SAYI: 42

MCLEGAL
Metin-Çiçek Avukatlık Ortaklığı
Attorney Partnership

VERİ & TEKNOLOJİ HUKUKU BÜLTENİ

TEMMUZ 2024

GÜNCEL HABERLER

- Temmuz Ayı İçerisinde Bildirilen Kişisel Veri İhlalleri
- Kişisel Verileri Koruma Kurumu Tarafından Kurula İletilen Şikayet ve İhbarlarda Sık Yapılan Hatalar Başlıklı Bir Broşür Yayımlandı
- Kripto Varlık Hizmet Sağlayıcıları Şüpheli İşlem Bildirimi Rehberi ve MASAK Online Sistemi Güncellendi
- Kişisel Verileri Koruma Kurumu Tarafından, Standart Sözleşmeler ve Bağlayıcı Şirket Kurallarına İlişkin Dokümanlar Hakkında Kamuoyu Duyurusu Yayımlandı
- Kişisel Verilerin Yurt Dışına Aktarılmasına İlişkin Usul ve Esasları Belirleyen Yönetmelik Resmi Gazete'de Yayınlanarak Yürürlüğe Girdi

GLOBAL GELİŞMELER

- Avrupa Birliği Yapay Zeka Yasası AB Resmi Gazetesi'nde Yayımlandı
- Avrupa Komisyonu, META'nın "Öde veya Kabul Et" Reklam Modelinin Dijital Pazarlar Yasası'na (DMA) Uygun Olmadığını Belirten Ön Bulgularını META'ya Bildirdi
- Avrupa KomİsyonU, Amazon'a Dijital Hizmetler Yasası (DSA) Kapsamında Bir Bilgi Talebi Gönderdi
- Litvanya Veri Koruma Otoritesi, Vinted İsimli Çevrimiçi İkinci El Kıyafet Alım Satım Platformuna 2.385.276 Euro Para Cezası Kesti

VPN (VIRTUAL PRIVATE NETWORK) NEDİR?

VPN (Virtual Private Network), bir diğer adıyla Sanal Özel Ağ; bir cihazdan bir ağa internet üzerinden şifrelenmiş bir bağlantıdır. Bu şifreli bağlantı, hassas verilerin güvenli şekilde iletilmesini sağlamaya yardımcı olmaktadır. Bu anlamda VPN, ele geçirilme veya izlenme endişesi olmaksızın özel ve güvenli veri aktarımını sağlamaktadır.

Bu anlamda, VPN'in; gizlilik, güvenlik, erişim ve anonimlik gibi birçok avantajı bulunuyor olmakla beraber; VPN kullanımı esnasında dikkat edilmesi gereken birtakım hususlar da bulunmaktadır. Veri güvenliği bağlamında; VPN hizmetinin güvenilirliğinin kontrol edilmesi ve güvenli bir sağlayıcı seçimi bu anlamda büyük önem arz etmektedir. Keza, güvenilir olmayan VPN uygulamaları kullanılırken sağlanan izinler doğrultusunda kişisel verilerin ele geçirilmesi, veri sızıntısı veya güvenlik açıkları yaşanması söz konusu olabilmektedir

