talep etmesi nedeniyle 1.200 Euro idari para cezası verdi. Kurum, İspanya'daki mevzuatın yalnızca kimlik doğrulamasını zorunlu kıldığını; ancak kimlik kopyalarının saklanmasını öngörmediğini vurgulamıştır. Ayrıca şirketin kayıt sisteminin değiştirilerek artık kimlik kopyalarının talep edilmemesi ve daha önce alınan kopyaların sistemden silinmesi yönünde talimat verilmiştir.

İlgili karara buradan ulaşabilirsiniz.

Norveç Veri Koruma Otoritesi, Telekom şirketine veri koruma görevlisi organizasyonu nedeniyle ceza uygulamıştır.

Norveç Veri Koruma Otoritesi, Telenor ASA'nın veri koruma görevlisi (DPO) rolünü yeterli şekilde yapılandırmaması ve iç kontrol mekanizmalarının yetersiz olması nedeniyle şirkete 4 milyon Norveç kronu idari para cezası vermiştir. Kararda, DPO'nun üst yönetime doğrudan raporlama hattının kurulmadığı ve rolün bağımsızlığı ile çıkar çatışması ihtimaline ilişkin gerekli değerlendirmelerin yapılmadığı belirtildi. Şirketin DPO görevini sonlandırma kararı aldığı belirtilirken, otorite şirkete yeniden değerlendirme ve gerekli ise uygun organizasyonel tedbirleri alma yükümlülüğü getirmiştir.

İlgili karara buradan ulaşabilirsiniz.

Polonya Veri Koruma Otoritesi, seçim verilerinin yasa dışı kullanımı sebebiyle yerel kuruma ceza uygulamıştır.

Polonya Veri Koruma Otoritesi, 2020'de yalnızca posta yoluyla yapılması planlanan başkanlık seçimleri kapsamında PESEL veri tabanından yaklaşık 30 milyon Polonya vatandaşının kişisel verisinin hukuka aykırı şekilde işlenmesi nedeniyle Poczta Polska'ya 27 milyon PLN, Dijital İşler Bakanlığı'na ise 100.000 PLN idari para cezası vermiştir.

Kararda, seçim sürecine ilişkin yasal dayanak yürürlüğe girmeden önce başlatılan veri aktarımı işlemlerinin, veri minimizasyonu ve hukuka uygunluk gibi temel GDPR ilkelerini ihlal ettiği vurgulandı. Özellikle PESEL numarası, isim-soyisim, ikamet adresi gibi hassas bilgilerin, vatandaşlarla artık yasal ilişkisi kalmamış üçüncü taraflara açıklanmasının ciddi sonuçlar doğurduğu belirtilmiştir.

İlgili karara buradan ulaşabilirsiniz.

İtalya Veri Koruma Otoritesi, izinsiz pazarlama çağrıları ve konum takibi sebebiyle enerji şirketine ceza uygulamıştır.

İtalya veri koruma otoritesi Garante, 82 şikayetin ardından bir enerji şirketine, geçerli onay almadan gerçekleştirdiği pazarlama çağrıları ve üçüncü taraflarla uygunsuz veri paylaşımı nedeniyle 300.000 Euro idari para cezası vermiştir.

İlgili karara buradan ulaşabilirsiniz.

İngiltere Veri Koruma Otoritesi, fidye yazılımı saldırısı sonrası yazılım şirketine tedbirsizlik nedeniyle ceza vermiştir.

İngiltere veri koruma otoritesi ICO, sağlık sektörüne yazılım hizmeti sağlayan bir şirketin uğradığı fidye yazılımı saldırısı sonucunda 79.404 kişinin verilerinin sızması üzerine, yeterli teknik ve organizasyonel tedbir alınmadığı gerekçesiyle şirkete 3,07 milyon Sterlin ceza vermiştir.

İlgili karara buradan ulaşabilirsiniz.

Norveç Veri Koruma Otoritesi, DPO atama yükümlülüğüne uymayan şirkete ceza uygulamıştır.

