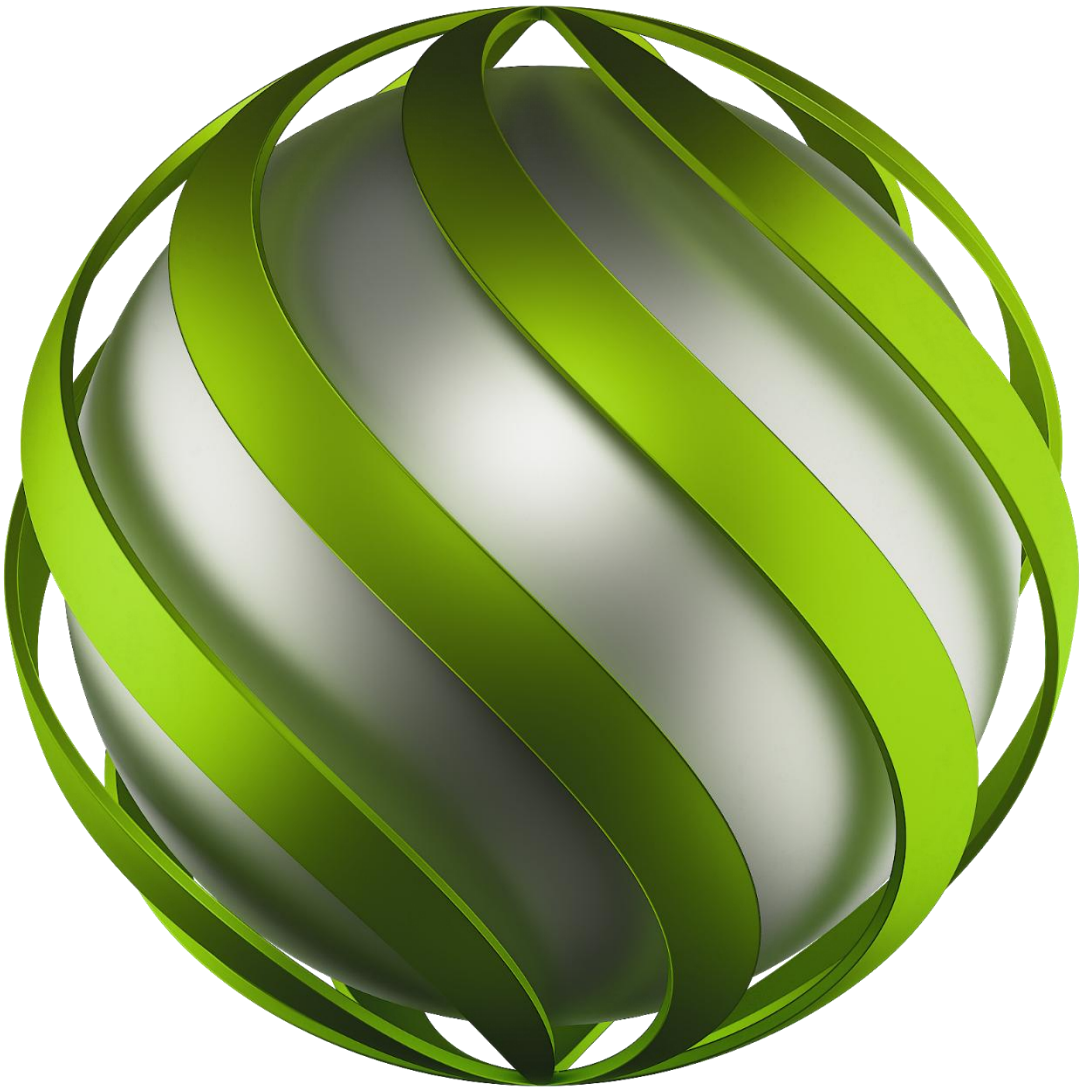
DL | Avukatlık Bürosu



Kişisel Verileri Koruma Hukuku Güncel Gelişmeler

Ocak – Şubat - Mart 2026

Türkiye'deki Gelişmeler

Veri İhlali Bildirimleri

Erciyes Üniversitesi tarafından Kişisel Verileri Koruma Kuruluna ("KVK Kurulu") bildirilen veri ihlali, 27.01.2026 tarihinde Kişisel Verileri Koruma Kurumunun ("KVK Kurumu") internet sitesinde yayımlanmıştır.

Veri sorumlusu Erciyes Üniversitesi tarafından KVK Kuruluna veri ihlali ("Veri İhlali" veya "İhlal") bildirilmiştir. Bildirimde aşağıdaki hususlar belirtilmiştir:

- İhlalin 26.12.2025 tarihinde başladığı ve 05.01.2026 tarihinde tespit edildiği,
- İlgili kişilere ait kişisel verilerin ele geçirilmesi ve veri sorumlusuna ait olmayan bir internet sitesinde yayınlanması neticesinde veri ihlalinin meydana geldiği,
- Veri sorumlusunun geçiş sistemleri yönetimi için kullanılan mevcut yazılım sözleşmesinin bitimine yaklaşılması ve gelecek dönem ihale sürecine yönelik ön araştırma çalışmalarının yürütülmesi sırasında ihlalin tespit edildiği,
- İhlalden etkilenen kişi grupları, ilgili kişi sayısı ve kişisel verilere ilişkin kesin tespitlerin yapılamadığı

Veri ihlaline ilişkin kamuoyu duyurusuna buradan ulaşabilirsiniz.

Türkiye'deki Gelişmeler

Veri İhlali Bildirimleri

Eurail B.V. tarafından KVK Kuruluna bildirilen veri ihlali, 27.01.2026 tarihinde KVK Kurumunun internet sitesinde yayımlanmıştır.

Veri sorumlusu Eurail B.V. tarafından KVK Kuruluna veri ihlali bildirilmiştir. Bildirimde aşağıdaki hususlar belirtilmiştir:

- İhlalin 26.12.2025 tarihinde başladığı ve 05.01.2026 tarihinde tespit edildiği,
- İhlalin veri sorumlusu sistemlerine yapılan siber saldırı neticesinde gerçekleştiği,
- İhlalden etkilenen kişisel verilerin; kimlik (ad-soyad, cinsiyet, doğum tarihi ve/veya yaş, pasaport numarası, pasaportun hangi ülkede düzenlendiği ve geçerlilik tarihi), iletişim (adres ve ikamet yeri - e-posta adresi - telefon numarası), müşteri işlem (tren yolculuklarına ilişkin seyahat bilgileri (ülke, şehir, seyahat tarih ve saatleri dahil)) verileri olduğu,
- İhlalden etkilenen Türkiye'de mukim 8.823 kişinin olduğu,
- İhlalden etkilenen ilgili kişi grubunun tren bileti satın alan müşteriler olduğu,
- İhlal ile ilgili teknik inceleme ve ek araştırmaların halen devam ettiği,

Veri ihlaline ilişkin kamuoyu duyurusuna buradan ulaşabilirsiniz.

Türkiye'deki Gelişmeler

Veri İhlali Bildirimleri

Codeway Dijital Hizmetler Anonim Şirketi tarafından KVK Kuruluna bildirilen veri ihlali, 27.01.2026 tarihinde KVK Kurumunun internet sitesinde yayımlanmıştır.

Veri sorumlusu Codeway Dijital Hizmetler Anonim Şirketi tarafından KVK Kuruluna veri ihlali bildirilmiştir.

Bildirimde aşağıdaki hususlar belirtilmiştir:

- İhlalin 15.01.2026-20.01.2026 tarihleri arasında gerçekleştiği ve 20.01.2026 tarihinde tespit edildiği,
- Chat & Ask AI adlı mobil uygulamasının veri tabanı ve dosya depolama altyapısı olarak kullanılan Google Firebase servisleri üzerindeki yetkilendirme yapılandırmasındaki zafiyet sebebiyle saldırganların kullanıcı verilerine ve dosya havuzuna erişim hakkı elde etmesiyle ihlalin gerçekleştiği,
- Teknik zafiyetin giderilmesinin akabinde veri ihlali olayına ilişkin iç kontrol ve denetim çalışmalarının ve araştırmaların halihazırda devam etmekte olduğu,
- İhlalden kullanıcılara ait e-posta adresi, uygulamaya kayıt esnasında seçilen takma isim ve uygulamayı kullanım esnasında uygulama ile paylaştıkları gönderi içeriklerinin etkilendiği,
- İhlalden yaklaşık 3.700 kişinin etkilendiğinin değerlendirildiği, sayının netleştirilmesine ilişkin çalışmaların devam ettiği

Veri ihlaline ilişkin kamuoyu duyurusuna buradan ulaşabilirsiniz.

Türkiye'deki Gelişmeler

Veri İhlali Bildirimleri

Özbeyler Sağlık ve Özel Hastahane Medikal İthalat İhracat Sanayi ve Ticaret Anonim Şirketi tarafından KVK Kuruluna bildirilen veri ihlali, 27.01.2026 tarihinde KVK Kurumunun internet sitesinde yayımlanmıştır.

Veri sorumlusu Özbeyler Sağlık ve Özel Hastahane Medikal İthalat İhracat Sanayi ve Ticaret Anonim Şirketi tarafından KVK Kuruluna veri ihlali bildirilmiştir. Bildirimde aşağıdaki hususlar belirtilmiştir:

- İhlalin 20.01.2026 tarihinde gerçekleştiği ve 20.01.2026 tarihinde tespit edildiği,
- İhlalin kaynağının fidye yazılımı saldırısı olduğu,
- İhlalden etkilenen kişisel veri kategorilerinin kimlik, iletişim, özlük, fiziksel mekan güvenliği, işlem güvenliği, finans, mesleki deneyim, görsel işitsel kayıtlar ile özel nitelikli kişisel veriler olduğu,
- İhlalden etkilenen ilgili kişi gruplarının çalışanlar, öğrenciler, müşteri ve potansiyel müşteriler, hastalar olduğu, ayrıca yapılan mevcut tespitler kapsamında; çalışan adayı, çalışan yakını, dışarıdan hizmet veren doktor, misafir, hasta yakını, hizmet veren kişi temsilcisi, referans, donör, görgü tanığı, kamu kurum çalışanı, kimliği kaybolan kişi, hissedar/ortak, potansiyel ürün veya hizmet alıcısı, stajyer, tedarikçi çalışanı, tedarikçi yetkilisi, ürün veya hizmet alan kişi, veli/vasi/temsilci, ziyaretçi, kamera kaydı alınan kişi ve diğer ilgili kişi gruplarına ait kişisel verilere de erişim sağlanmış olabileceğinin belirlendiği,
- İhlalden etkilenen ilgili kişi sayısının henüz tespit edilemediği, tespite yönelik incelemelerin devam ettiği

Veri ihlaline ilişkin kamuoyu duyurusuna buradan ulaşabilirsiniz.

Türkiye'deki Gelişmeler

Veri İhlali Bildirimleri

Köfteci Yusuf Hazır Yemek Temizlik Canlı Hayvan Et Mamulleri Entegre Gıda İthalat İhracat San. Tic. A.Ş. tarafından KVK Kurumuna bildirilen veri ihlali, 27.01.2026 tarihinde KVK Kurumunun internet sitesinde yayımlanmıştır.

Veri sorumlusu Köfteci Yusuf Hazır Yemek Temizlik Canlı Hayvan Et Mamulleri Entegre Gıda İthalat İhracat San. Tic. A.Ş. tarafından KVK Kuruluna veri ihlali bildirilmiştir. Bildirimde aşağıdaki hususlar belirtilmiştir:

- İhlalin 22.01.2026 tarihinde başladığı ve 23.01.2026 tarihinde tespit edildiği,
- İhlalin veri sorumlusunun bordro yazılımı ve online yemek siparişlerinin yönetildiği bilgi sistemlerini barındıran yerel SQL veritabanının dışardan bir müdahale ile şifrelenerek erişimin engellenmesi neticesinde gerçekleştiği,
- İhlalden etkilenen ilgili kişi grubunun çalışanlar ve müşteriler olduğu,
- İhlalden etkilenen kişisel verilerin müşteriler için kimlik (ad soyad), iletişim (adres, cep telefonu), müşteri işlem (yemek sipariş detayı) ve çalışanlar için kimlik, iletişim ve özlük verileri olduğu,
- İhlalden, veri sorumlusunun 13.000 çalışanı ve 150.000 müşterisi olmak üzere toplam 163.000 kişinin etkilendiği

Veri ihlaline ilişkin kamuoyu duyurusuna buradan ulaşabilirsiniz.

Türkiye'deki Gelişmeler

Veri İhlali Bildirimleri

Vodafone Net İletişim Hizmetleri A.Ş. tarafından KVK Kuruluna bildirilen veri ihlali, 03.02.2026 tarihinde KVK Kurumu internet sitesinde yayımlanmıştır.

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

- İhlalin 10.01.2026 tarihinde başladığı ve 26.01.2026 tarihinde tespit edildiği,
- VodafoneNet aboneleri, veri işleyen çalışanları ve veri işleyenin saha operasyonları adına hizmet aldığı tedarikçi çalışanı verilerinin DarkWeb üzerinden satışa sunulduğunun istihbar olunduğu,
- İstihbar olunan ilgili kayıtların yer alabileceği sistemler üzerinde detaylı bir soruşturma süreci başlatıldığı ve yapılan incelemeler sonucunda olaya konu kişisel verilerin veri işleyenin sisteminden elde edilmiş olabileceği kanısına varıldığı,
- İhlalden etkilenen ilgili kişi sayısının tam olarak bilinemediği ve tespit etme çalışmalarının devam ettiği; ihlalden etkilenen ilgili kişi sayısının çok daha az olduğu düşünülmekle birlikte en fazla 321.504 olabileceği,
- İhlalden etkilenmiş olabilecek kişisel veri kategorilerinin; kimlik, iletişim, müşteri işlem ve diğer (temin edilen ürün-hizmet kapsamında cihaz bilgileri) olduğu

Veri ihlaline ilişkin kamuoyu duyurusuna buradan ulaşabilirsiniz.

Türkiye'deki Gelişmeler

Veri İhlali Bildirimleri

Maremar K.Maraş Manyetik Rezonans Teşhis Merkezi ve Sağlık Hizmetleri Tic. ve San. A.Ş. tarafından KVK Kuruluna bildirilen veri ihlali, 18.02.2026 tarihinde KVK Kurumu internet sitesinde yayımlanmıştır.