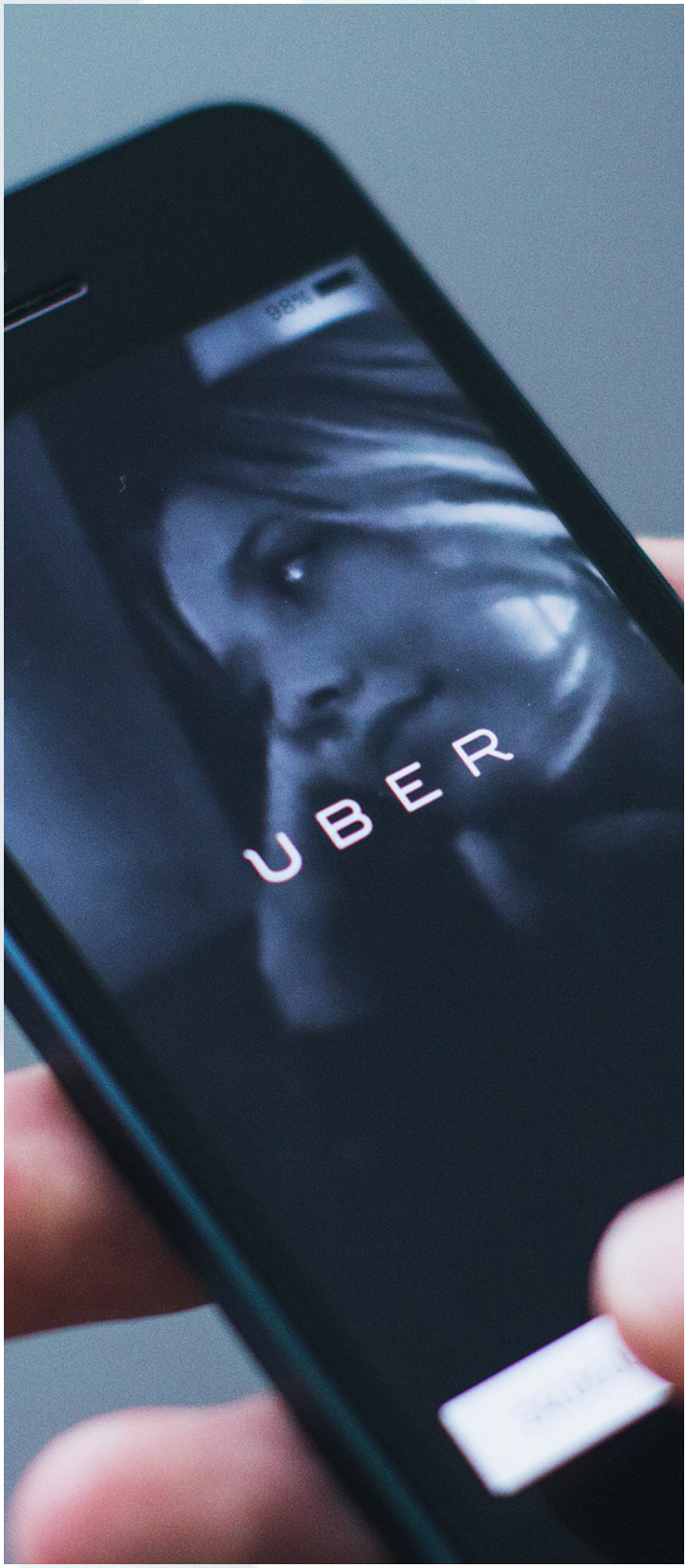
Bu anlamda, devlet tarafından erişimi engellenen sitelere *(örneğin suç teşkil eden terör örgütü, bahis siteleri)* bu uygulamalar vasıtasıyla erişim sağlanması yasal sorunlara yol açabilecektir. Keza, devlet tarafından bu tür sitelere erişim sağlandığı tespit edilebilecek ve ilgili yasaların ihlal edildiği şeklinde değerlendirilebilecektir.

Sonuç olarak; VPN uygulamalarının birçok avantajı bulunmasına karşılık, kullanıcılar açısından dezavantajlı durumlara da sebebiyet verebilmektedir. Bu doğrultuda, kişisel verilerin güvenliği bağlamında uygulamanın güvenilir bir kaynaktan ve platform üzerinden indirilmesi vb. tedbirlerin uygulanması oldukça önem teşkil etmektedir.

GÜNCEL HABERLER

TEMMUZ AYI İÇERİSİNDE BİLDİRİLEN KİŞİSEL VERİ İHLALLERİ

Uber Technologies Inc.



