SAYI: 44

MCLEGAL
Metin-Çiçek Avukatlık Ortaklığı
Attorney Partnership

VERİ & TEKNOLOJİ HUKUKU BÜLTENİ

EYLÜL 2024

GÜNCEL HABERLER

- 2024-2028 Ulusal Siber Güvenlik Stratejisi
- Eylül Ayı İçerisinde Bildirilen Kişisel Veri İhlalleri
- Ticari Elektronik İleti Yönetim Sİstemi Entegratörleri Hakkında Tebliğ
- ''108 Milyon Vatandaşa Ait Verİlerin Çalınmasına'' İlişkin Haberler Hakkında Kamuoyu Duyurusu Yayımlandı

GLOBAL GELİŞMELER

- İrlanda Veri Koruma Otoritesi X'e Karşı Açılan Davaların Geri Çekildiğini Duyurdu
- Veri Sorumlularının Veri İşleme Faalİyetlerine İlİşkin İnteraktİf Çalışma Birleşik Krallık Veri Koruma Otorİtesi Tarafından Yayımlandı
- Hollanda Veri Koruma Otoritesi, İnternetten Toplanan Milyarlarca Yüz Görüntüsünden Veritabanı Oluşturduğu Gerekçesiyle Clearview AI'a 30,5 Milyon Euro Ceza Kesti
- İrlanda Veri Koruma Otoritesi, Facebook'un Ana Şİrketi Meta'ya Parola Saklama Süreçleri Nedeniyle 91 Milyon Euro Para Cezası Verdi
- Kaliforniya Gizlilik Koruma Ajansı, Karanlık Tasarımlar (Dark Patterns) Konusuyla İlgili Bir Uygulama Bilgilendirmesi Yayınladı

YAPAY ZEKA VE İNSAN HAKLARI

Avrupa Konseyi, yapay zeka konusunda yasal olarak bağlayıcı ilk uluslararası anlaşma niteliğinde olan, “Yapay Zeka ve İnsan Hakları, Demokrasi ve Hukukun Üstünlüğü Çerçeve Sözleşmesi’ni imzaya sundu.

Yapay zeka teknolojilerinin hızla gelişmesi, insan hakları üzerinde önemli etkiler yaratmaktadır. Yapay zekanın kullanımı, ayrımcılıkla mücadele, şeffaflık ve hesap verebilirlik gibi temel insan hakları ilkelerine dikkat edilmesi gereğini doğurur. Özellikle mahremiyet, veri güvenliği ve bireysel otonomi gibi konularda riskler artmaktadır. Avrupa Konseyi tarafından geliştirilen "Yapay Zeka, İnsan Hakları, Demokrasi ve Hukukun Üstünlüğü Çerçeve Sözleşmesi" bu sorunlara çözüm getirmeyi hedeflemektedir.

Yapay zekanın kötüye kullanımına karşı bir önlem olarak, devletler ve şirketler, yapay zeka uygulamalarının etik ilkelerle uyumlu olmasını sağlamakla yükümlü tutulmuştur. Ayrıca, bu sistemlerin geliştirilmesinde toplumsal cinsiyet eşitliği ve ayrımcılık yasağı gibi temel insan hakları ilkelerinin de korunması gerekmektedir.

Yapay zeka teknolojilerinin insan haklarına zarar vermeden geliştirilmesi, güvenli ve adil bir dijital dünyanın temelidir. Avrupa Konseyi'nin çerçeve sözleşmesi, bu alandaki standartları belirleyerek, devletler ve şirketler için yol gösterici nitelik taşımaktadır.

ULUSAL SİBER GÜVENLİK STRATEJİSİ VE EYLEM PLANI YAYINLANDI

'Cumhurbaşkanlığı tarafından Ulusal Siber Güvenlik Stratejisi ve Eylem Planı (2024-2028)'na ilişkin 2024/11 sayılı genelge 07/09/2024 tarihli ve 32655 sayılı Resmî Gazete' de yayınlanmıştır.