Veri sorumlusu Maremar K.Maraş Manyetik Rezonans Teşhis Merkezi ve Sağlık Hizmetleri Tic. ve San. A.Ş. tarafından KVK Kuruluna veri ihlali bildirilmiştir. Bildirimde aşağıdaki hususlar belirtilmiştir:

- Veri sorumlusunun 12.02.2026 tarihinde fidye yazılımı saldırısına maruz kaldığı,
- İhlalin, bütün dosyaların şifrelenmiş olması dolayısıyla verilere erişim sağlanamayınca tespit edilebildiği,
- İhlalden etkilenen ilgili kişi grubunun hastalar olduğu,
- İhlalden etkilenen kişisel veri kategorilerinin kimlik, iletişim ve sağlık bilgileri olduğu,
- İhlalden etkilenen ilgili kişi sayısının tam olarak bilinmediği

Veri ihlaline ilişkin kamuoyu duyurusuna buradan ulaşabilirsiniz.

Türkiye'deki Gelişmeler

Veri İhlali Bildirimleri

TÜRKKEP Kayıtlı Elektronik Posta Hizmetleri Sanayi ve Anonim Şirketi tarafından KVK Kuruluna bildirilen veri ihlali, 18.02.2026 tarihinde KVK Kurumu internet sitesinde yayımlanmıştır.

Veri sorumlusu TÜRKKEP Kayıtlı Elektronik Posta Hizmetleri Sanayi ve Anonim Şirketi tarafından KVK Kuruluna veri ihlali bildirilmiştir. Bildirimde aşağıdaki hususlar belirtilmiştir:

- İhlalin 10.02.2026-16.02.2026 tarihleri arasında gerçekleştiği, 15.02.2026 tarihinde tespit edildiği,
- Veri sorumlusunun servislerine yönelik yapılan siber saldırı neticesinde uygulama kullanıcılarının listesine yetkisiz erişim sağlandığı,
- İhlalden etkilenen kişisel verilerin ad, soyad, kullanıcı adı, şifre (hashli), e-posta, telefon numarası, müşteri adı, T.C./Vergi kimlik numarası, şirket adı, şehir, ticaret sicil no olduğu,
- İhlalden etkilenen ilgili kişi sayısının tahmini olarak 8.170 olduğu, etkilenen ilgili kişi sayısının net olarak tespitine yönelik çalışmaların devam ettiği,
- İhlalden etkilenen ilgili kişi grubunun kullanıcılar olduğu

Veri ihlaline ilişkin kamuoyu duyurusuna buradan ulaşabilirsiniz.

Türkiye'deki Gelişmeler

Veri İhlali Bildirimleri

Sentez Sağlık Hizmetleri A.Ş. tarafından KVK Kuruluna bildirilen veri ihlali, 18.02.2026 tarihinde KVK Kurumu internet sitesinde yayımlanmıştır.

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

- Veri sorumlusunun fidye yazılımı saldırısına uğraması neticesinde kişisel veri ihlalinin gerçekleştiği,
- İhlalden etkilenen ilgili kişi sayısının henüz tespit edilemediği, tespite yönelik incelemelerin devam ettiği,
- İhlalden etkilenen ilgili kişi gruplarının çalışanlar ve hastalar olduğu,
- Kimlik, iletişim, lokasyon, özlük, hukuki işlem, finans, mesleki deneyim, pazarlama, görsel/işitsel kayıtlar ve sağlık bilgilerinin ihlalden etkilendiği; konuya ilişkin tespit çalışmalarının devam ettiği,

Veri ihlaline ilişkin kamuoyu duyurusuna buradan ulaşabilirsiniz.

Türkiye'deki Gelişmeler

Veri İhlali Bildirimleri

Garanti Finansal Kiralama A.Ş. tarafından KVK Kuruluna bildirilen veri ihlali, 04.03.2026 tarihinde KVK Kurumu internet sitesinde yayımlanmıştır.

Veri sorumlusu Garanti Finansal Kiralama A.Ş. tarafından KVK Kuruluna veri ihlali bildirilmiştir. Bildirimde aşağıdaki hususlar belirtilmiştir:

- Veri sorumlusunun bir çalışanının içerisinde müşteri bilgileri de bulunan birtakım dokümanları kendi kişisel e-posta adresine 22.12.2025 tarihinde gönderme girişiminin, kullanılan veri sızıntısı önleme sistemi (DLP) tarafından engellenerek raporlandığı,
- Bunun üzerine bahse konu çalışanın DLP tarafından engellenemeyen başka e-maillerinin olabileceği hususunda şüphe meydana geldiği,
- Yapılan inceleme sonucunda bahse konu çalışanın, veri sorumlusu müşterilerine ait unvan, müşteri numarası, müşterinin satın almak istediği ekipman, ekipmanın kullanım amacı, peşinat oranı/satıcıya ödeme şekli, teminat bilgisi, faaliyet ve ortaklık bilgileri, müşteri hakkında şirket görüşü, borçluluk ve kredi skoru, müşterinin çalıştığı diğer finansal kurumlar, güncel finansal performans ve ciro bilgileri, müşteri numarası, unvan, segment, ikamet ettikleri il/ilçe, bağlı olunan şube/bölge bilgisi, güncel risk ve gecikmiş borç bakiyeleri, toplam işlem hacmi, aktif ve toplam sözleşme sayısı, maksimum risk tutarı ve müşteri risk durumu bilgilerini kurumsal e-posta adresinden şahsi e-posta adresine birden çok seferde iletmesi ile ihlalin gerçekleştiğinin tespit edildiği,
- İhlalden etkilenen ilgili kişi sayısının 5664 olduğu,

Veri ihlaline ilişkin kamuoyu duyurusuna buradan ulaşabilirsiniz.

Türkiye'deki Gelişmeler

Veri İhlali Bildirimleri

Esea Sağlık ve Yatırım A.Ş. tarafından KVK Kuruluna bildirilen veri ihlali, 04.03.2026 tarihinde KVK Kurumu internet sitesinde yayımlanmıştır.

Veri sorumlusu Esea Sağlık ve Yatırım A.Ş. tarafından KVK Kuruluna veri ihlali bildirilmiştir. Bildirimde aşağıdaki hususlar belirtilmiştir:

- Veri sorumlusu adına bulunan Gaziantep Özel Medicalpoint hastanesine 21.02.2026 tarihinde siber saldırı gerçekleştirildiği,
- Saldırı sonrası sistemlerin güvenli yedeklerden geri dönülerek kurtarıldığı, veri kaybı olmadan güvenlik tedbirleri alınarak sistemlerin yeni ortama yüklenerek faaliyete devam edildiği,
- Yapılan tespitler uyarınca dışarı veri aktarımı sağlanmadığı,
- İhlalden çalışanlar ve hastalar olmak üzere 1000 kişinin kimlik, iletişim, özlük, finans ve sağlık verilerinin etkilendiği,
- İlgili kişilerin çağrı merkezi ve hasta hakları birimi aracılığıyla ihlal ile ilgili bilgi alabileceği

Veri ihlaline ilişkin kamuoyu duyurusuna buradan ulaşabilirsiniz.

Türkiye'deki Gelişmeler

Veri İhlali Bildirimleri

Civil Mağazacılık A.Ş. tarafından KVK Kuruluna bildirilen veri ihlali, 04.03.2026 tarihinde KVK Kurumu internet sitesinde yayımlanmıştır.

Veri sorumlusu Civil Mağazacılık A.Ş. tarafından KVK Kuruluna veri ihlali bildirilmiştir. Bildirimde aşağıdaki hususlar belirtilmiştir:

- Siber saldırganlarca veri sorumlusu CRM sisteminin çalıştığı 1 adet Windows Server üzerinde bulunan veritabanlarına, yönetici ve veritabanı seviyesinde bir hesap kullanılarak erişim sağlandığı ve ilgili veritabanı içeriklerinin sistem dışına aktarıldığı,
- İhlalin 12.02.2026 tarihinde başladığı ve 28.02.2026 tarihinde tespit edildiği,
- Veri ihlalinden etkilenen kişisel verilerin; kimlik (ad, soyad, T.C. kimlik no), iletişim (telefon, e-posta, adres) bilgileri olduğu,
- Veri ihlalinden etkilenen kişi sayısının tahmini 4.500.000 kişi olabileceği,
- İhlalden etkilenen ilgili kişi grubunun çalışanlar ve müşteriler olduğu

Veri ihlaline ilişkin kamuoyu duyurusuna buradan ulaşabilirsiniz.

Türkiye'deki Gelişmeler

Veri İhlali Bildirimleri

Şikayetvar Bilişim Anonim Şirketi tarafından KVK Kuruluna bildirilen veri ihlali, 04.03.2026 tarihinde KVK Kurumu internet sitesinde yayımlanmıştır.

Veri sorumlusu Şikayetvar Bilişim Anonim Şirketi tarafından KVK Kuruluna veri ihlali bildirilmiştir. Bildirimde aşağıdaki hususlar belirtilmiştir:

- İhlalin 24.04.2025-26.04.2025 tarihleri arasında gerçekleştiği ve 02.03.2026 tarihinde tespit edildiği,
- Veri sorumlusu tarafından müşteriye sağlanan geçerli erişim yetkilerinin/API anahtarlarının (www.sikayetplus.com alan adlı web sitesi için) üçüncü taraf kişilerce ele geçirilmesi ve kişisel verilere yetkisiz bir şekilde erişilmesi neticesinde kişisel veri ihlalinin meydana geldiği,
- İhlalden 212.523 kullanıcının etkilendiği,
- İhlalden etkilenen kişisel verilerin ad, soyadı, TCKN, telefon numarası ve e-posta adresi bilgileri olduğu,
- İlgili kişilerin "kvkk@sikayetvar.com" e-posta adresi aracılığıyla ihlal hakkında bilgi alabilecekleri

Veri ihlaline ilişkin kamuoyu duyurusuna buradan ulaşabilirsiniz.

Türkiye'deki Gelişmeler

Veri İhlali Bildirimleri

Baydöner Restoranları A.Ş. tarafından KVK Kuruluna bildirilen veri ihlali, 12.03.2026 tarihinde KVK Kurumu internet sitesinde yayımlanmıştır.

Veri sorumlusu Baydöner Restoranları A.Ş. tarafından KVK Kuruluna veri ihlali bildirilmiştir. Bildirimde aşağıdaki hususlar belirtilmiştir:

- İhlalin 15.02.2026 tarihinde başladığı, 08.03.2026 tarihinde tespit edildiği,
- İhlalin veri sorumlusu tedarikçi firması tarafından geliştirilen, yönetilen ve aynı zamanda host edilen Müşteri Hizmetleri ve Çağrı Merkezi yönetimi platformunda yer alan bilgilerin yetkisiz kişiler tarafından ele geçirilmesi sonucu gerçekleştiği,
- İhlal edilen kişisel verilerin; ad-soyad, telefon numarası, e-posta adresi, T.C. kimlik numarası, uygulama parolaları ve sipariş/teslimat bilgileri olduğu,
- İhlalden etkilenen kişi grubunun kullanıcılar olduğu,
- Sistemde bulunan kişi sayısının 1.490.789 olduğu, kaç kişinin etkilendiğinin bilinmediği

Veri ihlaline ilişkin kamuoyu duyurusuna buradan ulaşabilirsiniz.

Türkiye'deki Gelişmeler

Veri İhlali Bildirimleri

Cordamed Biomedikal Mühendislik A.Ş. tarafından KVK Kuruluna bildirilen veri ihlali, 12.03.2026 tarihinde KVK Kurumu internet sitesinde yayımlanmıştır.

Veri sorumlusu Cordamed Biomedikal Mühendislik A.Ş. tarafından KVK Kuruluna veri ihlali bildirilmiştir. Bildirimde aşağıdaki hususlar belirtilmiştir:

- İhlalin 27.02.2026-07.03.2026 tarihleri arasında gerçekleştiği ve 06.03.2026 tarihinde tespit edildiği,
- Veri sorumlusunun, Intuitive Surgical Operations Inc.'nin ("Intuitive") ürünlerinin Türkiye dağıtıcısı olduğu,
- Intuitive'in bir çalışanına ait oturum açma bilgilerinin siber saldırgan/saldırganlar tarafından ele geçirilmesi ve kişisel verilere yetkisiz bir şekilde erişilmesi neticesinde veri ihlalinin meydana geldiği,
- İhlalden etkilenen ilgili kişi gruplarının çalışanlar, kullanıcılar ve müşteriler olduğu; bu kişilere ek olarak tıbbi cihaz şikayetlerinde yer alan hastalara ait verilerin de ihlale konu olduğu ancak bu veriler takma adla gizlenmiş (psödonimleştirilmiş) olduğundan hastaların kimliğinin herhangi bir ek veri olmaksızın tespit edilmesinin mümkün olmadığı,
- İhlalden etkilenen kişi sayısının henüz bilinmediği,
- İhlalden etkilenen kişisel veri kategorilerinin; kimlik, iletişim, lokasyon, mesleki deneyim ve sağlık bilgileri olduğu,
- İlgili kişilerin e-posta aracılığıyla ihlal hakkında bilgi alabilecekleri

Veri ihlaline ilişkin kamuoyu duyurusuna buradan ulaşabilirsiniz.

Türkiye'deki Gelişmeler

Veri İhlali Bildirimleri

Intuitive Surgical Operations Inc. tarafından KVK Kuruluna bildirilen veri ihlali, 12.03.2026 tarihinde KVK Kurumu internet sitesinde yayımlanmıştır.

Veri sorumlusu Intuitive Surgical Operations Inc. tarafından KVK Kuruluna veri ihlali bildirilmiştir. Bildirimde aşağıdaki hususlar belirtilmiştir:

- İhlalin 27.02.2026-07.03.2026 tarihleri arasında gerçekleştiği ve 06.03.2026 tarihinde tespit edildiği,
- Veri sorumlusunun bir çalışanına ait oturum açma bilgilerinin siber saldırgan/saldırganlar tarafından ele geçirilmesi ve kişisel verilere yetkisiz bir şekilde erişilmesi neticesinde veri ihlalinin meydana geldiği,
- İhlalden etkilenen ilgili kişi gruplarının çalışanlar, kullanıcılar ve müşteriler olduğu; bu kişilere ek olarak tıbbi cihaz şikayetlerinde yer alan hastalara ait verilerin de ihlale konu olduğu ancak bu veriler takma adla gizlenmiş (psödonimleştirilmiş) olduğundan hastaların kimliğinin herhangi bir ek veri olmaksızın tespit edilmesinin mümkün olmadığı,
- İhlalden etkilenen kişi sayısının 1.885 olduğu,
- İhlalden etkilenen kişisel veri kategorilerinin; kimlik, iletişim, lokasyon, mesleki deneyim ve sağlık bilgileri olduğu,
- İlgili kişilerin, veri sorumlusunun e-posta adresi aracılığıyla ihlal hakkında bilgi alabilecekleri

Veri ihlaline ilişkin kamuoyu duyurusuna buradan ulaşabilirsiniz.