Veri sorumlusu olan Uber Technologies Inc. tarafından Kurul'a yapılan veri ihlal bildiriminde;

- 2 Temmuz 2024 tarihinde veri sorumlusunun, kendisinden kaynaklı olabilecek kişisel verileri kamuya açma tehdidi içeren bir e-posta almış olduğu,
- Veri ihlalinin ne zaman gerçekleştiğinin ve kaynağının henüz belirlenmemiş olduğu ve araştırmaların devam ettiği,
- İhlal kapsamında etkilenen ilgili kişi gruplarının; Uber kullanıcıları *(yolcular ve/veya yemek siparişi veren kişiler)*, sürücüler ve/veya teslimat yapan kişiler olduğu,
- İhlal kapsamında etkilenen kişisel veriler bakımından; Uber kullanıcılarının *(yolcular ve/veya yemek siparişi veren kişiler)* verilerine dair ekran görüntülerinde isim, e-posta adresi, telefon numarası, profil fotoğrafı, kayıt tarihi ve puan bilgilerinin bulunduğunun öngörüldüğü; sürücüler ve/veya teslimat yapan kişiler bakımından ise ihlalden etkilendiği öngörülen verilerin; ekran görüntülerindeki sürücü ehliyeti, sigorta, kimlik kartı, araç kaydı ve özen yükümlülüğü kapsamındaki kontroller gibi belgeler kapsamındaki veriler olduğu,
- İhlal kapsamında etkilenen kişi sayısının mevcut durumda tespit edilemediği

bilgilerine yer verilmiştir. Konuya ilişkin inceleme devam etmekle birlikte, Kişisel Verileri Koruma Kurulu'nun 10/07/2024 tarih ve 2024/1161 sayılı Kararı ile söz konusu veri ihlal bildiriminin Kurumun internet sitesinde ilan edilmesine karar verilmiştir.

İlgili karara buradan ulaşabilirsiniz.

GÜNCEL HABERLER

TEMMUZ AYI İÇERİSİNDE BİLDİRİLEN KİŞİSEL VERİ İHLALLERİ

Creditwest Faktoring A.Ş.

Veri sorumlusu olan Creditwest Faktoring A.Ş. tarafından Kurul'a yapılan veri ihlal bildiriminde;

- İhlalin, veri sorumlusu şirket sunucularına yönelik bir saldırı sonucu gerçekleştiği ve teknik analiz sürecinin devam etmekte olduğu,
- SOC izleme uyarıları sayesinde ihlalin tespit edildiği,
- Etkilenen kişi sayısının mevcut durumda belirlenemediği,
- İhlalin 27/06/2024 tarihinde başladığı ve aynı tarih itibariyle sona erdiği,
- İhlal kapsamında etkilenen kişisel veri kategorilerinin kimlik, iletişim, lokasyon, özlük, müşteri işlem bilgileri olduğu,
- İhlalden; çalışan ve müşteri kişi gruplarının etkilenmiş olduğu,
- Bilgi almak isteyen ilgili kişilerin, www.creditwest.com.tr, veri sorumlusu telefon hatları ve e-posta yoluyla bilgi alabileceği

bilgilerine yer verilmiştir. Konuya ilişkin inceleme devam etmekle birlikte, Kişisel Verileri Koruma Kurulu'nun 10/07/2024 tarih ve 2024/1161 sayılı Kararı ile söz konusu veri ihlal bildiriminin Kurumun internet sitesinde ilan edilmesine karar verilmiştir.

İlgili karara buradan ulaşabilirsiniz.

Güneş Ekspres Havacılık A.Ş.

Veri sorumlusu olan Güneş Ekspres Havacılık A.Ş. tarafından Kurul'a yapılan veri ihlal bildiriminde;

- Bir siber saldırgan tarafından, bir yönetici hesabının bilgileri çalınarak yönetim platformuna yetkisiz erişim sağlandığı, bu hesap üzerinden oltalama amaçlı e-postalar gönderildiği,
- İhlalin 15/07/2024 tarihinde gerçekleşmiş olduğu ve aynı gün içerisinde tespit edildiği,
- Saldırgan tarafından 596.659 tekil e-posta adresine toplamda 1.986.293 e-posta gönderildiği,
- İhlal kapsamında etkilenen kişi gruplarının çalışanlar, müşteriler ve potansiyel müşteriler olduğu, etkilenen veri kategorisinin iletişim (e-posta) bilgisi olduğu,
- Siber saldırganın e-posta gönderdiği 596.659 e-posta adresinin; 86 adedinin çalışanlara (mevcut ve eski çalışanlar), 249.668 adedinin müşterilere ait olduğu,
- 346.905 e-posta adresinin ise kaynağının bilinmediği ve siber saldırgan tarafından saldırı esnasında sisteme yüklenen e-posta adresleri olduğu,
- Bilgi almak isteyen ilgili kişilerin, veri sorumlusunun internet sitesindeki form aracılığıyla detaylı bilgi edinebileceği