2024-2028 Ulusal Siber Güvenlik Strateji Belgesi'nin, Türkiye'nin dijital dünyada karşı karşıya olduğu siber tehditlere karşı koymayı amaçlayan kapsamlı bir yol haritası niteliği taşıması hedeflenmiştir. Türkiye'nin siber güvenliğinin güçlendirilmesi için yenilikçi ve sürdürülebilir çözümler geliştirmek amaçlanmıştır.

Strateji belgesi, siber güvenliğin ülke açısından ne denli önemli olduğuna vurgu yaparak başlamakta olup akabinde Türkiye'nin bu alandaki hedeflerine ulaşmak için belirlenmiş stratejik unsurları sıralamıştır.

Siber güvenliğin milli güvenliğin temel bir parçası olduğuna dikkat çekerken, özellikle kritik altyapıların korunması ve yerli teknolojilerin geliştirilmesine odaklanmıştır.

2024-2028 döneminde 6 stratejik amaç belirlenmiştir:

1. **Siber Dayanıklılık:** Kritik altyapılar başta olmak üzere, bilgi ve iletişim teknolojileri altyapılarının siber tehditlere karşı dayanıklılığının artırılması

2. Proaktif Siber Savunma: Tehditleri erken aşamada tespit edip önlemeye yönelik çalışmalar

3. İnsan Odaklı Yaklaşım: Farkındalık artırma ve siber güvenlik eğitimlerine odaklanılması

4.Teknolojinin Güvenli Kullanımı: Yeni teknolojilerin güvenliği için tedbirler alınması

5. Yerli ve Milli Teknolojiler: Siber tehditlere karşı yerli ürünlerin geliştirmesi ve kullanılması

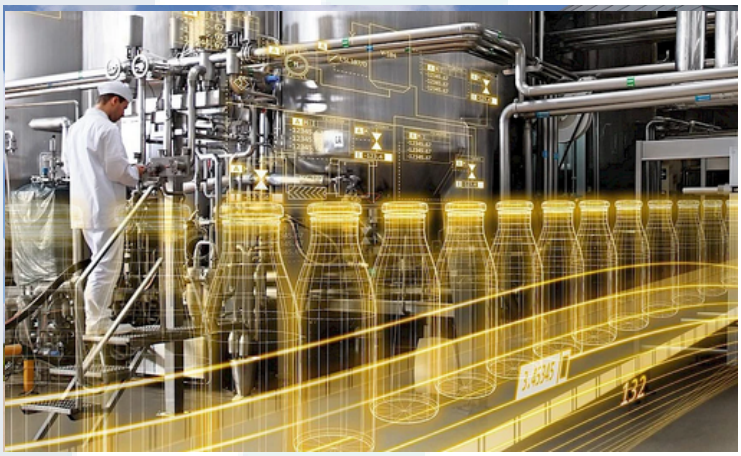
6.Uluslararası Alanda Türkiye Markası: Türkiye'nin siber güvenlikte uluslararası görünürlüğünü artırma ve iş birliklerinin geliştirilmesi

Ulaştırma ve Altyapı Bakanlığı tarafından hazırlanan Ulusal Siber Güvenlik Stratejisi ve Eylem Planı'na buradan ulaşabilirsiniz.

GÜNCEL HABERLER

EYLÜL AYI İÇERİSİNDE BİLDİRİLEN KİŞİSEL VERİ İHLALLERİ

Kentaş Gıda



Veri sorumlusu olan Kentaş Gıda Pazarlama ve Dağıtım Ticaret Ltd. Şti. tarafından Kurula iletilen veri ihlal bildiriminde özetle;

- 12.09.2024 tarihinde fidye yazılımı saldırısına maruz kalındığı ve dosyaların şifrelendiği,
- İhlalden muhasebe programına ait bilgilerin etkilendiği, dolayısıyla muhasebeyle ilgili fatura bilgileri ile veri sorumlusuna ait resmi defterlere, borç/alacak hesaplarına ve sistemde kayıtlı olan personel adres ve kimlik numaralarına ulaşıldığının tahmin edildiği,
- İhlalden etkilenen ilgili kişi gruplarının çalışanlar, kullanıcılar ve müşteriler ile potansiyel müşteriler olduğu,
- İhlalden tahmini 1000 kişinin etkilendiği,
- İhlalden etkilenen kişisel veri kategorilerinin kimlik, iletişim, lokasyon, müşteri işlem, işlem güvenliği, finans, pazarlama olduğu

bilgilerine yer verilmiştir.