Türkiye'deki Gelişmeler

Veri İhlali Bildirimleri

İzelman Genel Hizmet Otopark Özel Eğitim Danışmanlık İtfaiye ve Sağlık Hizmetleri Ticaret A.Ş. tarafından KVK Kuruluna bildirilen veri ihlali, 12.03.2026 tarihinde KVK Kurumu internet sitesinde yayımlanmıştır.

Veri sorumlusu İzelman Genel Hizmet Otopark Özel Eğitim Danışmanlık İtfaiye ve Sağlık Hizmetleri Ticaret A.Ş. tarafından KVK Kuruluna veri ihlali bildirilmiştir. Bildirimde aşağıdaki hususlar belirtilmiştir:

- Veri sorumlusunun 16.03.2026 tarihinde fidye yazılımı saldırısına uğradığı, sunuculardaki datanın ve back up olarak saklanan verilerin şifrelendiği,
- İhlalden etkilenen kişisel veri kategorilerinin; kimlik, iletişim, lokasyon, özlük, hukuki işlem, finans, mesleki deneyim, pazarlama, sendika üyeliği, sağlık bilgileri, biyometrik veriler olduğu,
- İhlalden etkilenen kişi sayısının 10.000'den fazla olduğunun tahmin edildiği,
- İhlalden etkilenen ilgili kişi grubunun çalışanlar olduğu, başka kişilerin etkilenip etkilenmediğinin henüz bilinmediği

Veri ihlaline ilişkin kamuoyu duyurusuna buradan ulaşabilirsiniz.

Türkiye'deki Gelişmeler

Veri İhlali Bildirimleri

NSB Med. Sağ. Hiz. Tic. A.Ş. tarafından KVK Kuruluna bildirilen veri ihlali, 12.03.2026 tarihinde KVK Kurumu internet sitesinde yayımlanmıştır.

Veri sorumlusu NSB Med. Sağ. Hiz. Tic. A.Ş. tarafından KVK Kuruluna veri ihlali bildirilmiştir. Bildirimde aşağıdaki hususlar belirtilmiştir:

- İhlalin 09.03.2026 tarihinde başladığı ve aynı gün tespit edildiği,
- Veri sorumlusunun halihazırda kullandığı yazılıma bir siber saldırı gerçekleştiği,
- Saldırı sonrası verilerin siber saldırganlarca ele geçirildiği, fakat verinin büyüklüğü hakkında tespit yapılamadığı,
- İhlalden etkilenen kişisel verilerin sağlık bilgileri olduğu,
- İhlalden etkilenen kişi sayısının tespit edilemediği,
- İhlalden etkilenen ilgili kişi grubunun hastalar olduğu

Veri ihlaline ilişkin kamuoyu duyurusuna buradan ulaşabilirsiniz.

Türkiye'deki Gelişmeler

Duyurular ve Haberler

KVK Kurumu tarafından VERBİS'e kayıt yükümlülüğüne ilişkin istisna kriterlerinin uygulanmasına yönelik kamuoyu duyurusu yayımlanmıştır.

6698 sayılı Kişisel Verilerin Korunması Kanunu'nun 16'ncı maddesi uyarınca, kişisel veri işleyen gerçek ve tüzel kişi veri sorumlularının Veri Sorumluları Sicil Bilgi Sistemine (VERBİS) kayıt yükümlülüğü bulunmakla birlikte, Kişisel Verileri Koruma Kurulu tarafından belirlenen objektif kriterler çerçevesinde bu yükümlülüğe istisna getirilebilmektedir.

Bu kapsamda, Kişisel Verileri Koruma Kurulunun 04.09.2025 tarihli ve 2025/1572 sayılı Kararı ile daha önce belirlenen istisna kriterleri güncellenmiş;

- Yıllık çalışan sayısı 50'den az ve yıllık mali bilanço toplamı 100 milyon TL'den az olan ve ana faaliyet konusu özel nitelikli kişisel veri işleme olmayan veri sorumlularının yanı sıra,
- Ana faaliyet konusu özel nitelikli kişisel veri işleme olmakla birlikte yıllık çalışan sayısı 10'dan az ve yıllık mali bilanço toplamı 10 milyon TL'den az olan veri sorumlularının da VERBİS'e kayıt yükümlülüğünden istisna tutulmasına karar verilmiştir.

Öte yandan Kuruma iletilen görüş talepleri doğrultusunda, bilanço esasına göre defter tutmayan veri sorumluları bakımından "yıllık mali bilanço toplamı" kriterinin nasıl değerlendirileceğine açıklık getirilmiştir. Bu çerçevede, Kişisel Verileri Koruma Kurulunun 25.12.2025 tarihli ve 2025/2393 sayılı Kararı ile;

- Bilanço esasına göre defter tutan veri sorumluları bakımından çalışan sayısı ve yıllık mali bilanço toplamı kriterlerinin birlikte,
- Bilanço esasına göre defter tutmayan veri sorumluları bakımından ise yalnızca yıllık çalışan sayısı kriterinin esas alınacağı belirtilmiştir.

Söz konusu duyuru ile, VERBİS'e kayıt yükümlülüğüne ilişkin istisna kriterlerinin uygulamasında ortaya çıkan tereddütlerin giderilmesi ve veri sorumlularına yol gösterilmesi amaçlanmaktadır.

İlgili kamuoyu duyurusuna buradan ulaşabilirsiniz.

Türkiye'deki Gelişmeler

Duyurular ve Haberler

KVK Kurumu tarafından mobil uygulamalar üzerinden gönderilen anlık bildirimlere (push notification) ilişkin kamuoyu duyurusu yayımlanmıştır.

Kamuoyu duyurusunda, Kurum'a intikal eden benzer nitelikteki şikayetler kapsamında yürütülen incelemeler sonucunda, mobil uygulamalar aracılığıyla kullanıcılara gönderilen anlık bildirimlerin kişisel verilerin korunması mevzuatına uygunluğu konusunda kamuoyunun bilgilendirilmesine ihtiyaç duyulduğu belirtilmiştir.

6698 sayılı Kişisel Verilerin Korunması Kanunu uyarınca, mobil uygulama sağlayıcılarının veri sorumlusu sıfatıyla yürüttükleri veri işleme faaliyetlerinin Kanun'un genel ilkelerine ve veri işleme şartlarına uygun şekilde gerçekleştirilmesi gerekmektedir. Bu kapsamda, anlık bildirim gönderimi süreçlerinin kullanıcıların cihazları üzerinden verdikleri izinlere dayandığı ve bu izinlerin hukuka uygun şekilde alınmasının önem taşıdığı vurgulanmıştır.

Kurum tarafından incelenen somut bir olayda, mobil uygulama yükleme aşamasında sunulan bildirim onayının birden fazla veri işleme amacını kapsayacak şekilde tek bir rıza beyanı olarak kurgulandığı tespit edilmiştir. Özellikle hizmetin sunumu bakımından zorunlu nitelikteki operasyonel bildirimler ile pazarlama ve kampanya içerikli bildirimlerin birlikte sunulmasının, ilgili kişilerin özgür iradeye dayalı açık rıza vermesini engelleyebileceği ifade edilmiştir.

Bu doğrultuda, birden fazla veri işleme amacının söz konusu olduğu durumlarda "parçalı açık rıza" (granularity) ilkesine uygun hareket edilmesi, her bir bildirim türü için kullanıcıya ayrı ve bağımsız tercih imkanı sunulması gerektiği belirtilmiştir. Ayrıca mobil uygulamaların teknik yapısının, kullanıcıların hangi bildirimleri almak istediklerini uygulama içi veya cihaz ayarları üzerinden yönetebilecekleri şekilde yapılandırılmasının önem taşıdığı ifade edilmiştir.

Söz konusu duyuru ile, veri sorumlularının mobil uygulamalar üzerinden yürüttükleri bildirim süreçlerini belirlilik, özgür irade ve teknik/idari tedbir yükümlülükleri çerçevesinde gözden geçirmeleri gerektiğine dikkat çekilmektedir.

İlgili kamuoyu duyurusuna buradan ulaşabilirsiniz.

Türkiye'deki Gelişmeler

Duyurular ve Haberler

KVK Kurumu tarafından "Yapay Zeka Araçları Kullanan Çocuklar İçin Ebeveynlere Yönelik Tavsiyeler" dokümanı yayınlanmıştır.

Dokümanda, yapay zeka teknolojilerinin çocukların eğitim, iletişim ve sosyal yaşamlarının önemli bir parçası haline geldiği; sohbet botları, yapay zeka destekli öğrenme uygulamaları ve içerik üretim araçlarının öğrenmeyi destekleyici fırsatlar sunabildiği ifade edilmiştir. Bununla birlikte, bu teknolojilerin bilinçsiz kullanımı halinde mahremiyet ihlalleri, çevrim içi güvenlik riskleri ve yanıltıcı içeriklerle karşılaşma gibi risklerin ortaya çıkabileceğine dikkat çekilmiştir.

- Bu kapsamda ebeveynlerin, çocuklarının yapay zeka araçlarını hangi amaçlarla kullandığını takip etmesinin ve bu teknolojilerle kurdukları ilişkiye rehberlik etmesinin önem taşıdığı vurgulanmıştır. Özellikle kullanılan uygulamaların yaşa uygunluğu, kullanım koşulları, gizlilik politikaları ve ebeveyn kontrolü seçeneklerinin değerlendirilmesinin çocukların daha güvenli bir dijital ortamda bulunmasına katkı sağlayacağı belirtilmiştir.

Dokümanda ayrıca, yapay zeka sistemlerinin her zaman doğru ve güvenilir bilgi sunmayabileceği; sahte video, görsel ve ses içeriklerinin (deepfake vb.) çocuklar açısından aldatılma, korkutulma veya siber zorbalık risklerini artırabileceği ifade edilmiştir. Bu doğrultuda ebeveynlerin çocuklarını dijital içeriklere karşı sorgulayıcı bir bakış açısı geliştirmeleri konusunda bilinçlendirmesi ve fotoğraf-video paylaşımları ile sosyal medya gizlilik ayarları konusunda yönlendirmesi gerektiği belirtilmiştir.

- Kişisel verilerin korunmasına ilişkin farkındalığın artırılması amacıyla, çocuklara ad-soyad, adres, okul bilgisi veya telefon numarası gibi kişisel bilgilerin paylaşılmasının riskleri hakkında yaşlarına uygun şekilde bilgi verilmesi gerektiği vurgulanmıştır. Bunun yanında dijital ebeveynlik anlayışı çerçevesinde, çocuklarla açık iletişim kurulması, ekran süresinin dengelenmesi ve dijital ortamda etik ve saygılı kullanım alışkanlıklarının kazandırılmasının önemine dikkat çekilmiştir.

Söz konusu bilgilendirme ile, yapay zeka teknolojilerinin bilinçli ve ölçülü kullanımının desteklenmesi ve ebeveyn rehberliğinin çocukların dijital dünyada güvenli şekilde var olabilmeleri açısından belirleyici rol oynadığı ifade edilmektedir.

İlgili bilgilendirme metnine buradan ulaşabilirsiniz.

Türkiye'deki Gelişmeler

Duyurular ve Haberler

KVK Kurumu tarafından kişisel veri ihlali bildirimlerinin Kurum internet sitesinde ilan edilme süresine ilişkin kamuoyu duyurusu yayımlanmıştır.

KVK Kurumunun internet sitesinde yayımlanan kamuoyu duyurusu kapsamında aşağıdaki bilgilere yer verilmiştir.

6698 sayılı Kanun'un 12'nci maddesi uyarınca veri sorumlularının, kişisel verilerin kanuni olmayan yollarla elde edilmesi halinde durumu en kısa sürede ilgili kişilere ve Kurula bildirme yükümlülüğü bulunmaktadır. Kurulun 24.01.2019 tarihli ve 2019/10 sayılı Kararı ile bu sürenin en geç 72 saat olarak uygulanacağı belirlenmiştir.

Bu kapsamda Kişisel Verileri Koruma Kurulunun 25.12.2025 tarihli ve 2025/2451 sayılı Kararı ile veri ihlali bildirimlerinin Kurum internet sitesinde ilan edilmesine ilişkin uygulamada değişikliğe gidilmiştir.

Buna göre;

- Veri ihlali bildirimlerinin en fazla 60 gün süreyle ilan edilmesine,
- Veri sorumlusu tarafından ilgili kişilere bildirim yapıldığının daha kısa sürede tevsik edilmesi halinde ilanın internet sitesinden kaldırılmasına

karar verilmiştir.

Kurul tarafından ihlal bildirimlerinin ilan edilip edilmeyeceği değerlendirilirken ise;

- İhlalden etkilenen kişi grubu ve kişi sayısı
- İhlale konu kişisel verilerin niteliği ve kapsamı
- İhlalin gerçekleşme şekli
- Veri sorumlusunun faaliyet alanıİlgili kişilere bildirim yapılıp yapılmadığı

gibi kriterlerin dikkate alındığı belirtilmiştir.

Söz konusu duyuru ile veri ihlali bildirim süreçlerine ilişkin uygulamada standartlaşmanın sağlanması ve veri sorumlularına yol gösterilmesi amaçlanmaktadır.

İlgili kamuoyu duyurusuna buradan ulaşabilirsiniz.

Türkiye'deki Gelişmeler

Duyurular ve Haberler

KVK Kurumu tarafından Kişisel Verilerin Korunması İle İlgili Seçilmiş Güncel Gelişmeler'in 52. bölümü yayımlanmıştır.

KVK Kurumu tarafından yayınlanan gelişmelerden öne çıkan husular aşağıdaki gibidir;

EDPB & EDPS

- Avrupa Komisyonu'nun Digital Omnibus on AI teklifine ilişkin ortak görüş yayımlanmış, AI Act'in uygulanmasında idari basitleştirmenin temel hakların korunmasını zayıflatmaması gerektiği vurgulanmıştır.