bilgilerine yer verilmiştir. Konuya ilişkin inceleme devam etmekle birlikte, Kişisel Verileri Koruma Kurulu'nun 18/07/2024 tarih ve 2024/1230 sayılı Kararı ile söz konusu veri ihlal bildiriminin Kurumun internet sitesinde ilan edilmesine karar verilmiştir.

İlgili karara buradan ulaşabilirsiniz.

MCLEGAL
Metin-Çiçek Avukatlık Ortaklığı
Attorney Partnership

GÜNCEL HABERLER

TEMMUZ AYI İÇERİSİNDE BİLDİRİLEN KİŞİSEL VERİ İHLALLERİ

Adnan Özen İnşaat Taah. Enerji Turizm Tic. ve San. A.Ş.

Veri sorumlusu olan Adnan Özen İnşaat Taah. Enerji Turizm Tic. ve San. A.Ş. tarafından Kurul'a yapılan veri ihlal bildiriminde;

- İhlalin, şirketin araç kiralama rezervasyonlarının alındığı web sitesinin API'sinde yaşanan bir sızıntı nedeniyle gerçekleştiği,
- İhlalin 26/06/2024 tarihinde bir siber saldırganın şirket personeline gönderdiği e-posta ile tespit edildiği,
- İhlal kapsamında etkilenen ilgili kişi gruplarının müşteriler ve potansiyel müşteriler olduğu,
- Etkilenen veri kategorilerinin kimlik (ad, soyad, TCKN), iletişim (adres, telefon numarası, e-posta adresi) ve müşteri işlem bilgilerini (rezervasyon tarihi, kiralama süresi, kiralama bedeli) kapsadığı,
- Toplamda 185 kişinin etkilendiği, veri tabanında yaklaşık 12.000 adet müşteriye ait kişisel verinin bulunduğu ve konuya ilişkin teknik incelemenin sürdüğü

bilgilerine yer verilmiştir. Konuya ilişkin inceleme devam etmekle birlikte, Kişisel Verileri Koruma Kurulu'nun 04/07/2024 tarih ve 2024/1089 sayılı Kararı ile söz konusu veri ihlal bildiriminin Kurumun internet sitesinde ilan edilmesine karar verilmiştir.

İlgili karara buradan ulaşabilirsiniz.

Ann & Robert H. Lurie Children's Hospital of Chicago

Veri sorumlusu olan Ann & Robert H. Lurie Children's Hospital of Chicago tarafından Kurul'a yapılan veri ihlal bildiriminde;

- 26-31 Ocak 2024 tarihlerinde hastane sistemlerine siber saldırı gerçekleştirildiği ve suçluların bu dönemde erişim sağladığı,
- Dünya genelinde yaklaşık 791.784 kişiye ait kişisel verilerin dışarı sızdırıldığının belirlendiği ve bu bilgilerin hastalar ve hasta yakınları, mevcut ve eski Lurie Children's ekip üyeleri ve aile üyeleri ile mevcut ve eski yüklenicilerle ilgili olduğu,
- İhlal kapsamında etkilenen verilerin kişiden kişiye değişiklik göstermekle birlikte, iletişim bilgileri, kimlik bilgileri veya bir hastanın sağlığı ya da tıbbi bakımıyla ilgili bilgiler olabileceği,
- İhlal kapsamında Türkiye'den etkilenen kişi sayısına ilişkin net bir sayı bulunmadığı,
- Bilgi almak isteyen ilgili kişilerin, "https://www.luriechildrens.org" adresini ziyaret ederek ve sayfanın üst kısmındaki "Cybersecurity Matter" linki üzerinden ulaşılabileceği

bilgilerine yer verilmiştir. Konuya ilişkin inceleme devam etmekle birlikte, Kişisel Verileri Koruma Kurulu'nun 10/07/2024 tarih ve 2024/1291 sayılı Kararı ile söz konusu veri ihlal bildiriminin Kurumun internet sitesinde ilan edilmesine karar verilmiştir.