Konuya ilişkin inceleme devam etmekle birlikte, Kişisel Verileri Koruma Kurulunun 19.09.2024 tarih ve 2024/1627 sayılı Kararı ile söz konusu veri ihlali bildiriminin Kurumun internet sitesinde ilan edilmesine karar verilmiştir.

İlgili karara buradan ulaşabilirsiniz.

İncirli Sağlık

Veri sorumlusu olan İncirli Sağlık ve Sosyal Tesisler A.Ş. tarafından Kuruma gönderilen kişisel veri ihlali bildiriminde özetle;

- İhlalin; veri sorumlusunun bilişim sistemine dışarıdan müdahale edilerek kayıtlı olan tüm uygulamalar dahil tüm verilerin silinmesi, yok edilmesi ve yedeklerinin imha edilmesi şeklinde gerçekleştiği,
- İhlalin 14.08.2024 tarihinde başladığı, 04.09.2024 tarihinde sona erdiği,
- İhlalden etkilenen kişi grubunun çalışanlar ve hastalar olduğu,
- İhlalden etkilenen kişisel veri kategorilerinin; kimlik, iletişim, lokasyon, özlük, hukuki işlem, müşteri işlem, fiziksel mekan güvenliği, sağlık bilgileri, cinsel hayat, biyometrik veri, genetik veri kategorileri olduğu,
- Tüm kayıtların silinmesi sebebi ile veri sorumlusunda şimdiye kadar çalışmış olan tüm personel ile ayakta ve yatan hasta sayısının bilinmesinin mümkün olmadığı ancak ihlalden etkilenen kişi sayısının tahmini 1000 ve üzeri olduğu,
- İlgili kişilerin veri sorumlusu internet adresi ve çağrı merkezinden bilgi alabileceği

ifade edilmiştir.

Konuya ilişkin inceleme devam etmekle birlikte, Kişisel Verileri Koruma Kurulunun 10.09.2024 tarih ve 2024/1565 sayılı Kararı ile söz konusu veri ihlali bildiriminin Kurumun internet sayfasında ilan edilmesine karar verilmiştir.

Igili karara buradan ulaşabilirsiniz.

MCLEGAL
Metin-Çiçek Avukatlık Ortaklığı
Attorney Partnership

GÜNCEL HABERLER

TİCARİ ELEKTRONİK İLETİ YÖNETİM SİSTEMİ ENTEGRATÖRLERİ HAKKINDA TEBLİĞ

Ticari elektronik ileti onay ve ret bilgilerinin İleti Yönetim Sistemi'ne ("İYS") kaydedilmesine, bu işlemlerin İYS üzerinden entegratörler aracılığıyla veya hizmet sağlayıcılar tarafından gerçekleştirilmesine, entegratörlerin yetkilendirilmesi ve yetkilerinin iptaline dair usul ve esasların düzenlendiği Ticari Elektronik İleti Yönetim Sistemi Entegratörleri Hakkında Tebliğ ("Tebliğ") 18 Eylül 2024 tarih ve 32666 sayılı Resmî Gazete'de yayınlanarak yürürlüğe girmiştir.

Tebliğ uyarınca, ticari elektronik ileti gönderimi yapan veya adına gönderim yapılan İYS'ye kayıt olmakla yükümlü gerçek veya tüzel kişilerin ("Hizmet Sağlayıcı") ticari elektronik ileti gönderimi, alıcılara ait onay ve ret bilgilerinin İYS'ye kaydedilmesi, İYS üzerinden onay alınması ve reddetme hakkının kullanılmasının entegratörler vasıtasıyla yapılabileceği düzenlenmiştir. Ticaret Bakanlığı tarafından entegratör yetkisinin verilebilmesi için aşağıdaki kriterlerin sağlanması gerekmektedir:

- Ödenmiş sermaye olarak en az bir milyon Türk lirası olması
- Paylarının tamamı nama yazılı bir anonim şirket olması
- Şirket bünyesinde teknik uzmanlık alanlarında çalışacak personelin doğrudan veya dışarıdan hizmet alım yoluyla istihdam edilmesi
- ISO 22301 İş Sürekliliği Yönetim Sistemi Belgesi ile Türk Akreditasyon Kurumu tarafından akredite edilmiş bir belgelendirme kuruluşundan alınan ISO/IEC 27001 Bilgi Güvenliği Yönetim Sistemi Belgesi ve ISO/IEC 27701 Kişisel Veri Yönetim Sistemi Belgesine sahip olunması
- Başvuru tarihinden en çok üç ay öncesinde olmak kaydıyla, Türk Standartları Enstitüsü ("TSE") tarafından onaylı A veya B seviye sızma testi yapan kuruluşlarca sızma testinin yapılmış olması
- Teknik alt yapının ticari elektronik ileti onay ve ret işlemlerinde herhangi bir kesinti olmaksızın 7 gün 24 saat iş sürekliliğini sağlayabilecek yedekli bir yapıda, log kayıt mekanizması bulunan, yetkisiz erişime karşı koruma sağlanması ve tutulan kayıtların tutarlı bir zaman kaynağına göre ayarlanarak senkronize şekilde çalışması ve
- Entegratörlük hizmetinde kullanılacak bilgi işlem sisteminin, yazılım, donanım ve sunucu alt yapısının Türkiye Cumhuriyeti sınırları içerisindeki bir veri tabanında bulunması gerekmektedir.

Bu şartların kaybedilmesi halinde entegratöre Kuruluş tarafından, aykırılığın giderilmesi için otuz gün süre verileceği, talep üzerine bir defaya mahsus olmak üzere otuz güne kadar ek süre verilebileceği ve verilen süre içinde aykırılığın giderilememesi veya şartların yeniden sağlanamaması halinde entegratörlük yetkisinin, Kuruluşun bildirimi üzerine Bakanlık tarafından iptal edileceği düzenlenmiştir. Bu durumda Kuruluş tarafından, entegratörün hizmet verdiği hizmet sağlayıcılara İYS üzerinden veya yazılı olarak gecikmeksizin bilgi verilecektir.

Ayrıca, mevcut durumda ticari elektronik ileti onay ve ret işlemlerinde hizmet sağlayıcılara hizmet verenlerden entegratörlük yetkisi almak isteyenlerin Tebliğ'in yayın tarihi ile Kuruluş'a başvuruda bulunabileceği düzenlenmiş olup Tebliğin yürürlüğe girdiği tarihi takip eden altıncı ayın sonuna kadar Bakanlıktan entegratörlük yetkisi almayanların, hizmet sağlayıcı adına ticari elektronik iletilere ilişkin hiçbir işlem tesis edemeyeceği ve İYS üzerinden herhangi bir işlem gerçekleştiremeyeceği belirtilmiştir.

MCLEGAL
Metin-Çiçek Avukatlık Ortaklığı
Attorney Partnership

GÜNCEL HABERLER

"108 MİLYON VATANDAŞA AİT VERİLERİN ÇALINMASINA" İLİŞKİN HABERLER HAKKINDA KAMUOYU DUYURUSU YAYIMLANDI

Bununla birlikte; Kanunun veri güvenliğine ilişkin yükümlülükler başlıklı 12 nci maddesinin (1) numaralı fıkrasında "veri sorumlusunun;

a) Kişisel verilerin hukuka aykırı olarak işlenmesini önlemek,

b) Kişisel verilere hukuka aykırı olarak erişilmesini önlemek,

c) Kişisel verilerin muhafazasını sağlamak

amacıyla uygun güvenlik düzeyini temin etmeye yönelik gerekli her türlü teknik ve idari tedbirleri almak zorunda olduğu, (5) numaralı fıkrasında ise, işlenen kişisel verilerin kanuni olmayan yollarla başkaları tarafından elde edilmesi hâlinde, veri sorumlusunun bu durumu en kısa sürede ilgilisine ve Kişisel Verileri Koruma Kuruluna (Kurul) bildireceği, Kurulun, gerekmesi hâlinde bu durumu, kendi internet sitesinde ya da uygun göreceği başka bir yöntemle ilan edebileceği hükme bağlanmıştır.