Norveç veri koruma otoritesi, bir telekomünikasyon şirketine, GDPR kapsamında gerekli veri koruma görevlisini (DPO) usulüne uygun şekilde atamaması ve bu yükümlülüğü ihlal etmesi nedeniyle 4.000.000 NOK (yaklaşık 351.000 Euro) para cezası vermiştir.

İlgili karara buradan ulaşabilirsiniz.

İspanya Veri Koruma Otoritesi, sistem hatasıyla banka verilerine yetkisiz erişim sağlanması nedeniyle para cezası uygulamıştır.

İspanya veri koruma otoritesi AEPD, bir bankaya, sistem hatası nedeniyle bir müşterinin annesinin yetkisiz şekilde banka hesaplarına erişim sağlaması üzerine 3.500.000 Euro idari para cezası verdi. Olayda, bankanın yeterli kontrol mekanizmalarını kurmaması temel ihlal olarak değerlendirildi.

İlgili karara buradan ulaşabilirsiniz.

Birleşik Krallık Veri Koruma Otoritesi (Information Commissioner's Office veya ICO) AFK Letters Co aleyhine £ 90.000 idari para cezasına hükmedilmiştir.

AFK Letters, müşterileri adına geri ödeme ve tazminat talep eden bir işletmedir. Veri Koruma Otoritesi (''**DPA**''), AFK Letters Co'nun, Telefon Tercih Servisi (''**TPS**'') ve Kurumsal Telefon Tercih Servisi (''**CTPS**'') kaydedilmiş numaralara toplam 95.277 pazarlama araması yaparak, Gizlilik ve Elektronik İletişim Düzenlemeleri (''**PECR**'') Madde 21'i ihlal ettiğini tespit etmiştir.

DPA, söz konusu ihlali ciddi nitelikte değerlendirmiştir. İlgili dönemde yapılan pazarlama aramalarına ilişkin olarak bireylerden toplamda 22 şikayet alınmıştır.

Verilecek para cezasının belirlenmesinde, yapılan pazarlama aramalarının çoğunun TPS kayıtlı numaralara yapılmış olması ve soruşturma başladıktan sonra veri sorumlusuyla ilgili ek şikayetlerin alınmış olması belirleyici olmuştur.

DPA, AFK Letters Co'ya 90.000 £ tutarında para cezası vermiştir.

Kararın detaylarına buradan ulaşabilirsiniz.

İspanya Veri Koruma Otoritesi *(Agencia Española de Protección de Datos veya AEPD),* School Fitness aleyhine € 36.000 idari para cezasına hükmedilmiştir.

7 Şubat 2021 tarihinde, salon üyesi, fitness dersleri sırasında rızası olmadan film çekildiği için School Fitness'ın web sitesi üzerinden şikayette bulunmuştur. School Fitness, verdiği yanıtta, salon üyesinin üyelik sözleşmesini imzalayarak kaydedilen görüntülerin kullanılmasına onay verdiğini belirtti. Sözleşmede, üyelik sözleşmesini imzalayan üyelerin, şirketin kendi görüntülerini, fotoğraflarını, videolarını, ses kayıtlarını, grafiklerini vb. kullanmasına izin verdiği bir madde bulunmaktadır.

Ancak, 9 Mayıs 2023 tarihinde, salon üyesi, dersin kaydedildiğini fark etti, buna rağmen defalarca kaydedilmek istemediğini belirtti. Salon üyesi, e-posta yazışmasında bahsedilen sözleşme maddesinin haksız olduğunu düşündü ve 30 Mayıs 2023 tarihinde **AEPD (''İspanyol Veri Koruma Otoritesi'')'ne** şikayette bulundu.

AEPD'ye yapılan şikayet üzerine, School Fitness, iddiaları reddetti. Sözleşme imzalayan üyelerin, kaydedilmek için açıkça onay verdiğini ve kaydedilen materyalin tanıtım amaçlı dağıtılmasına rıza gösterdiğini belirtti. Ayrıca, dersler sırasında sözlü onay alındığını da iddia etti.

Sonuç olarak, School Fitness aleyhine €36.000 idari para cezasına hükmedilmiştir.

Kararın detaylarına buradan ulaşabilirsiniz.