Avrupa Komisyonu

- AB Veri Tüzüğü'nün (Data Act) uygulanmasına destek amacıyla hazırlanan güncellenmiş SSS dokümanını yayımlanmış ve AB siber güvenlik kapasitesini güçlendirmeye yönelik yeni bir paket önerilmiştir.

Hamburg Veri Koruma Otoritesi (HmbBfDI)

- Yapay zekanın finans sektörü üzerindeki etkilerine ilişkin bir karar kabul edilerek, finansal hizmetlerde yapay zeka kullanımının riskler ve temel haklar boyutuyla ele alınması gerektiği ortaya konulmuştur.

CNIL (Fransa)

- Çerezler ve izleme teknolojilerinde çoklu cihaz üzerinden rıza (cross-device consent) konusuna ilişkin nihai tavsiyeler paylaşılmış ve yapay zekada veri korumaya ilişkin rehber dokümanların İngilizce versiyonları yayımlanmıştır.

EPRS (Avrupa Parlamentosu Araştırma Servisi)

- Çevrim içi yaş doğrulama sistemlerinin VPN kullanımıyla aşılmasına yönelik artan eğilimin çocukların dijital ortamda korunması açısından oluşturduğu riskleri ele alan bir çalışma yayımlanmıştır.

ICO (Birleşik Krallık)

- Etken yapay zeka (Agentic AI) sistemlerinin potansiyel faydaları ve veri koruma risklerini değerlendiren bir rapor yayımlanmıştır.

OECD ve Ulusal Otoriteler

- Eğitimde üretken yapay zeka kullanımına ilişkin raporlar ve etik rehberler yayımlanmış, Güney Kore'de yapay zekanın güvenli kullanımına yönelik kapsamlı bir yasal düzenlemenin yürürlüğe girdiği bildirilmiştir.

İlgili bölümün tamamına buradan ulaşabilirsiniz.

Türkiye'deki Gelişmeler

Duyurular ve Haberler

KVK Kurumu tarafından kamu kurumlarında yurt dışı menşeli haberleşme uygulamalarının kullanımına ilişkin kamuoyu duyurusu yayımlanmıştır.

Kurum'a iletilen ihbar ve şikayetlerde, bazı kamu kurumlarında idari iş ve işlemlerin yürütülmesi kapsamında WhatsApp gibi haberleşme uygulamalarının kullanıldığı, bu uygulamalar üzerinden talimat verildiği ve resmi belge paylaşımı yapıldığı yönünde tespitlere yer verildiği belirtilmiştir.

Duyuruda öne çıkan hususlar aşağıdaki şekildedir:

- Kamu hizmetlerinin yürütülmesi sırasında kişisel verilerin korunması ve veri güvenliği yükümlülüklerine azami dikkat gösterilmesi gerektiği vurgulanmıştır.
- 2019/12 sayılı Cumhurbaşkanlığı Genelgesi uyarınca, yerli ve yetkilendirilmiş uygulamalar haricindeki mobil haberleşme uygulamaları üzerinden gizlilik dereceli veri paylaşılmaması gerektiği hatırlatılmıştır.
- Yurt dışı menşeli uygulamalar üzerinden resmi belge veya kritik veri paylaşımının veri güvenliği riskleri doğurabileceği ifade edilmiştir.
- Bu tür uygulamalar aracılığıyla kişisel veri içeren bilgi ve belgelerin paylaşılmasının KVKK kapsamında veri işleme faaliyeti olarak değerlendirileceği ve gerekli işleme şartlarının bulunmaması halinde idari ve disiplin yaptırımları söz konusu olabileceği belirtilmiştir.
- Kamu personeline ait GSM numaralarının da kişisel veri niteliğinde olduğu ve bu verilerin işlenmesinde Kanun'un 5'inci maddesindeki işleme şartlarına uygun hareket edilmesi gerektiğine dikkat çekilmiştir.

Söz konusu duyuru ile kamu kurumlarında haberleşme uygulamalarının kullanımında veri güvenliği ve mevzuata uyumun sağlanmasına yönelik farkındalık oluşturulması amaçlanmaktadır.

İlgili kamuoyu duyurusuna buradan ulaşabilirsiniz..

Türkiye'deki Gelişmeler

Duyurular ve Haberler

KVK Kurumu tarafından Grok yapay zeka asistanına ilişkin kamuoyu duyurusu yayımlanmıştır.

Duyuruda, yapay zeka asistanı Grok'un kişilerin rızası olmaksızın cinsel içerikli görüntü ve video üretimi amacıyla kullanıldığına ve bu içeriklerin dolaşıma sokulduğuna yönelik iddialar kapsamında Avrupa Komisyonu tarafından soruşturma başlatıldığı belirtilmiştir. Bu çerçevede, Grok'un geliştirilmesi ve uygulanması süreçlerinde 6698 sayılı Kanun kapsamında gerekli teknik ve idari tedbirlerin alınıp alınmadığının değerlendirilmesi amacıyla Kişisel Verileri Koruma Kurulu tarafından X Internet Unlimited Company ve X.AI Corporation hakkında re'sen inceleme başlatılmasına karar verildiği ifade edilmiştir.

İlgili kamuoyu duyurusuna buradan ulaşabilirsiniz.

KVK Kurumu tarafından çocukların sosyal medya kullanımında kişisel verilerinin korunmasına ilişkin kamuoyu duyurusu yayımlanmıştır.

Duyuruda, çocukların dijital ortamlarda karşılaşabilecekleri risklerin önlenmesi ve üstün yararlarının gözetilmesi amacıyla sosyal medya platformlarında çocuklara ait kişisel verilerin işlenme süreçleri ile alınan veri güvenliği tedbirlerinin incelenmesi kapsamında TikTok, Instagram, Facebook, YouTube, X ve Discord hakkında Kişisel Verileri Koruma Kurulu tarafından re'sen inceleme başlatılmasına karar verildiği belirtilmiştir.

İlgili kamuoyu duyurusuna buradan ulaşabilirsiniz.

Türkiye'deki Gelişmeler

Duyurular ve Haberler

KVK Kurumu tarafından Kişisel Verilerin Korunması İle İlgili Seçilmiş Güncel Gelişmeler'in 53. bölümü yayımlanmıştır.

KVK Kurumu tarafından yayınlanan gelişmelerden öne çıkan husular aşağıdaki gibidir;

EDPB

- Silme hakkının (unutulma hakkı) uygulanmasına ilişkin 2025 yılı Koordineli Uygulama Çerçevesi raporunu yayımlanmış; veri sorumlularının silme taleplerinin yönetimi, saklama süreleri ve yedekleme sistemlerinde silme süreçlerine ilişkin çeşitli zorluklarla karşılaştığına dikkat çekilmiştir.

ERPS ve AB Kurumları

- AB veri koruma politikasının genel çerçevesini ele alan çalışmalar ile Digital Omnibus on AI teklifine ilişkin değerlendirmeler yayımlanmıştır.

ICO (Birleşik Krallık)

- Veri koruma başvurularının veri sorumlularınca nasıl ele alınması gerektiğine ve Otorite'ye yapılan şikayet süreçlerinin işleyişine yönelik rehber içerikler paylaşılmıştır.

CNIL (Fransa)

- Deepfake teknolojilerinin riskleri ve bireylerin kendilerini nasıl koruyabileceklerine ilişkin bilgilendirici bir içerik yayımlanmıştır.

OECD ve EIOPA

- Finans sektöründe yapay zeka kullanımına yönelik denetim yaklaşımlarını ve sigorta sektöründe üretken yapay zekanın benimsenme düzeyini ele alan raporlar yayımlanmıştır.

ABD Çalışma Bakanlığı & NIST

- Yapay zeka okuryazarlığına ilişkin çerçeve dokümanı yayımlanmış ve yapay zeka aracılarının güvenli kullanımını desteklemek amacıyla yeni bir standart girişimi başlatılmıştır.

İlgili bölümün tamamına buradan ulaşabilirsiniz.

Türkiye'deki Gelişmeler

Duyurular ve Haberler

KVK Kurumu tarafından "QR Kodlarla Gelen Risk: Quishing" başlıklı bilgilendirme dokümanı yayımlanmıştır.

KVK Kurumu tarafından yayınlanan bilgilendirme dokümanında öne çıkan husular aşağıdaki gibidir;

Quishing Nedir?

"QR" ve "phishing" kelimelerinin birleşiminden oluşan quishing, siber tehdit aktörlerinin sahte veya sonradan değiştirilmiş QR kodlar aracılığıyla bireyleri kötü amaçlı internet sitelerine yönlendirmesi, kişisel verilerini ele geçirmesi veya cihazlara zararlı yazılım yüklenmesine neden olması şeklinde gerçekleştirilen bir saldırı yöntemidir. Rehberde özellikle dinamik QR kodların içeriklerinin sonradan değiştirilebilmesinin risk oluşturabileceği ve QR kodların hem fiziksel hem dijital ortamlarda yaygın kullanılmasının saldırı tehlikesini artırdığı vurgulanmaktadır.

Saldırı Yöntemi ve Riskler

Quishing saldırılarında;

- Kötü amaçlı bağlantılar içeren QR kodlar oluşturulmakta,
- Bu kodlar fiziksel ortamlara yerleştirilmekte veya e-posta yoluyla görsel olarak hedefteki kişilere iletilmekte,
- QR kodun taranmasıyla kişi sahte giriş sayfalarına yönlendirilmekte ya da zararlı dosyalar indirmeye sevk edilebilmektedir.

Bu süreç sonucunda kimlik ve ödeme bilgileri dahil olmak üzere kişisel veriler yetkisiz kişilerce ele geçirilebilmektedir.

Saldırılardan Korunmak Adına Dikkat Edilmesi Gereken Hususlar

Rehberde bireylerin özellikle şu konularda dikkatli olması gerektiği belirtilmektedir:

1. Kaynağı belirsiz veya beklenmeyen QR kodların taranmayın, yalnızca güvendiğiniz fiziksel ortamlardan veya dijital kanallardan tarayın.
2. Bir QR kod taraması sonucunda kişisel veri veya ödeme bilgisi isteniyorsa, işlemi yapmadan önce sitenin doğruluğundan emin olun; mümkünse adresi tarayıcınıza elle yazın.
3. Yönlendirilen internet sitesinin alan adının kontrol ederek tarama sonrası ulaştığınız bağlantının gerçekten ilgili kuruma ait olup olmadığını ve güvenliğini mutlaka inceleyin.
4. İşletim sisteminizi güncel tutun, hesabınızda güçlü parola ve çok faktörlü kimlik doğrulaması kullanmaya özen gösterin.

İlgili dokümanın tam metnine buradan ulaşabilirsiniz.

Türkiye'deki Gelişmeler

Duyurular ve Haberler

KVK Kurumu tarafından sadakat kartı üyeliklerinde üçüncü kişi kullanımına ilişkin İlke Kararı yayımlanmıştır.

KVK Kurumu tarafından yayınlanan ilke kararında öne çıkan husular aşağıdaki gibidir;

Kurul'a iletilen ihbar ve şikayetler kapsamında yapılan incelemelerde, ilgili kişilerin bilgisi ve rızası dışında üçüncü kişiler tarafından sadakat kartı bilgilerinin kullanıldığı, herhangi bir doğrulama mekanizması işletilmeden alışveriş işlemleri gerçekleştirilebildiği ve bu işlemlere ilişkin fatura ile müşteri kayıtlarının kart sahibi adına düzenlenebildiği tespit edilmiştir.

Kurul değerlendirmesinde;

- İlgili kişinin bilgisi ve rızası olmaksızın sadakat kartı bilgilerinin kullanılması suretiyle gerçekleştirilen veri işleme faaliyetlerinin 6698 sayılı Kanun'un 5'inci maddesinde yer alan veri işleme şartlarına dayanmadığı ve hukuka aykırılık teşkil ettiği,
- İlgili kişi tarafından yapılmamış alışverişlere ilişkin işlem bilgilerinin kayıt altına alınmasının "doğru ve gerektiğinde güncel olma" ilkesine aykırılık oluşturduğu,
- Üyelik sözleşmelerinde kartın üçüncü kişilerce kullanılmamasına yönelik hükümlerin bulunmasının, veri sorumlusunun veri güvenliğine ilişkin teknik ve idari tedbir alma yükümlülüğünü ortadan kaldırmayacağı

hususlarını vurgulamıştır.

Bu kapsamda Kurul, sadakat kartı bilgilerinin yalnızca cep telefonu numarasının beyanı ile kullanılmasına imkan tanıyan uygulamaların sonlandırılmasına, veri sorumlularının sadakat kartı kullanım süreçlerini Kanun'a uygun hale getirecek teknik ve idari tedbirleri almasına ve işlem türü ile risk seviyesine göre SMS ile tek kullanımlık doğrulama kodu (OTP), mobil uygulama üzerinden QR/barkod doğrulaması, fiziki kart ibrazı, şifre kullanımı veya "opt-in" tercih mekanizmaları gibi doğrulama yöntemlerinin uygulanmasına karar vermiştir.

Ayrıca veri sorumlularına İlke Kararı'nın yayım tarihinden itibaren 6 ay uyum süresi tanınmış olup, yükümlülüklere aykırı hareket edilmesi halinde Kanun'un 18'inci maddesi kapsamında idari yaptırım uygulanabileceği belirtilmiştir. Bu doğrultuda veri sorumlularının; sadakat kartı kullanım senaryolarını gözden geçirmesi, doğrulama altyapılarını güçlendirmesi, aydınlatma metinlerini güncellemesi, kasa personeline yönelik prosedür ve eğitim süreçlerini oluşturması ile sistemsel kontrol ve izleme mekanizmalarını tesis etmesi önem arz etmektedir.

İlgili ilke kararının tam metnine buradan ulaşabilirsiniz.

Türkiye'deki Gelişmeler

Duyurular ve Haberler

KVK Kurumu tarafından İş Yerlerinde Üretken Yapay Zeka Araçlarının Kullanımı dokümanı yayımlanmıştır.

KVK Kurumu tarafından yayınlanan bilgilendirme dokümanında öne çıkan husular aşağıdaki gibidir;

Üretken Yapay Zeka Araçlarının İş Yerlerinde Kullanımı

Rehberde "Üretken Yapay Zeka (ÜYZ)" sistemleri, kullanıcı tarafından verilen komutlara (prompt) yanıt olarak metin, görsel, video, ses veya yazılım kodu gibi farklı formatlarda içerik üretebilen yapay zeka sistemleri olarak tanımlanmaktadır.