Veri sorumlularının, Kişisel Verileri Koruma Kurulunun 24.01.2019 tarih ve 2019/10 Sayılı Kararı gereğince ihlali öğrendiği tarihten itibaren gecikmeksizin ve en geç 72 saat içinde Kurula bildirme yükümlülüğü bulunmaktadır.

Veri ihlal bildirimlerinde, Kurula ve ihlalden etkilenmiş kişilere bildirim yapılmasındaki amaç, ilgili kişiler hakkında ortaya çıkabilecek olumsuz sonuçların bir an önce önüne geçilmesi veya en aza indirilmesine imkan verecek önlemler alınmasını sağlamaktır.

Veri sorumlusunun Kanunun 12 inci maddesinin (5) numaralı fıkrası gereğince bildirim yükümlülüğünü yerine getirmesinden sonra Kurul tarafından inceleme kararı alınabilmektedir.

Diğer taraftan Kurul, şikâyet üzerine veya ihlal iddiasını öğrenmesi durumunda, görev alanına giren konularda Kanunun 15 inci maddesinin (1) numaralı fıkrası hükmü gereğince gerekli incelemeyi resen yapmaktadır.

Muhtelif haber kanallarında ve sosyal medya platformlarında 108 milyon vatandaşımızın verilerinin çalındığına ilişkin haberler yer almakta olup Kurumumuza konuya ilişkin olarak intikal etmiş herhangi bir veri ihlali bildirimi bulunmamaktadır.

Medyada daha önce de benzer haberlerin yer almış olması sebebiyle özellikle pandemi sürecinde meydana geldiği iddia edilen veri ihlali haberleri ile ilgili halihazırda Kişisel Verileri Koruma Kurulu tarafından alınmış resen inceleme kararı bulunmakta olup, ilgili kamu kurumları ile koordineli bir şekilde çalışmalara devam edilmektedir.

İlgili duyuruya buradan ulaşabilirsiniz.

MCLEGAL
Metin-Çiçek Avukatlık Ortaklığı
Attorney Partnership

GLOBAL GELİŞMELER

İRLANDA VERİ KORUMA OTORİTESİ X'E KARŞI AÇILAN DAVALARIN GERİ ÇEKİLDİĞİNİ DUYURDU

İrlanda Veri Koruma Komisyonu (DPC), X'in (eski adıyla Twitter) yapay zeka (YZ-AI) modeli Grok'u eğitmek için Avrupa Birliği (AB) ülkelerinden kullanıcıların kişisel verilerini kullanmama sözü vermesinin üzerine platforma yönelik açılan davanın düşürüldüğünü duyurdu.

DPC, yapay zekânın eğitilmesi sürecindeki veri işleme faaliyetlerine ilişkin olarak sosyal medya platformu X'e karşı dava açmıştı. X'in yapay zekâ modeli olan Grok'un kullanıcı verilerini işlemesine ilişkin açıldığı belirtilen davada, X'in yapay zekâ sistemlerini eğitmek için kullanıcı verilerini işlemesinin durdurulmasına veya bu veri işleme faaliyetinin kısıtlanmasına hükmedilmesi yönünde talepte bulunulmuştu.

DPC, X'e karşı açılan davanın, şirketin 8 Ağustos'ta ajansa yaptığı, kullanıcıların gönderilerini chatbot'unu eğitmek için kullanmayı kalıcı olarak durdurma taahhüdü nedeniyle düşürüldüğünü duyurmuştur.

Ayrıca, bu vaka, DPC'nin AB/AEA genelinde Lead Supervisory Authority (Baş Denetim Yetkisi) olarak böyle bir eyleme başvurduğu ilk durum olarak önem arz etmektedir.