Fransız Veri Koruma Otoritesi *("The French Supervisory Authority veya CNIL")* tarafından, KASPR aleyhine € 240.000 idari para cezasına hükmedilmiştir.

KASPR müşterilerine, bir bedel karşılığı LinkedIn üzerinden ziyaret edilen profillere ait profesyonel iletişim bilgileri sağlayan bir Chrome tarayıcı uzantısı pazarlayan bir şirkettir. Diğer websitelerinden toplamış oldukları veri tabanı üzerinden müşterilerine söz konusu bilgileri sağlamaktadır. Veri tabanında yaklaşık 160 milyon iletişim bilgisi bulunmaktadır.

CNIL, iletişim bilgileri edinilen kişiler tarafından birçok şikayet almıştır. Bunun üzerine yapılan soruşturmada birden fazla ihlal tespit edilmiştir. Bu ihlaller aşağıdaki gibidir:

- Hukuki dayanak yükümlülüğüne uyulmaması,
- Veri işleme amacına orantılı bir veri saklama süresi belirleme ve buna uyma yükümlülüğüne uyulmaması,
- Kişilere şeffaflık ve bilgi sağlama yükümlülüğüne uyulmaması,
- Bireylerin erişim hakkına uyulmaması.

Bu sayılan ihlaller sonucunda, KASPR aleyhine € 240.000 idari para cezasına hükmedilmiştir. Ayrıca iletişim bilgilerine görünürlük kısıtlaması getiren kullanıcıların verilerinin toplanmasının durdurulmasına, bu şekilde toplanan verilerin silinmesine, ilgili kişilere verilerinin toplandığına dair bilgilendirme yaparak buna itiraz edebilecekleri konusunda bilgi verilmesine, otomatik olarak saklamanın durdurulmasına ve bilgi almak isteyen ilgili kişilere eksiksiz olarak yanıt verilmesini emretmiştir.

Kararın detaylarına buradan ulaşabilirsiniz.

Hellenic SA tarafından, National Bank of Greece S.A aleyhine € 120.000 idari para cezasına hükmedilmiştir.

Yunanistan Ulusal Bankası, "i-bank Pay" uygulamasında, bir müşterinin banka hesabı yanlışlıkla başka bir müşterinin cep telefonu numarasıyla ilişkilendirilmiştir. Bu hata nedeniyle, "IRIS çevrimiçi ödeme hizmeti" üzerinden yapılan para transferleri, ikinci müşteriye gitmesi gerekirken birinci müşteri hesabına aktarılmıştır.

Gerçekleştirilen idari denetim kapsamında, Yunanistan Ulusal Bankası, söz konusu sorunun 2020 yılında mobil bankacılık uygulamasının güncellenmesi sırasında yapılan yanlış yapılandırmadan kaynaklandığını tespit etmiştir. Bu hata, diğer 24 müşterisini de etkilemiş olup, Banka durumu Veri İhlali Bildirimi ile Yetki Kurumu'na bildirmiştir. Ayrıca, Banka, durumu düzeltmek için ek önlemler almıştır.

ORANGE, reklam amaçlı e-postaları göstermek suretiyle; ilgili kişilerin rızası olmadan ticari pazarlama mesajları atması sebebiyle ve rızasını geri almış kullanıcıların çerezlerinin okunmaya devam etmesi sebebiyle GDPR hükümlerine uymamıştır.

İnceleme sonucunda Hellenic SA, Veri Sorumlusu olarak Yunanistan Ulusal Bankası'na, veri doğruluğu, bütünlüğü ve gizliliği ilkelerinin yanı sıra, veri koruma tasarımı ve varsayılan olarak veri koruma ilkelerinin ihlali nedeniyle 100.000 EUR tutarında idari para cezası uygulamıştır. Bu ceza, GDPR'nin Madde 32, 33 ve 34 hükümleri ile bağlantılı olarak verilmiştir. Ayrıca, şikâyetçilerin erişim hakkını ihlal ettiği için banka, 20.000 EUR tutarında bir idari para cezası daha almıştır.

Kararın detaylarına buradan ulaşabilirsiniz.