Bu araçlar belirli bir sektör veya meslek grubuyla sınırlı olmayıp müşteri hizmetleri, pazarlama, eğitim, sağlık, hukuk ve yazılım geliştirme gibi pek çok alanda kullanılmakta ve iş yerlerinde özellikle şu amaçlarla tercih edilmektedir:

Gölge Yapay Zeka (Shadow AI) ve Ortaya Çıkardığı Riskler

Dokümanda özellikle "Gölge Yapay Zeka (Shadow AI)" kavramına dikkat çekilmektedir. Gölge yapay zeka, üretken yapay zeka araçlarının kurumun bilgisi, onayı ve kontrolü dışında çalışanlar tarafından iş süreçlerinde kullanılması durumunu ifade etmektedir.

Çalışanların bireysel inisiyatifle bu araçları kullanması, hangi araçların kullanıldığı ve hangi verilerin paylaşıldığı konusunda kurumsal denetim imkanını sınırlayabilmektedir. Bu durum çeşitli riskleri beraberinde getirmektedir.

Rehberde öne çıkan başlıca riskler şu şekilde belirtilmektedir: Denetlenebilirlik ve hesap verebilirliğe ilişkin riskler, karar kalitesi ve doğruluğa ilişkin riskler, fikri mülkiyet ve ticari sırların korunmasına ilişkin riskler, kurumsal itibar ve güven kaybına ilişkin riskler, bilgi güvenliği ve siber güvenliğe ilişkin riskler, kişisel verilerin korunmasına ilişkin riskler.

İş Yerlerinde Üretken Yapay Zeka Araçlarının Kullanımında Dikkat Edilmesi Gereken Hususlar

- ÜYZ araçlarının iş süreçlerinde kullanımına ilişkin olarak, doğru ve uygun kullanımın sınırlarını ortaya koyan açık bir kurumsal politika veya yönlendirme çerçevesinin oluşturulması
- ÜYZ araçlarının iş süreçlerinde kullanımı kapsamında, çalışanların bu araçlarla etkileşim sırasında kurumsal açıdan hassas nitelik taşıyan bilgiler ile kişisel veriler bakımından dikkatli bir yaklaşım benimsemelerinin sağlanması
- ÜYZ araçlarıyla etkileşim sırasında mümkün olduğunca anonimleştirilmiş, genelleştirilmiş ve soyut ifadelerin tercih edilmesi

İlgili dokümanın tam metnine buradan ulaşabilirsiniz.

Türkiye'deki Gelişmeler

Duyurular ve Haberler

KVK Kurumu tarafından Etken Yapay Zeka (Agentic AI) hakkında bilgilendirme dokümanı yayımlanmıştır.

KVK Kurumu tarafından yayınlanan bilgilendirme dokümanında öne çıkan husular aşağıdaki gibidir;

Etken Yapay Zeka Sistemlerine Genel Bakış

Dokümanda etken yapay zeka (Etken YZ) sistemleri, belirli hedeflere ulaşmak amacıyla çevresel koşulları değerlendirebilen, değişen durumlara uyum sağlayabilen ve farklı düzeylerde otonom biçimde eylem başlatabilen yapay zeka sistemleri olarak tanımlanmaktadır.

Etken Yapay Zeka Sistemlerinin Potansiyel Kullanım Alanları

Kurum tarafından yayımlanan dokümanda etken yapay zeka sistemlerinin farklı sektörlerde çeşitli amaçlar ile kullanılabileceği ifade edilmektedir. Örneğin; araştırma ve geliştirme süreçleri, müşteri destek süreçleri, finans ve yatırım hizmetleri vb.

Etken Yapay Zeka Sistemlerinin Kullanımı ile İlişkili Temel Riskler

Dokümanda etken yapay zeka sistemlerinin sunduğu operasyonel faydaların yanında çeşitli riskler doğurabileceği de ifade edilmektedir. Özellikle sistemlerin artan otonomi düzeyi insan müdahalesi olmaksızın eylem başlatabilme kapasitesini artırmakta ve bu durum sistem davranışlarının öngörülebilirliğini azaltabilmektedir.

Etken Yapay Zeka Sistemleri Bağlamında Kişisel Verilerin Korunmasına İlişkin Riskler

- veri işleme faaliyetlerinin çok adımlı ve dinamik bir yapı kazanması
- başlangıçta işlenmesi öngörülmeyen verilerin süreçlere dahil edilebilmesi
- anonim olduğu varsayılan veri setlerinin yeniden ilgili kişi ile ilişkilendirilebilir hale gelmesi
- veri işleme faaliyetlerine ilişkin sorumluluk paylaşımının belirsizleşmesi

Kurum Tarafından Önerilen Yaklaşım

Dokümanda etken yapay zeka sistemlerinin tamamen yasaklanması yerine risk temelli ve insan merkezli bir yaklaşım ile yeterli insan gözetiminin sağlanması, sistem davranışlarının izlenilebilirliğinin artmasını sağlayacak mekanizmaların geliştirilmesi, verilerin güncelliğinin gözetilmesi, sürece dahil olan aktörlerin rollerinin ve sorumluluklarının netleştirilmesi, privacy by design ve privacy by default yaklaşımlarının benimsenmesi, çalışan farkındalığının artırılması gibi hususlara önem gösterilmesi tavsiye edilmektedir.

İlgili dokümanın tam metnine buradan ulaşabilirsiniz.

Türkiye'deki Gelişmeler

Duyurular ve Haberler

KVK Kurumu tarafından Kişisel Verilerin Korunması İle İlgili Seçilmiş Güncel Gelişmeler'in 54. bölümü yayımlanmıştır.

KVK Kurumu tarafından yayınlanan gelişmelerden öne çıkan husular aşağıdaki gibidir;

Avrupa Parlamentosu

- "Digital Omnibus" teklifinin dijital düzenlemeler arasındaki bağlantılar ve olası örtüşmeler açısından değerlendirildiği bir analiz çalışması yayımlamıştır.

ANPD (Brezilya)

- Çocukların çevrim içi ortamlarda korunmasına yönelik yaş güvence mekanizmalarını inceleyen çalışmanın İngilizce versiyonunu kamuoyuyla paylaşılmıştır.

Yeni Zelanda Mahremiyet Komisyonerliği

- Eğitim sektöründe görev yapan paydaşlara yönelik olarak çocukların ve gençlerin mahremiyetinin korunmasına ilişkin kapsamlı bir rehber yayımlanmıştır.

Uluslararası Veri Koruma Otoriteleri

- Yapay zeka tarafından üretilen gerçekçi görüntülerin mahremiyet üzerindeki etkilerine ilişkin ortak bir bildiri yayımlayarak özellikle çocuklar bakımından ortaya çıkabilecek risklere dikkat çekilmiştir.

OECD ve UNESCO

- Etken yapay zeka kavramının tanımı ve kullanım alanlarına ilişkin analiz çalışmaları ile yargı alanında yapay zeka kullanımına yönelik bilgilendirici dokümanlar yayımlanmıştır.

Singapur Adalet Bakanlığı

- Hukuk sektöründe üretken yapay zekanın güvenli ve sorumlu kullanımına ilişkin rehber yayımlanmıştır.

İlgili bölümün tamamına buradan ulaşabilirsiniz.

Türkiye'deki Gelişmeler

Duyurular ve Haberler

KVK Kurumu tarafından iş ortaklığı, konsorsiyum ve adi ortaklık yapılarında işlenen kişisel verilerin VERBİS'e bildirimi hakkında kamuoyu duyurusu yayımlanmıştır.

Duyuruda, bu tür yapıların ayrı bir tüzel kişiliği bulunmaması nedeniyle kendi adlarına Veri Sorumluları Siciline kayıt başvurusunda bulunmamaları gerektiği hatırlatılmıştır.

Bu kapsamda, iş ortaklığı veya benzeri yapılar kapsamında gerçekleştirilen faaliyetlerde işlenen kişisel verilere ilişkin VERBİS bildirimlerinin, ortaklığı oluşturan taraflardan Sicile kayıt yükümlülüğü bulunan veri sorumluları tarafından, kendi faaliyetleri ile birlikte ortaklık faaliyetleri çerçevesinde işlenen kişisel verileri de kapsayacak şekilde yapılması gerektiği belirtilmiştir. Duyuru ile, uygulamada yaşanan tereddütlerin giderilmesi ve veri sorumlularının VERBİS yükümlülüklerini doğru şekilde yerine getirmelerine yönelik farkındalık oluşturulması amaçlanmaktadır.

İlgili kamuoyu duyurusuna buradan ulaşabilirsiniz.

KVK Kurumu tarafından açık rıza metinleri ile aydınlatma metinlerinin ayrı ayrı düzenlenmesine ilişkin İlke Kararı hakkında kamuoyu duyurusu yayımlanmıştır.

Duyuruda, aydınlatma yükümlülüğünün kişisel veri işleme faaliyetinin dayanağından bağımsız olarak her durumda ve veri işlemeye başlanmadan önce yerine getirilmesi gerektiği, açık rızaya dayalı veri işleme faaliyetlerinde ise aydınlatma metni ile açık rıza metninin farklı başlıklar altında ve ayrı metinler şeklinde düzenlenmesinin zorunlu olduğu vurgulanmıştır.

Ayrıca, açık rıza dışındaki veri işleme şartlarına dayanılması halinde yalnızca aydınlatma yapılması gerektiği, ilgili kişilerden aydınlatma metninde yer alan hususlar için onay talep edilmemesi gerektiği ve metinlerin her veri sorumlusu tarafından kendi faaliyetlerine özgü, açık, sade ve anlaşılır bir dil kullanılarak hazırlanmasının önem taşıdığı belirtilmiştir. Bunun yanında, muğlak veya yanıltıcı ifadelerden kaçınılması, aşırı uzun ve karmaşık metinlerin kullanılmaması ve işlenen veri kategorileri ile veri işleme amaçlarının açık şekilde ortaya konulması gerektiğine dikkat çekilmiştir.

Söz konusu İlke Kararı ile, veri sorumlularının kişisel verilerin hukuka uygun şekilde işlenmesini teminen gerekli idari ve teknik tedbirleri almaları gerektiği hatırlatılmış; belirtilen yükümlülüklere aykırı hareket edilmesi halinde Kanun'un 18'inci maddesi kapsamında işlem tesis edilebileceği ifade edilmiştir.

İlgili kamuoyu duyurusuna buradan ulaşabilirsiniz.

Türkiye'deki Gelişmeler

Duyurular ve Haberler

KVK Kurulu tarafından, toplu yapılarda apartman/site sakinlerine ait borç bilgilerinin ortak alanlara asılması suretiyle gerçekleştirilen kişisel veri işleme faaliyetlerine ilişkin 18.02.2026 tarihli ve 2026/348 sayılı İlke Kararı hakkında kamuoyu duyurusu yayımlanmıştır.

İlke kararında, apartman ve site yönetimi süreçlerinde aidat, avans ve benzeri borçlara ilişkin bilgilendirme yapılması amacıyla ad-soyad, daire numarası, borç tutarı, gecikme süresi gibi kişisel verileri içeren listelerin asansör, bina girişi ve koridor gibi ortak alanlara asılmasının uygulamada yaygın olduğu belirtilmiştir. Bu kapsamda Kurul, söz konusu uygulamaların kişisel verilerin korunması mevzuatı çerçevesinde değerlendirilmesi gerektiğini vurgulamıştır. İlgili mevzuat kapsamında, kat maliklerinin ortak giderlere katılma yükümlülüğü ve yöneticilerin hesap verme sorumluluğu bulunduğu, ayrıca kat maliklerinin yöneticiyi denetleme hakkına sahip olduğu ifade edilmiştir. Bununla birlikte, bu yükümlülükler kapsamında gerçekleştirilen kişisel veri işleme faaliyetlerinde, seçilecek yöntemlerin 6698 sayılı Kanun'un genel ilkelerine uygun olması gerektiğinin altı çizilmiştir. Bu çerçevede Kurul tarafından yapılan değerlendirmede; kişisel veri içeren borç listelerinin ortak alanlara asılması suretiyle yapılan veri işleme faaliyetinin, Kanun'un 5'inci maddesinde yer alan herhangi bir işleme şartına dayanmadığı ve söz konusu verilerin muhatabı belirli olmayan kişilere ifşa edilmesi nedeniyle veri güvenliğine ilişkin yükümlülüklerin ihlal edildiği belirtilmiştir. Duyuru kapsamında ayrıca, apartman ve site sakinlerine yönelik bilgilendirmelerin; kapalı e-posta grupları, mesajlaşma uygulamaları veya yalnızca ilgili kişilerin erişimine açık sistemler aracılığıyla gerçekleştirilmesi gerektiği ifade edilmiştir. Söz konusu İlke Kararı ile, toplu yapılarda kişisel veri içeren duyuruların ortak alanlarda paylaşılmasının hukuka aykırı olduğuna açıklık getirilmiş; veri sorumlularının teknik ve idari tedbir yükümlülüklerini yerine getirmeleri gerektiği ve aksi halde Kanun'un 18 inci maddesi kapsamında yaptırımlarla karşılaşabileceği hatırlatılmıştır.İlgili kamuoyu duyurusuna buradan ulaşabilirsiniz.

İlgili ilke kararına ilişkin detaylara buradan ulaşabilirsiniz.

Dünyadaki Gelişmeler

Duyurular ve Haberler

Meta tarafından Instagram doğrudan mesajlaşma (DM) özelliğinde sunulan uçtan uca şifreleme (end-to-end encryption) seçeneğinin kaldırılacağı duyurulmuştur.

Şirket tarafından yapılan açıklamada, söz konusu özelliğin kullanıcılar tarafından sınırlı ölçüde tercih edilmesi nedeniyle 8 Mayıs 2026 tarihi itibarıyla desteklenmeyeceği belirtilmiştir. Instagram'da uçtan uca şifreleme özelliği, tüm kullanıcılar için varsayılan olarak sunulmamış; yalnızca belirli bölgelerde ve sohbet bazında isteğe bağlı şekilde etkinleştirilebilmiştir.Meta, uçtan uca şifreli mesajlaşma hizmetini kullanmak isteyen kullanıcıların bu kapsamda WhatsApp uygulamasını tercih edebileceğini ifade etmiştir. Şirketin şifreleme yaklaşımının son yıllarda güvenlik, çocukların korunması ve mahremiyet dengesi bağlamında kamuoyunda tartışma konusu olduğu da bilinmektedir.