Daha geniş bir perspektifte, DPC, endüstride yapay zeka modellerinde kişisel verilerin kullanımından kaynaklanan sorunları ele almaktadır. DPC, Genel Veri Koruma Tüzüğü'nün (GDPR) 64(2) Maddesi uyarınca Avrupa Veri Koruma Kurulu'na (EDPB) bir görüş talebinde bulunacağı iddia edilmektedir. Bu talep, yapay zeka modeli geliştirme ve eğitme amacıyla yapılan veri işlemede ortaya çıkan bazı temel konuların tartışılmasını ve EDPB düzeyinde bir uzlaşmaya varılmasını sağlamak için yapılacak olup böylece bu karmaşık alana netlik sağlanması amaçlanmaktadır. Görüş, EDPB'yi, bir yapay zeka modelinin eğitimi ve işletilmesinin çeşitli aşamalarında kişisel verilerin işlenmesi boyutunu, hem birinci taraf hem de üçüncü taraf verileri dahil olmak üzere, ve veri sorumlusunun bu işlemeyi hangi yasal dayanağa dayandırdığına ilişkin özel değerlendirmeleri ele almaya davet etmektedir.

GLOBAL GELİŞMELER

VERİ SORUMLULARININ VERİ İŞLEME FAALİYETLERİNE İLİŞKİN İNTERAKTİF ÇALIŞMA BİRLEŞİK KRALLIK VERİ KORUMA OTORİTESİ TARAFINDAN YAYIMLANDI

Birleşik Krallık Veri Koruma Otoritesi (ICO), 2,280 veri sorumlusunun katılımına dayanan bir anket kapsamında, veri sorumlularının veri işleme faaliyetlerine ilişkin interaktif bir çalışma yayımladı.

Çalışma; kuruluşların kişisel veri toplama ve kullanımı konusundaki anlayışı genişletmek, düzenleyici kararları kapsamlı içgörülerle bilgilendirmek ve kalıcı hedefleri yerine getirmek amacıyla hayata geçirilmiştir. ICO tarafından bu çalışma *"Veri Sorumlusu Çalışması, Bilgi Komiserliği Ofisi'nin (ICO) stratejik, düzenleyici ve araştırma faaliyetlerine içgörü sağlamak ve bu faaliyetleri desteklemek amacıyla yürütülen bir çalışmadır."* şeklinde tanımlanmıştır.

Çalışma, kişisel verileri toplayan, işleyen ve depolayan kuruluşlarla hem nicel hem de nitel veri toplamayı içermektedir. Amacı, aşağıdaki hususları anlamaktır:

- Veri sorumlularının demografik özellikleri ve kişisel veri işleme faaliyetleri;
- Veri sorumluları tarafından kullanılan teknoloji;
- Veri sorumlularının yenilikle ilgili değerlendirmeleri; ve
- Veri sorumlularının hem ICO'nun (Bilgi Komiserliği Ofisi) çalışmaları hem de genel olarak veri koruma hakkındaki görüşleri.

Nicel araştırmanın bulguları, bulguları hayata geçiren interaktif bir gösterge panosu ve eşlik eden anlatımla sunulmaktadır. Nitel bulguların özeti ise, veri sorumlularının veri koruma düzenlemeleri konusundaki deneyimlerine dair bir bakış açısı sunmaktadır.

GLOBAL GELİŞMELER

HOLLANDA VERİ KORUMA OTORİTESİ, İNTERNETTEN TOPLANAN MİLYARLARCA YÜZ GÖRÜNTÜSÜNDEN VERİTABANI OLUŞTURDUĞU GEREKÇESİYLE CLEARVIEW AI'A 30,5 MİLYON EURO CEZA KESTİ

Hollanda Veri Koruma Kurumu (DPA) tarafından yapılan açıklamada, dünya genelinde yüz tanıma teknolojisi hizmeti veren Amerikalı Clearview AI'ın milyarlarca yüz fotoğrafından oluşan "yasa dışı bir veritabanı" oluşturması nedeniyle şirkete ceza kesildiği belirtildi. Ayrıca, DPA, Clearview AI'ın hizmetlerini kullanmanın da yasak olduğunu bildirmiştir.

Clearview AI, kişisel veri niteliğindeki fotoğrafları internetten otomatik olarak toplayarak her bir yüz için benzersiz bir biyometrik kod oluşturmaktadır. Bu işlemler, insanların izni olmadan ve bilgileri dahilinde gerçekleşmektedir.