İlgili karara buradan ulaşabilirsiniz.

MCLEGAL
Metin-Çiçek Avukatlık Ortaklığı
Attorney Partnership

GÜNCEL HABERLER

KRİPTO VARLIK HİZMET SAĞLAYICILARI ŞÜPHELİ İŞLEM BİLDİRİMİ REHBERİ VE MASAK ONLİNE SİSTEMİ GÜNCELLENDİ

Hazine ve Maliye Bakanlığı Mali Suçları Araştırma Kurulu tarafından 23 Temmuz 2024 tarihinde yayınlanan duyuru ile, şüpheli işlem bildirim rehberi ve formu hakkında bilgilendirme yapılmıştır.

5549 sayılı Suç Gelirlerinin Aklanmasının Önlenmesi Hakkında Kanuna istinaden, yükümlülerin MASAK Başkanlığına şüpheli işlem bildirimlerini göndermekle yükümlü oldukları hükme bağlanmıştır. MASAK 13 Sıra No.lu Genel Tebliği'nde, MASAK Başkanlığının yükümlüler için genel ve sektörel mahiyette şüpheli işlem bildirim rehberleri yayınlama yetkisi olduğu belirtilmiştir.

Kripto Varlık Hizmet Sağlayıcıları sektörüne özgü Şüpheli İşlem Bildirimlerine ilişkin usul ve esasları düzenleyen Şüpheli İşlem Bildirimi Rehberi ve Formu, sektör temsilcilerinden alınan görüş ve öneriler doğrultusunda ve Kara Paranın Aklanması ve Terörizmin Finansmanıyla Mücadele Ulusal Risk Değerlendirmesi Raporu çerçevesinde güncellenmiştir.

Yeni Şüpheli İşlem Bildirim Rehberiyle özetle:

- Kripto Varlık Hizmet Sağlayıcıların çalışma sistematiği ve kripto varlıkların işlem sistematiğine uygun şüpheli işlem bildirim formu geliştirilmiştir.
- Şüpheli İşlem Bildirim Formu sadeleştirilerek güncel finansal teknolojilerin tümünü kapsayacak şekilde yenilenmiştir.
- Sektöre özgü işlem ve hesap tipleri eklenmiştir.
- Gelişen ve değişen suç tipolojileri dikkate alınarak yeni şüpheli işlem tipleri eklenmiştir.
- Bildirim kategorilerine terör örgütü bilgileri ve Kitle İmha Silahlarının Yayılmasının Finansmanı kategorileri eklenmiştir.
- Şüpheli işleme ilişkin açıklama alanında bildirimlerin kalitesini artırmaya yönelik kontrol noktaları eklenmiştir.
- Referans değer tabloları güncellenmiş ve kodlamalar değiştirilmiştir.
- Kimlik tespit türü ve İşleme Aracılık Eden Finansal Kuruluş bilgileri bölümleri eklenmiştir.
- Yeni şüphe kategorileri eklenerek şüphe kategorisi seçimi zorunlu hale getirilmiştir.

Ayrıca, şüpheli işlem bildirim Rehberi ve Formunun güncellenmesiyle eş zamanlı olarak; elektronik ortamda bildirime imkân sağlayan MASAK Online 1.0 sistemi de güncel teknoloji ile yeniden tasarlanarak Kripto Varlık Hizmet Sağlayıcılarının hizmetine sunulmuştur. MASAK Online 2.0 projesi ile erişim güvenliği artırılmış, esnek ve sektöre özgü yapıların oluşturulmasına imkan sağlanmıştır. Yükümlülerin daha hızlı ve kolay şekilde bildirim yapabilmeleri için XML kılavuzu hazırlanmış ve sektör temsilcileri ile paylaşılmıştır.