Konuya ilişkin detaylı bilgilere buradan ulaşabilirsiniz.

Avrupa Parlamentosu tarafından, siber güvenlik ve kişisel verilerin korunmasına ilişkin riskler nedeniyle milletvekilleri ve Parlamento personeline tahsis edilen kurumsal cihazlarda yer alan bazı yapay zeka özelliklerinin devre dışı bırakıldığı duyurulmuştur.

Kurum içi teknik incelemeler kapsamında, söz konusu yapay zeka araçlarının bazı işlemleri gerçekleştirebilmek için cihaz üzerindeki verileri bulut hizmetleri aracılığıyla harici hizmet sağlayıcılara aktarabildiği, bu durumun ise veri güvenliği ve gizliliği bakımından belirsizlikler doğurabileceği değerlendirilmiştir. Parlamento bilgi teknolojileri birimi tarafından yapılan açıklamada, bu özelliklerin gelişmeye devam ettiği ve hizmet sağlayıcılarla paylaşılan verilerin kapsamının henüz tam olarak netleştirilemediği ifade edilmiştir. Bu nedenle, risklerin açıklığa kavuşturulmasına kadar önleyici bir tedbir olarak ilgili yapay zeka fonksiyonlarının kullanımının geçici olarak sınırlandırıldığı belirtilmiştir.Devre dışı bırakılan özelliklerin; metin yazma ve özetleme yardımcıları, gelişmiş sanal asistanlar ve web sayfası içeriklerini analiz eden yapay zeka araçları gibi cihaza entegre yapay zeka işlevlerini kapsadığı, buna karşılık e-posta, takvim, belge yönetimi ve benzeri günlük kurumsal uygulamaların bu uygulamadan etkilenmediği aktarılmıştır. Parlamento ayrıca üyelerine ve çalışanlarına, özellikle iş amaçlı kullanılan kişisel cihazlarda da benzer veri güvenliği önlemlerini değerlendirmeleri, kurumsal e-posta ve belgelerin yapay zeka araçlarıyla analiz edilmesine izin verirken dikkatli olunması yönünde tavsiyede bulunmuştur. Kurum tarafından yapılan açıklamada, siber güvenlik tehditlerinin sürekli olarak izlenmeye devam edildiği ve veri güvenliğinin sağlanması amacıyla gerekli teknik tedbirlerin süratle hayata geçirileceği vurgulanmıştır.

Konuya ilişkin detaylı bilgilere buradan ulaşabilirsiniz.

Dünyadaki Gelişmeler

Duyurular ve Haberler

Avusturya merkezli kredi derecelendirme kuruluşu CRIF'in veri işleme faaliyetlerine ilişkin yürütülen bir inceleme kapsamında, kamuya açık sicillerde yer alan kişisel verilerin veri aracıları aracılığıyla ticari amaçlarla kullanıldığı ve bu durumun veri minimizasyonu ile amaçla sınırlılık ilkeleri bakımından önemli riskler doğurabileceği yönünde değerlendirmeler yapılmıştır.

Yapılan analizlerde, CRIF veri tabanındaki adres bilgilerinin önemli bir bölümünün adres veri aracıları aracılığıyla ticaret sicili, taşınmaz kayıtları, dernekler sicili ve ticari faaliyet sistemleri gibi kamu kayıtlarından elde edildiği belirtilmiştir. Bununla birlikte, bazı veri sağlayıcılarının milyonlarca kişiye ait veriyi hangi kaynaklardan temin ettiğinin açık şekilde ortaya konulamaması, ilgili kişilerin veri işleme faaliyetlerine ilişkin şeffaflık ve hesap verebilirlik ilkeleri kapsamında haklarını kullanmalarını zorlaştıran bir unsur olarak değerlendirilmiştir.

İlgili değerlendirmenin detaylarına buradan ulaşabilirsiniz.

İspanya Veri Koruma Otoritesi (AEPD) tarafından, biyometrik veri işleme sürecine ilişkin yeterli veri koruma etki değerlendirmesi (DPIA) yapılmadığı gerekçesiyle FC Barcelona'ya 500.000 avro tutarında idari para cezası uygulanmıştır.

Karara konu olayda kulübün, yaklaşık 143.000 üyesine yönelik dijital üyelik güncelleme süreci kapsamında yüz tanıma ve ses doğrulama gibi biyometrik veriler işlediği, ancak söz konusu veri işleme faaliyetleri başlamadan önce GDPR'ın 35. maddesinde öngörülen nitelikte kapsamlı ve hukuka uygun bir DPIA gerçekleştirmediği tespit edilmiştir. Otorite, sunulan değerlendirme dokümanının; işleme faaliyetlerinin sistematik biçimde tanımlanması, veri işleme yöntemlerinin gereklilik ve ölçülülüğünün analiz edilmesi ve ilgili kişilerin hak ve özgürlüklerine yönelik risklerin yeterince ortaya konulması bakımından yetersiz kaldığını belirtmiştir. AEPD ayrıca, biyometrik doğrulama yöntemine alternatif daha az müdahaleci yöntemlerin yeterince değerlendirilmemesinin ve biyometrik verilerin hassas niteliğine uygun risk analizinin yapılmamasının ihlalin temel unsurları arasında yer aldığını vurgulamıştır. İnceleme kapsamında özel nitelikli veri işleme şartlarına ilişkin ayrı bir değerlendirme ise sonuçlandırılmadan dosya yönünden kapatılmıştır. Uygulanan idari para cezasının belirlenmesinde, işlenen veri kapsamı ve etkilenen kişi sayısı ile birlikte kulübün soruşturma sürecindeki iş birliği ve veri işleme faaliyetini şikayet sonrasında durdurmuş olması gibi hafifletici unsurların dikkate alındığı ifade edilmiştir.

Konuya ilişkin detaylı bilgilere buradan ulaşabilirsiniz.

Dünyadaki Gelişmeler

Duyurular ve Haberler

Avrupa Veri Koruma Kurulu (EDPB) tarafından, uluslararası veri koruma uygulama iş birliğinin mevcut durumunu analiz eden ve sınır ötesi yaptırım süreçlerinin güçlendirilmesine yönelik öneriler içeren bir rapor yayımlanmıştır.

Raporda, veri koruma alanında sınır ötesi yaptırım ve denetim süreçlerinde kullanılan bağlayıcı ve bağlayıcı olmayan araçların pratikteki işleyişi incelenmiş; ayrıca tüketicinin korunması ve rekabet hukuku gibi diğer düzenleyici alanlardaki iş birliği modellerinden çıkarılabilecek olası iyileştirme alanları değerlendirilmiştir. Bu kapsamda, veri koruma uygulamalarında daha etkin uluslararası koordinasyon sağlanmasına yönelik karşılaşılan temel zorluklar ile ileriye dönük politika önerilerine yer verilmiştir.

Konuya ilişkin rapora buradan ulaşabilirsiniz.

International Association of Privacy Professionals (IAPP) tarafından, dünya genelinde veri koruma görevlisi (Data Protection Officer – DPO) atanmasına ilişkin ülke bazlı gereklilikleri ortaya koyan kapsamlı bir karşılaştırma çalışması yayımlanmıştır.

Söz konusu çalışmada, farklı veri koruma mevzuatları kapsamında DPO atanmasına ilişkin yükümlülüklerin kapsamı ile bu rolün organizasyon yapısı içindeki konumu ayrıntılı şekilde incelenmektedir. Bu kapsamda çalışmada özellikle aşağıdaki hususlara yer verilmektedir:

- Veri koruma görevlisi atanması gereken kamu kurumları, veri sorumluları ve veri işleyenler ile bu yükümlülüğün ortaya çıktığı veri işleme faaliyetlerinin niteliği,
- DPO'nun organizasyon içerisindeki bağımsızlığı, raporlama yapısı ve görevlerini yerine getirebilmesi için sağlanması gereken kaynaklar,
- Uyumun izlenmesi, veri koruma etki değerlendirmelerine destek verilmesi, ilgili kişi başvurularının yönetimi ve denetim otoriteleri ile iletişim kurulması gibi temel görev ve sorumluluklar,
- DPO'nun sahip olması beklenen mesleki yeterlilikler, veri koruma hukuku ve uygulamalarına ilişkin uzmanlık düzeyi,
- Bazı hukuk sistemlerinde öngörülen atamanın denetim otoritesine bildirilmesi veya iletişim bilgilerinin kamuya açıklanması gibi ilave yükümlülükler.

Çalışma, veri koruma uyum programlarının küresel ölçekte yapılandırılmasına katkı sağlamayı hedeflemekte olup, farklı ülke uygulamalarını karşılaştırmalı olarak ortaya koyarak kuruluşlar açısından uyum stratejilerinin geliştirilmesine yönelik pratik bir referans kaynağı niteliği taşımaktadır.

İlgili çalışmaya buradan ulaşabilirsiniz.

Dünyadaki Gelişmeler

Duyurular ve Haberler

OpenAI tarafından, çevrim içi ortamda çocuk ve genç kullanıcıların korunmasına yönelik olarak ChatGPT kullanıcılarının yaşını tahmin etmeye imkan tanıyan yeni bir güvenlik özelliğinin geliştirildiği duyurulmuştur.

Söz konusu sistem kapsamında, kullanıcıların hesap oluşturma süresi, uygulamayı kullandıkları zaman aralıkları ve platform üzerindeki kullanım davranışları gibi çeşitli veriler analiz edilerek kullanıcının 18 yaşın altında olup olmadığına ilişkin tahminde bulunulması öngörülmektedir.

Bu kapsamda, sistem tarafından reşit olmayan kullanıcı olarak değerlendirilen hesaplar bakımından; şiddet, cinsel içerik, kendine zarar verme veya riskli davranışları teşvik edebilecek içeriklere karşı ilave koruma ve içerik sınırlamaları otomatik olarak devreye alınacaktır. Bununla birlikte, genç kullanıcıların eğitim, yaratıcılık ve bilgi edinme amaçlı kullanımının devam edebileceği ifade edilmektedir.

Ayrıca, hatalı şekilde 18 yaş altı olarak sınıflandırılan kullanıcıların canlı selfie doğrulaması veya resmi kimlik belgesi yüklenmesi yoluyla yaş doğrulaması yaparak söz konusu kısıtlamaları kaldırabilecekleri belirtilmektedir.

Söz konusu gelişmenin, teknoloji şirketlerinin çocukların çevrim içi ortamda korunmasına yönelik sorumluluklarının uluslararası ölçekte artan şekilde tartışıldığı bir dönemde gündeme geldiği değerlendirilmektedir..

İlgili haberin detaylarına buradan ulaşabilirsiniz.

Avrupa Veri Koruma Kurulu (EDPB) tarafından, Koordine Denetim Çerçevesi (CEF) kapsamında silme hakkının uygulanmasına ilişkin yürütülen denetim faaliyetlerinin sonuçlarını içeren nihai rapor ile anonimleştirme ve takma adlandırma konulu paydaş çalıştayına ilişkin değerlendirme raporu yayımlanmıştır.

Söz konusu raporda, Avrupa Birliği Genel Veri Koruma Tüzüğü (“GDPR”) kapsamında silme hakkının uygulanmasına yönelik olarak 32 ulusal veri koruma otoritesinin katılımıyla yürütülen koordineli denetim faaliyetlerinin bulgularına yer verilmiştir. Bu kapsamda, bazı veri sorumlularının silme taleplerinin yönetimine ilişkin yeterli iç prosedürlere sahip olmaması, ilgili kişilere yeterli bilgilendirme yapılmaması ve silme hakkının mutlak bir hak olmaması nedeniyle denge testlerinin uygulanmasında zorluklar yaşanması gibi ortak sorun alanlarının tespit edildiği belirtilmiştir. Ayrıca, bazı veri sorumlularının silme yükümlülüğü yerine geri döndürülemezliği yeterince güvence altına alınmamış anonimleştirme yöntemlerine başvurduğu ve yedekleme sistemlerinden veri silme süreçlerinde uygulama farklılıkları bulunduğu ifade edilmiştir.

İlgili rapora buradan ulaşabilirsiniz.

Dünyadaki Gelişmeler

Duyurular ve Haberler

ABD'de Nvidia Corporation hakkında, yapay zeka modelinin eğitimi kapsamında YouTube verilerinin izinsiz kullanıldığı iddialarına ilişkin toplu dava açılmıştır.

ABD'de açılan davada, Nvidia'nın yapay zeka modeli "Cosmos"un eğitimi amacıyla YouTube platformundaki içerikleri gerekli yetkilendirmeleri almaksızın kullandığı ve bu kapsamda telif hakları ile veri koruma mevzuatının ihlal edilmiş olabileceği ileri sürülmektedir. Dava kapsamında Nvidia Corporation ile YouTube Inc. davalı olarak gösterilmiştir.Söz konusu gelişmenin, yapay zeka sistemlerinin eğitimi sürecinde üçüncü taraf veri kaynaklarının hukuka uygun kullanımı, fikri mülkiyet haklarının korunması ve kişisel verilerin işlenmesine ilişkin yükümlülükler bakımından sektörel ölçekte önemli sonuçlar doğurabileceği değerlendirilmektedir.

İlgili haberin detaylarına buradan ulaşabilirsiniz.

Avrupa Veri Koruma Kurulu (European Data Protection Board – EDPB) tarafından, e-ticaret sitelerinde kullanıcıların hesap oluşturmaya zorlanmasına ilişkin 2/2025 sayılı Tavsiye Kararı yayımlanmıştır.