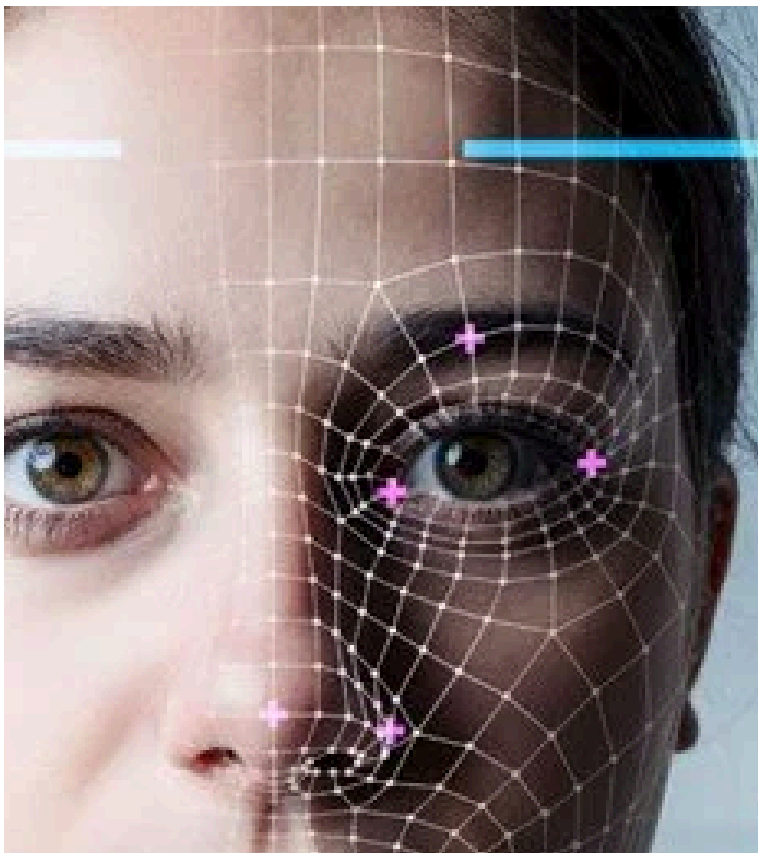
DPA Başkanı Aleid Wolfsen, yüz tanımanın çok müdahaleci bir teknoloji olduğunu ve Clearview AI'ın hizmetlerinin yasadışı olduğunu belirtmiştir. Clearview AI, insanların biyometrik verilerini izinsiz toplamakta ve kullanmakta olduğu için şirketin bu faaliyetleri Genel Veri Koruma Tüzüğü (GDPR) ihlali olarak değerlendirilmektedir.

DPA, Clearview AI'ın ihlalleri durdurmaması durumunda ek cezalar uygulamaya devam edecektir.

Avrupa'nın diğer veri koruma otoritelerinden Clearview AI'a verilen bazı para cezaları:

- Fransa 20 Milyon Euro - Ekim 2022
- Yunanistan 20 Milyon Euro - Temmuz 2022
- Birleşik Krallık 7,5 Milyon Sterlin - Mayıs 2022
- İtalya 20 Milyon Euro - Şubat 2022

Clearview AI verilen çeşitli cezalara rağmen, şirket politikalarını değiştirmemektedir. Bu nedenle, DPA, Clearview AI'ın ihlalleri durdurmasını sağlamak için çeşitli yollar aramaktadır. Bunun yanında, şirketin yöneticilerinin ihlallerden şahsen sorumlu tutulup tutulamayacağı da araştırmaktadır.



GLOBAL GELİŞMELER

İRLANDA VERİ KORUMA OTORİTESİ, FACEBOOK'UN ANA ŞİRKETİ META'YA PAROLA SAKLAMA SÜREÇLERİ NEDENİYLE 91 MİLYON EURO PARA CEZASI VERDİ

İrlanda Veri Koruma Komisyonu (DPC), Meta Platforms Ireland Limited (MPIL)'a karşı MPIL'in sosyal medya kullanıcılarının belirli şifrelerini kendi iç sistemlerinde "düz metin" olarak (şifreleme veya kriptografik koruma olmadan) yanlışlıkla depoladığını DPC'ye bildirmesinin üzerine başlatılan soruşturmanın nihai kararını açıkladı.