Bu kapsamda; 6362 sayılı Sermaye Piyasası Kanununa istinaden yükümlülüklerini yerine getiren ve bu çerçevede faaliyet gösteren Kripto Varlık Hizmet Sağlayıcıları, 26/07/2024 tarihinden itibaren şüpheli işlem bildirimlerini bu rehberde belirtilen usul ve esaslar çerçevesinde göndereceklerdir. Yayınlanan duyuru metnine buradan ulaşabilirsiniz.

GÜNCEL HABERLER

KİŞİSEL VERİLERİ KORUMA KURUMU TARAFINDAN KURULA İLETİLEN ŞİKAYET VE İHBARLARDA SIK YAPILAN HATALAR BAŞLIKLI BİR BROŞÜR YAYIMLANDI

Kişisel Verileri Koruma Kurumu **("Kurum")** tarafından, 17/07/2024 tarihinde "Kurula İletilen Şikâyet ve İhbarlarda Sık Yapılan Hatalar" başlıklı bir broşür **("Broşür")** yayımlandı. Broşürün; şikâyet ve/veya ihbarların, 6698 sayılı Kişisel Verilerin Korunması Kanunu **("Kanun")** ve Veri Sorumlusuna Başvuru Usul ve Esasları Hakkında Tebliğ'e **("Tebliğ")** uygun şekilde Kişisel Verileri Koruma Kurumu'na iletilmesi ve ilgili kişilerin bilgilendirilmesi amacıyla hazırlandığı ifade edilerek şikâyet/ihbarlar bakımından uygulamada sıkça gündeme gelen hatalara yer verilmiştir. Bu anlamda, Broşür kapsamında yer verilen başlıklar şu şekildedir:

- Veri Sorumlusuna Başvuru Yolunun Tüketilmemesi
- Vekil Aracılığıyla Yapılan Şikâyet/İhbarda Vekaletname Puluna Yer Verilmemesi
- Vekil Aracılığıyla Yapılan Şikâyet/İhbar Başvuru Ekinde İlgili Kişiye Ait Vekâletname Örneğinin Eksiksiz Bir Şekilde ve/veya Süresine Dikkat Edilerek Sunulmaması
- Veri Sorumlusuna Yapılmış Başvuruya ve Gerekmesi Halinde Başvuru Yöntemine İlişkin Bilgi ve Belgeye Yer Verilmemesi
- Veri Sorumlusuna Elektronik Posta Aracılığıyla Başvuru Yapılması Halinde, Bu Başvurunun Veri Sorumlusuna Daha Önceden Bildirilen ve Veri Sorumlusunun Sisteminde Kayıtlı Elektronik Posta Adresini Kullanmak Suretiyle Yapılmaması
- Kanunda Öngörülen Yasal Süre İçerisinde Kurula Şikâyetin İletilmemesi
- Veri Sorumlusuna Yapılan Başvurunun Veri Sorumlusuna Tebliğ Edildiğine Dair Belgenin Sunulmaması
- Veri Sorumlusu Tarafından İlgili Kişiye Cevap Verilmiş ise Verilen Cevabın Dilekçe Ekinde Yer Almaması ve/veya Veri Sorumlusu Cevabının İlgili Kişiye Tebliğ Edildiğine Dair Belgenin Sunulmaması
- Şikâyet/İhbar Konusuna İlişkin Tevsik Edici Bilgi ve Belgelerin İletilmemesi
- Kurula İletilen Dilekçelerin, Veri Sorumlusuna Yapılan Başvuruların, Alınan Cevapların ve Bu Belgelere Dair Gönderi Belgelerinin Tarihlerinin Açık ve Anlaşılır Olmaması
- Kurula İletilen Şikâyette/İhbarda, Şikâyet/İhbar Konusu ve Talebin Açık Şekilde Belirtilmemesi ve Kurula İletilen Şikâyet/ İhbar Dilekçesi ve Ekinin Okunaklı Olmaması
- 3071 sayılı Dilekçe Hakkının Kullanılmasına Dair Kanun Gereğince Yazılı Başvurularda Şikâyet Edenin Adına Soyadına, İmzasına, İş veya İkametgâh Adresi Bilgisine Yer Verilmemesi
- İlgili Kişi Adına Temsil Yetkisi Bulunmayan Bir Kişi Tarafından Kurula Şikâyette Bulunulması
- Veri Sorumlusuna Yapılan Başvurunun Yazılı Yapılması Halinde İmzaya Yer Verilmemesi, Vekaletname ile Başvurulmuşsa Vekaletname Örneğine Yer Verilmemesi
- Veri Sorumlusuna Yapılan Başvuruların Ad, Soyad, T.C. Kimlik No., Yabancılar İçin Uyruğu, Pasaport Numarası veya Varsa Kimlik Numarası, Tebligata Esas Yerleşim Yeri veya İş Yeri Adresi, Varsa Bildirime Esas Elektronik Posta Adresi, Telefon ve Faks Numarası ve Talep Konusu İçermemesi
- Veri Sorumlularının KEP Adresine, KEP Niteliğine Haiz Olmayan Elektronik Posta Aracılığıyla Başvuru Yapılması
- Veri Sorumlularının İnternet Sitesinde Yer Alan Kişisel Verilerle İlgili Kısımların Kontrol Edilmeden Başvuruların Gerçekleştirilmiş Olması
- Şikâyetin/İhbarın İlgili Kişi Olarak Addedilmeyecek Tüzel Kişinin Verilerinin Korunmasına Yönelik Bir Talep İçermesi
- Şikâyetin/İhbarın Ölmüş Kişilerin Verilerinin Korunmasına Yönelik Bir Talep İçermesi