Avusturya'da faaliyet gösteren kredi derecelendirme kuruluşu CRIF'in veri işleme süreçlerine ilişkin yürütülen incelemelerde, şirketin veri tabanında yer alan adres bilgilerinin önemli bir bölümünün adres veri brokerları aracılığıyla elde edildiği ve bu brokerların verileri büyük ölçüde ticaret sicili, tapu sicili, dernekler sicili ve ticari faaliyet bilgi sistemi gibi kamuya açık kayıt kaynaklarından temin ettiği ortaya konulmuştur. Yapılan değerlendirmelerde, söz konusu kamu sicillerinin esasen hukuki durumun veya mülkiyet ilişkilerinin ispatı amacıyla tutulmasına rağmen, bu kayıtların geniş ölçekte veri toplama ve ticari analiz faaliyetleri kapsamında yeniden kullanıldığına dikkat çekilmiştir.İnceleme kapsamında, kredi skorlama süreçlerinde ekonomik veya finansal performansa ilişkin ayrıntılı verilerden ziyade, kişilerin isim, doğum tarihi ve adres gibi temel kimlik verilerinin kullanıldığı; bu durumun ise kredi risk değerlendirmesinin doğruluğu ve orantılılığı bakımından tartışma yarattığı ifade edilmiştir. Ayrıca kamu sicillerine dijital erişimin yaygınlaşmasıyla birlikte, bu kayıtların toplu şekilde otomatik araçlarla taranmasına (scraping) karşı yeterli teknik ve hukuki koruma mekanizmalarının bulunmadığı yönünde eleştiriler dile getirilmiştir.Konuya ilişkin değerlendirmelerde, kamuya açık verilerin sınırsız biçimde yeniden kullanılabileceği yönündeki yaklaşımın, Genel Veri Koruma Tüzüğü (GDPR) kapsamında düzenlenen amaçla sınırlılık ilkesi ile bağdaşmayabileceği ve bu tür veri işleme faaliyetlerinin hukuka uygunluk bakımından ayrıca incelenmesi gerektiği vurgulanmıştır. Bununla birlikte, veri kaynaklarının şeffaf şekilde açıklanmamasının ilgili kişilerin erişim, düzeltme ve silme gibi veri koruma haklarını etkin biçimde kullanmalarını zorlaştırabileceği belirtilmiştir.

İlgili tavsiye kararına buradan ulaşabilirsiniz.

Dünyadaki Gelişmeler

Duyurular ve Haberler

Avrupa Veri Koruma Kurulu (European Data Protection Board – EDPB) ve Avrupa Veri Koruma Denetçisi (European Data Protection Supervisor – EDPS) tarafından, Avrupa Komisyonu'nun "Digital Omnibus" girişimi kapsamında GDPR ve e-Privacy düzenlemelerinde öngörülen değişikliklere ilişkin ortak görüş yayımlanmıştır.

Söz konusu ortak görüşte, önerilen değişikliklerin özellikle kişisel veri tanımının daraltılması, yapay zeka eğitimi bakımından yeni hukuki dayanakların oluşturulması ve ilgili kişilerin erişim hakkının sınırlandırılması gibi temel veri koruma ilkeleri üzerinde önemli etkiler doğurabileceği yönünde ciddi endişeler dile getirilmiştir. Değerlendirmede, GDPR kapsamında yer alan kişisel veri tanımının daraltılmasına yönelik teklifin, yalnızca teknik bir değişiklik veya içtihatların kodifikasyonu niteliğinde olmadığı; aksine veri koruma rejiminin kapsamını esaslı biçimde etkileyebileceği ifade edilmiştir. Ayrıca Avrupa Komisyonu'na takma adlandırılmış verilerin kapsamını belirleme konusunda geniş yetkiler tanınmasının, bazı veri işleme faaliyetlerinin GDPR uygulama alanı dışında bırakılmasına yol açabilecek riskler barındırdığı belirtilmiştir.

Ortak görüşte, yapay zeka sistemlerinin eğitimi bakımından meşru menfaat hukuki sebebine dayalı veri işleme önerisinin de hukuki belirsizlikleri tamamen ortadan kaldırmadığı; veri sorumlularının bu kapsamda her halükarda üç aşamalı denge testini yürütmek zorunda kalacağına dikkat çekilmiştir. Buna ek olarak, ilgili kişilerin erişim hakkının belirli amaçlarla sınırlandırılmasına yönelik düzenleme teklifinin, Avrupa Birliği Adalet Divanı içtihadı ile uyumlu olmayabileceği değerlendirilmiştir.

EDPB ve EDPS, Avrupa Komisyonu'nun idari yüklerin azaltılması ve düzenleyici çerçevenin sadeleştirilmesi yönündeki hedeflerini anlaşılır bulmakla birlikte, mevcut teklif metinlerinin uygulamada yeterli açıklık ve öngörülebilirlik sağlamadığını vurgulamıştır. Ortak görüşte ayrıca, önerilen bazı değişikliklerin veri koruma uygulamalarını basitleştirmek yerine karmaşıklığı artırabileceği ve özellikle büyük teknoloji şirketleri bakımından farklı sonuçlar doğurabileceği yönünde değerlendirmelere yer verilmiştir.

İlgili görüşün detaylarına buradan ulaşabilirsiniz.

Dünyadaki Gelişmeler

Duyurular ve Haberler

Avrupa Komisyonu'nun "Digital Omnibus" girişimi kapsamında GDPR ve e-Privacy düzenlemelerinde öngörülen değişikliklere ilişkin kapsamlı hukuki analiz içeren "Digital Omnibus Report V3" başlıklı rapor yayımlanmıştır.

Raporda, Komisyonun 19 Kasım 2025 tarihli teklifinde yer alan veri koruma alanına ilişkin düzenlemeler mevcut mevzuat ile karşılaştırmalı olarak incelenmiş; önerilen değişikliklerin veri sahiplerinin hakları, veri sorumlularının yükümlülükleri ve denetim otoritelerinin uygulamaları bakımından doğurabileceği etkiler değerlendirilmiştir.

24 Şubat 2026 tarihinde yayımlanan üçüncü versiyonun, önceki analizlere ek olarak Avrupa Veri Koruma Kurulu (EDPB) ile Avrupa Veri Koruma Denetçisi'nin (EDPS) ortak görüşüne ilişkin değerlendirmeleri de içerdiği belirtilmiştir.

İlgili rapora buradan ulaşabilirsiniz.

Avrupa Komisyonu'nun "Digital Omnibus" girişimi kapsamında GDPR'da öngörülen sadeleştirme önerilerinin işletmelerin uyum süreçlerine etkisini inceleyen ve veri koruma profesyonellerinin görüşlerine dayanan bir anket çalışması yayımlanmıştır.

Söz konusu çalışmada, veri koruma görevlileri (DPO) ve gizlilik profesyonellerinin GDPR hükümlerinin uygulamada oluşturduğu iş yüküne ilişkin değerlendirmelerine yer verilmiş; katılımcıların büyük çoğunluğunun veri sahiplerine tanınan hakların daraltılması yerine belgelendirme yükümlülüklerinin azaltılması ve hukuki düzenlemelerin daha açık ve öngörülebilir hale getirilmesi yönünde beklenti içinde olduğu belirtilmiştir.Raporda ayrıca, erişim hakkı başta olmak üzere veri sahibi haklarının çoğu işletme bakımından sınırlı bir operasyonel yük oluşturmasına rağmen bireylerin veri koruma haklarının etkin şekilde kullanılmasını sağladığı; buna karşılık GDPR'daki temel veri işleme ilkeleri ve şeffaflık yükümlülüklerinin daha fazla uyum çabası gerektirmekle birlikte veri koruma açısından yüksek fayda sağladığı ifade edilmiştir. Bunun yanında, risk temelli yaklaşımın uygulamada özellikle küçük ve orta ölçekli işletmeler açısından belirsizlik yaratabildiği, katılımcıların önemli bir bölümünün şirket büyüklüğü veya işlenen veri hacmine dayalı daha net eşiklerin belirlenmesini ve belirli veri işleme faaliyetleri bakımından "beyaz liste" veya "kara liste" gibi daha somut rehberlik mekanizmalarının oluşturulmasını desteklediği vurgulanmıştır.Çalışmada ayrıca, işletmeler arası veri işleme ilişkilerinden kaynaklanan sözleşmesel uyum maliyetlerinin azaltılmasına yönelik yapısal düzenlemelerin veri koruma uyumunu güçlendirebileceği değerlendirilmiştir.

İlgili çalışmaya ilişkin detayı bilgiye buradan ulaşabilirsiniz.

Dünyadaki Gelişmeler

Güncel Kararlar

Lüksemburg İdare Mahkemesi tarafından, Amazon hakkında Lüksemburg Veri Koruma Otoritesi (Commission Nationale pour la Protection des Données – CNPD) tarafından 2021 yılında verilen 746 milyon Avro tutarındaki GDPR para cezasına ilişkin kararın iptal edildiği, ancak dosyanın yeniden değerlendirilmek üzere CNPD'ye geri gönderildiği duyurulmuştur.

Mahkeme, para cezasına ilişkin kararı usul yönünden iptal etmekle birlikte, ilgili dönemde tespit edilen Genel Veri Koruma Tüzüğü (GDPR) ihlallerinin esasına ilişkin değerlendirmeleri geçerli kabul etmiştir. Kararda, düzenleyici otoritenin yaptırım sürecinde bazı hukuki incelemeleri yeterince gerçekleştirmediği ve özellikle Avrupa Birliği Adalet Divanı'nın 2023 tarihli içtihadı doğrultusunda, şirketin ihlali kasten veya ihmalen gerçekleştirip gerçekleştirmediğine yönelik değerlendirme yapılmadığı belirtilmiştir. Ayrıca mahkeme, yaptırım türünün belirlenmesi sürecinde daha hafif bir tedbirin uygulanıp uygulanamayacağına ilişkin orantılılık değerlendirmesinin yeterli şekilde yapılmadığını tespit etmiş ve CNPD'nin bu hususları yeniden incelemesi gerektiğini ifade etmiştir. Söz konusu süreç, Fransa'da bir dijital haklar savunuculuğu grubu tarafından organize edilen kullanıcı şikayetleri üzerine başlatılmış olup, Amazon'un çevrim içi davranışsal reklamcılık faaliyetleri kapsamında kişisel verilerin işlenmesine ilişkin açık rıza mekanizmalarının yeterince sağlanmadığı iddialarına dayanmaktadır. Amazon'un Avrupa merkezinin Lüksemburg'da bulunması nedeniyle inceleme CNPD tarafından yürütülmüştür.Taraflar, yargılama sürecinde ilgili veri koruma uygulamalarına ilişkin eksikliklerin büyük ölçüde giderildiğini belirtmiş olup, CNPD'nin dosyayı yeniden ele alarak GDPR hükümlerinin etkin şekilde uygulanmasını sağlamaya yönelik süreci sürdürmesi beklenmektedir.

İlgili karara ilişkin detaylara buradan ulaşabilirsiniz.

Avrupa Birliği Adalet Divanı, GDPR kapsamında veri sahibinin erişim taleplerinin hangi durumlarda aşırı veya kötüye kullanım niteliği taşıyabileceğine ilişkin önemli bir karar vermiştir.

Karar, bir veri sahibinin bir şirkete kişisel verilerini paylaşarak kısa süre sonra GDPR m. 15 kapsamında erişim talebinde bulunması ve talebin reddedilmesi üzerine manevi tazminat talep etmesi üzerine verilen ön karar başvurusuna ilişkindir. ABAD, erişim talebinin ilk kez yapılmış olmasının tek başına talebin aşırı sayılmasına engel olmadığını belirtmiştir. Talebin, verilerin işlenip işlenmediğini öğrenmekten ziyade tazminat zemini oluşturma amacı taşıdığının somut şekilde ortaya konulması halinde, veri sorumlusunun talebi reddedebileceği ifade edilmiştir. Mahkeme ayrıca, erişim hakkının ihlalinin tek başına GDPR m. 82 kapsamında tazminat talebine konu olabileceğini, ancak veri sahibinin zararını ve ihlal ile zarar arasındaki nedensellik bağını ortaya koyması gerektiğini vurgulamıştır.

İlgili karara ilişkin detaylara buradan ulaşabilirsiniz.

Dünyadaki Gelişmeler

Güncel Kararlar

Fransa Danıştayı tarafından, reklam teknolojisi şirketi Criteo hakkında kişiselleştirilmiş reklam amaçlı çerez kullanımı kapsamında verilen 40 milyon avro tutarındaki idari para cezasının hukuka uygun olduğuna hükmedilmiştir.

Fransa Veri Koruma Otoritesi (CNIL) tarafından uygulanan cezanın, kullanıcıların geçerli rızası olmaksızın kişisel verilerin işlenmesi, veri işleme amaçları hakkında yeterli bilgilendirme yapılmaması, erişim ve silme taleplerinin gereği gibi yerine getirilmemesi ve iş ortaklarıyla müşterek veri sorumluluğuna ilişkin gerekli düzenlemelerin tesis edilmemesi gerekçelerine dayandığı belirtilmiştir. Mahkeme, çerezler aracılığıyla toplanan ve farklı veri unsurlarıyla ilişkilendirilebilen tarama verilerinin kişisel veri niteliği taşıdığını değerlendirerek, veri sorumlusunun rıza alma yükümlülüğünden sözleşmesel düzenlemeler yoluyla kaçınamayacağını vurgulamıştır. Ayrıca silme taleplerine rağmen verilerin işlenmeye devam edilmesinin GDPR kapsamında hukuka aykırılık oluşturduğu ifade edilmiştir. Danıştay, ihlallerin kapsamı ve etkilenen kişi sayısı dikkate alındığında uygulanan idari para cezasının ölçülü ve caydırıcı olduğu sonucuna vararak şirketin itirazını reddetmiştir.

İlgili karara ilişkin detaylara buradan ulaşabilirsiniz.

İtalya Veri Koruma Otoritesi (Garante Per La Protezione Dei Dati Personali) tarafından, doğrudan pazarlama faaliyetleri kapsamında kişisel verilerin hukuka aykırı şekilde işlenmesi nedeniyle Verisure Italia hakkında 400.000 € tutarında idari para cezası uygulanmıştır.

Otorite tarafından yürütülen incelemede, ilgili kişilerin pazarlama iletişimlerine karşı itiraz hakkını kullanmalarına rağmen reklam amaçlı mesaj gönderilmeye devam edildiği ve potansiyel müşterilerden pazarlama amaçlı geçerli bir açık rıza alınmadığı tespit edilmiştir. Ayrıca, yalnızca teklif talebinde bulunulmasının pazarlama iletişimlerine onay verilmiş gibi değerlendirilmesinin GDPR hükümleriyle bağdaşmadığı belirtilmiştir. Karar da, veri saklama sürelerinin ölçüsüz şekilde uzun tutulmasının ve aydınlatma yükümlülüğünün gereği gibi yerine getirilmemesinin de ihlal teşkil ettiği vurgulanmıştır.

İlgili karara ilişkin detaylı bilgiye buradan ulaşabilirsiniz.