DPC'nin kararında aşağıda sıralanan GDPR ihlalleri tespit edilmiştir:

- MPIL'in kullanıcı şifrelerinin düz metin olarak depolanmasıyla ilgili kişisel veri ihlalini DPC'ye bildirmemesi nedeniyle GDPR Madde 33(1) ihlali,
- MPIL'in kullanıcı şifrelerinin düz metin olarak depolanmasına ilişkin kişisel veri ihlallerini belgelendirmemesi nedeniyle GDPR Madde 33(5) ihlali,
- MPIL'in, kullanıcı şifrelerinin yetkisiz işleme karşı güvenliğini sağlamak için uygun teknik veya organizasyonel önlemleri almaması nedeniyle GDPR Madde 5(1)(f) ihlali,
- MPIL'in, risklere uygun bir güvenlik düzeyi sağlamak için uygun teknik ve organizasyonel önlemleri uygulamaması nedeniyle GDPR Madde 32(1) ihlali.

Bu karar, GDPR'ın bütünlük ve gizlilik ilkelerine dayanmaktadır. GDPR, veri işleyenlerin, kişisel verileri işlerken uygun güvenlik önlemleri almalarını düzenlemekte olup her veri işleyen, işleme ile ilgili riskleri değerlendirmekle beraber söz konusu riskleri azaltmak için önlemler almak zorunludur. Bu kararla kullanıcı şifrelerinin depolanması sırasında bu tür önlemlerin alınmasının gerekliliği vurgulanmıştır.

GDPR, veri işleyenlerin kişisel veri ihlallerini düzgün bir şekilde belgelendirmesini ve denetleyici otoritelere zamanında bildirmesini zorunlu kılmıştır. Veri işleyiciler, kişisel veri ihlalini fark ettiğinde, gecikmeden bu ihlali raporlamakla yükümlüdür.

GLOBAL GELİŞMELER

KALIFORNİYA GİZLİLİK KORUMA AJANSI, KARANLIK TASARIMLAR (DARK PATTERNS) KONUSUYLA İLGİLİ BİR UYGULAMA BİLGİLENDİRMESİ YAYINLADI

Kaliforniya Gizlilik Koruma Ajansı (CPPA), "karanlık tasarımlar" (dark patterns) konusuyla ilgili dikkat çekici bir adım atarak bir "Uygulama Bilgilendirmesi" yayınladı. Karanlık tasarımlar, genellikle kullanıcıların gizlilik haklarını koruyan seçeneklere ulaşmasını zorlaştırarak kullanıcıları manipüle eder.

Ajansın bu konuya verdiği önemin bir sonucu olarak, işletmelere kullanıcı arayüzlerinde açıklık ve simetri sağlamaları gerektiği hatırlatılıyor. Yani kullanıcıya sunulan seçeneklerin net, anlaşılır bir dille sunulmuş olması ve teknik ya da hukuki jargonlardan uzak olması beklenmektedir.

Anahtar Noktalar:

- Karanlık tasarımlar, kullanıcıların gizlilik haklarını kullanmasını zorlaştıran tasarım uygulamalarıdır.
- Kaliforniya Tüketici Gizliliği Yasası (CCPA), bu tür uygulamaların yasadışı olduğuna işaret etmekle beraber tüketicilerin verilerini daha iyi koruyabilmek için karanlık tasarımların önlenmesi gerekliliğini vurgulamaktadır.
- CPPA'nın Uygulama Bilgilendirmesi kapsamında şirketler arayüzlerini değerlendirirken seçimlerin açık, simetrik ve gizlilik dostu olduğundan emin olmalıdırlar.

CPPA'nın bu adımı, tüketici gizliliğini korumaya yönelik daha net düzenlemeler getirilmesi ve karanlık tasarım uygulamalarının önlenmesi hususlarında önemli rol oynamaktadır.

MCLEGAL
Metin-Çiçek Avukatlık Ortaklığı
Attorney Partnership