Dünyadaki Gelişmeler

Güncel Kararlar

İspanya Veri Koruma Otoritesi (Agencia Española de Protección de Datos – AEPD) tarafından, mobil hat sahipliğinin hukuka aykırı şekilde değiştirilmesi ve üçüncü bir kişiye usulsüz şekilde yedek SIM kart verilmesi nedeniyle bir telekomünikasyon hizmet sağlayıcısına 300.000 € tutarında idari para cezası uygulanmıştır.

Otorite tarafından yürütülen incelemede, veri sorumlusunun müşteri hizmetleri kanalı üzerinden gerçekleştirilen hat devri talebinde kimlik doğrulama prosedürlerini eksiksiz uygulamadığı, ardından fiziksel mağaza aracılığıyla aynı hat için üçüncü kişiye yedek SIM kart düzenlendiği tespit edilmiştir. Bu süreç sonucunda ilgili kişinin mobil hizmete erişiminin kesildiği ve yetkisiz bankacılık işlemlerine maruz kaldığı belirlenmiştir. Kararda, veri sorumlusunun yalnızca teknik ve idari tedbirleri belirlemesinin yeterli olmadığı, bu tedbirlerin uygulamada etkin biçimde hayata geçirilmesini sağlama yükümlülüğünün de bulunduğu vurgulanmıştır. Ayrıca çalışanların veya iş ortaklarının iç prosedürlere uymamasından doğan ihlallerden veri sorumlusunun sorumluluğunun devam ettiği ifade edilmiştir. AEPD, söz konusu veri işleme faaliyetinin geçerli bir hukuki dayanağa dayanmadığına hükmederek ihlali GDPR madde 6/1 kapsamında değerlendirmiş ve ihlalin ağır nitelikte olduğuna karar vermiştir.

İlgili karara ilişkin detaylara buradan ulaşabilirsiniz.

Fransa Veri Koruma Otoritesi (Commission Nationale de l'Informatique et des Libertés – CNIL) tarafından, abonelere ait kişisel verilerin güvenliğinin sağlanmasına yönelik yeterli teknik ve idari tedbirlerin alınmaması nedeniyle FREE MOBILE ve FREE şirketlerine toplam 42 milyon € tutarında idari para cezası uygulanmıştır.

Yapılan incelemelerde, bir siber saldırı sonucunda milyonlarca aboneye ait kişisel verilere bazı durumlarda finansal bilgiler de dahil olmak üzere yetkisiz erişim sağlandığı, şirketlerin özellikle kimlik doğrulama ve sistem güvenliği tedbirlerinin yetersiz olduğu tespit edilmiştir. Ayrıca veri ihlalinden etkilenen kişilere yapılan bilgilendirmenin GDPR kapsamında gerekli unsurları içermediği ve bazı verilerin gereğinden uzun süre saklandığı belirlenmiştir. CNIL, ihlalin kapsamı ve etkilenen kişi sayısını dikkate alarak FREE MOBILE'a 27 milyon €, FREE şirketine ise 15 milyon € idari para cezası verilmesine karar vermiştir.

İlgili karara ilişkin detaylara buradan ulaşabilirsiniz.

Dünyadaki Gelişmeler

Güncel Kararlar

Belçika Veri Koruma Otoritesi (Autorité de protection des données/ Gegevensbeschermingsautoriteit–APD/GBA) tarafından, bir hastanenin elektronik sağlık kayıtlarına erişimin yönetilmesine yönelik yeterli teknik ve idari tedbirleri almaması nedeniyle kınama kararı verilmiştir.

Yapılan incelemede, bir fizyoterapistin yetkisi dışında hamile bir hastaya ve doğmamış çocuğuna ait sağlık kayıtlarına eriştiği ve bu kayıtlarda yer alan çocuğun cinsiyetine ilişkin bilgiyi hasta ile paylaştığı tespit edilmiştir. Otorite, doğmamış çocuğa ait kişisel verilerin de somut olayın koşulları çerçevesinde veri koruma hukuku kapsamında korunması gerektiğini değerlendirmiştir.

Karar da, söz konusu hukuka aykırı erişimin doğrudan ilgili sağlık personelinin sorumluluğunda olduğu belirtilmekle birlikte, hastanenin erişim yetkilerinin yönetimi ve veri güvenliğinin sağlanmasına ilişkin yeterli önlemleri uygulamaması nedeniyle GDPR'ın veri güvenliği, hesap verebilirlik ve veri sorumluluğuna ilişkin hükümlerini ihlal ettiği sonucuna varılmıştır. Bu kapsamda hastane hakkında kınama yaptırımı uygulanmıştır..

İlgili karara ilişkin detaylara buradan ulaşabilirsiniz.

Polonya Veri Koruma Otoritesi (Urząd Ochrony Danych Osobowych – UODO) tarafından, veri koruma görevlisinin (DPO) görevini bağımsız şekilde yerine getirmesini sağlayacak organizasyonel yapının oluşturulmaması nedeniyle Poczta Polska S.A. hakkında yaklaşık 978.000 PLN tutarında idari para cezası uygulanmıştır.

Otorite tarafından yürütülen incelemede, veri koruma görevlisi olarak atanan kişinin aynı zamanda kişisel veri işleme faaliyetleriyle doğrudan bağlantılı yönetsel görevler üstlendiği ve bu durumun çıkar çatışmasına yol açarak DPO'nun bağımsızlığını zedelediği tespit edilmiştir. Ayrıca şirketin, DPO görevine ilişkin olası çıkar çatışmalarını değerlendiren bir analiz yapmadığı ve iç düzenlemelerinde bu görevin önceliğine ilişkin açık hükümlere yer vermediği belirlenmiştir.

Karar da, veri koruma görevlisinin görevlerini etkili ve tarafsız şekilde yerine getirebilmesi için organizasyonel ve işlevsel bağımsızlığının sağlanmasının GDPR kapsamında temel bir yükümlülük olduğu vurgulanmıştır. İnceleme sürecinde şirketin DPO'nun organizasyon içindeki konumunu değiştirerek doğrudan üst yönetime bağlı hale getirdiği dikkate alınmakla birlikte, tespit edilen ihlaller nedeniyle idari para cezası uygulanmasına karar verilmiştir..

İlgili karara ilişkin detaylara buradan ulaşabilirsiniz.

Dünyadaki Gelişmeler

Güncel Kararlar

Fransa Veri Koruma Otoritesi (Commission Nationale de l'Informatique et des Libertés – CNIL) tarafından, iş arayan kişilere ait kişisel verilerin güvenliğinin sağlanmasına yönelik yeterli teknik ve organizasyonel tedbirlerin alınmaması nedeniyle FRANCE TRAVAIL hakkında 5 milyon € tutarında idari para cezası uygulanmıştır.

Otorite tarafından yapılan incelemede, saldırganların sosyal mühendislik yöntemleri kullanarak sisteme sızdığı ve son 20 yıl içerisinde kuruma kayıtlı olan veya çevrim içi aday hesabı bulunan milyonlarca kişinin kimlik numarası, iletişim bilgileri ve diğer kişisel verilerine erişim sağladığı tespit edilmiştir. CNIL, özellikle kullanıcı hesaplarına erişim için uygulanan kimlik doğrulama mekanizmalarının yeterince güçlü olmaması, anormal erişim faaliyetlerini tespit etmeye yönelik kayıt ve izleme sistemlerinin yetersizliği ile erişim yetkilerinin gereğinden geniş tanımlanmış olmasını veri güvenliği yükümlülüğünün ihlali olarak değerlendirmiştir.

Kararda ayrıca, veri sorumlusunun risk analizleri kapsamında gerekli güvenlik önlemlerini önceden tespit etmiş olmasına rağmen bunları fiilen uygulamaya koymamasının ihlalin ağırlığını artırdığı vurgulanmıştır. CNIL, para cezasının yanı sıra kurumun belirli bir takvim çerçevesinde düzeltici önlemleri hayata geçirdiğini belgelemekle yükümlü olduğunu; aksi halde gecikilen her gün için ek idari yaptırım uygulanabileceğini belirtmiştir.

İlgili karara ilişkin detaylara buradan ulaşabilirsiniz.

İsveç Veri Koruma Otoritesi (Integritetsskyddsmyndigheten – IMY) tarafından, kişisel verilerin güvenliğinin sağlanmasına yönelik yeterli teknik ve organizasyonel tedbirlerin alınmaması nedeniyle Sportadmin hakkında 6 milyon İsveç kronu tutarında idari para cezası uygulanmıştır.

Otorite tarafından yürütülen incelemede, Ocak 2025'te gerçekleşen bir siber saldırı sonucunda 2,1 milyondan fazla kişiye ait verilerin ele geçirilerek Darknet ortamında yayımlandığı tespit edilmiştir. İhlalin özellikle çocuklara ve gençlere ait kimlik ve iletişim bilgileri, kişisel kimlik numaraları, bağlı oldukları spor kulübü bilgileri ile bazı sağlık verilerini kapsadığı belirlenmiştir.Kararda, veri sorumlusunun sistemlerindeki güvenlik açıklarının saldırıdan önce uzun süredir bilindiği, ancak bu risklerin giderilmesine yönelik yeterli ve etkili önlemlerin alınmadığı vurgulanmıştır. Ayrıca gerçek zamanlı saldırı tespit mekanizmalarının ve mevcut güvenlik önlemlerinin etkinliğini düzenli olarak değerlendirmeye yönelik süreçlerin bulunmamasının, ihlalin kapsamını artıran unsurlar arasında yer aldığı ifade edilmiştir.IMY, veri güvenliği yükümlülüğünün veri işleme faaliyetinin niteliği ve işlenen verilerin hassasiyeti dikkate alınarak yerine getirilmesi gerektiğini hatırlatarak, Sportadmin'in Genel Veri Koruma Tüzüğü'nün (GDPR) 32'nci maddesini ihlal ettiğine hükmetmiştir.

İlgili karara ilişkin detaylara buradan ulaşabilirsiniz.

Dünyadaki Gelişmeler

Güncel Kararlar

Birleşik Krallık Veri Koruma Otoritesi (Information Commissioner's Office – ICO) tarafından, çocukların kişisel verilerinin korunmasına yönelik yeterli yaş doğrulama tedbirlerinin uygulanmaması nedeniyle Reddit hakkında 14,47 milyon sterlin tutarında idari para cezası uygulanmıştır.

Otorite tarafından yürütülen incelemede, platformun kullanım şartlarında 13 yaş altı kullanıcıların yasaklanmasına rağmen etkili bir yaş doğrulama mekanizmasının uzun süre tesis edilmediği ve bu nedenle çocukların uygunsuz içeriklere maruz kalma riski ile karşı karşıya kaldığı tespit edilmiştir.Kararda, kullanıcı yaşının yalnızca beyana dayalı olarak belirlenmesinin çocukların korunması bakımından yeterli bir güvence sağlamadığı; ayrıca şirketin çocuklara yönelik riskleri değerlendirmek ve azaltmak amacıyla veri koruma etki değerlendirmesi (DPIA) gerçekleştirmediği vurgulanmıştır. Bu kapsamda, 13 yaş altı kullanıcıların kişisel verilerinin işlenmesinin hukuki dayanağının bulunmadığı değerlendirilmiştir.

ICO, büyük ölçekli çevrim içi platformların çocukların kişisel verilerinin korunmasına yönelik daha güçlü teknik ve organizasyonel önlemler alması gerektiğini belirtmiş; Reddit'in Temmuz 2025 itibarıyla bazı yaş doğrulama tedbirleri uygulamaya başladığını ancak bu önlemlerin yeterli görülmeyerek sürecin izlenmeye devam edildiğini ifade etmiştir..

İlgili karara ilişkin detaylara buradan ulaşabilirsiniz.

İtalya Veri Koruma Otoritesi (Garante per la Protezione dei Dati Personali) tarafından, çalışanlara ait hassas nitelikli kişisel verilerin hukuka aykırı şekilde toplanması ve uzun süre saklanması nedeniyle Amazon Italia Logistica'nın söz konusu veri işleme faaliyetlerini derhal durdurmasına karar verilmiştir.

Otorite tarafından yapılan incelemelerde, şirketin çalışanların devamsızlık sonrası yapılan görüşmeler kapsamında sağlık durumlarına, sendikal faaliyetlerine ve aile hayatlarına ilişkin ayrıntılı bilgileri sistematik olarak kaydettiği ve bu verileri işten ayrılmalarından sonra dahi uzun süre sakladığı tespit edilmiştir. Söz konusu verilerin çok sayıda yönetici tarafından erişilebilen bir iç platform üzerinden işlendiği belirlenmiştir.Kararda ayrıca, çalışanların mesleki yeterliliklerinin değerlendirilmesiyle doğrudan ilgili olmayan bu tür verilerin işlenmesinin iş hukuku ve veri koruma mevzuatına aykırılık teşkil ettiği vurgulanmış; tuvalet ve dinlenme alanları yakınındaki gözetim kameraları aracılığıyla elde edilen verilerin işlenmesine de son verilmesi gerektiği ifade edilmiştir.

İlgili karara ilişkin detaylara buradan ulaşabilirsiniz.

www.dlattorneysatlaw.com

İstanbul'da bulunan DL Avukatlık Bürosu ("DL"), müvekkillerine genellikle kurumsal çözümler üzerinde odaklanmış kapsamlı hukuki hizmet sunmaktadır. DL Türkiye'nin önde gelen hukuk bürolarından biri olarak, ticari ve vergisel çözümler sunarak piyasadaki deneyimi ile müvekkillerine çözüm odaklı ve kişiye özel hukuki hizmet vermektedir.

Büromuzda hizmet veren avukatlar, Şirketler Hukuku – Birleşme & Devralmalar, Regüle Sektörler, Rekabet Hukuku, Kişisel Verilerin Korunması, Ticaret Hukuku, İş Hukuku, Tasfiye ve Kurumsal Yeniden Yapılandırma, Taşınmazlar, Davalar ve Vergi Uyuşmazlıkları dahil ve fakat bunlarla sınırlı olmamak üzere birçok alanında uzmanlaşmışlardır. DL Avukatlık Bürosu şirketler hukuku alanında karmaşık Birleşme & Devralma işlemlerinde hukuki danışmanlık hizmeti sunmak başta olmak üzere ortak girişim, yeniden yapılandırma ve genel şirketler hukuku konularına ilişkin hukuki görüş ve destek vermektedir. DL Avukatlık Bürosu gerek yerli gerekse yabancı şirket ve şirket gruplarına hizmet vermektedir.