Konuya ilişkin detaylı bilgiye buradan, KVKK tarafından yayımlanan broşüre ise buradan ulaşabilirsiniz.

MCLEGAL
Metin-Çiçek Avukatlık Ortaklığı
Attorney Partnership

GÜNCEL HABERLER

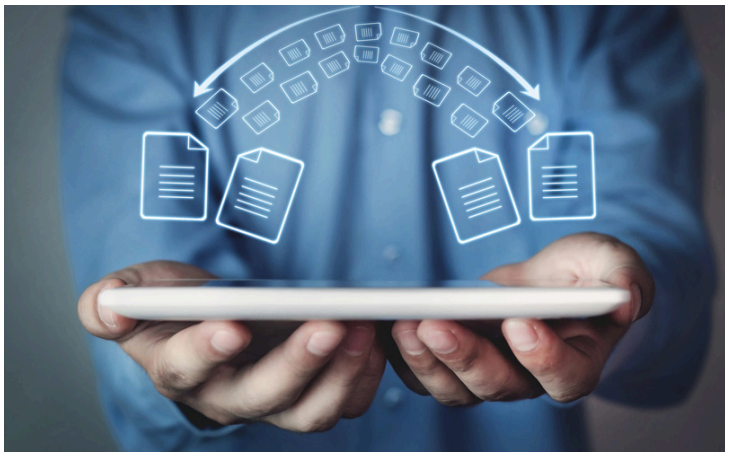
KİŞİSEL VERİLERİN YURT DIŞINA AKTARILMASINA İLİŞKİN USUL VE ESASLARI BELİRLEYEN YÖNETMELİK RESMÎ GAZETE'DE YAYINLANARAK YÜRÜRLÜĞE GİRDİ

12/03/2024 tarih ve 32487 sayılı Resmî Gazete'de yayımlanan 7499 sayılı Ceza Muhakemesi Kanunu ile Bazı Kanunlarda Değişiklik Yapılmasına Dair Kanun kapsamında, Kişisel Verilerin Korunması Kanunu'nun ("Kanun") çeşitli maddelerinde önemli değişiklikler ("Kanun Değişikliği") yapılmıştır. Bu değişikliklerden biri de Kanun'un "kişisel verilerin yurt dışına aktarımı"nı düzenleyen 9. maddesinde gerçekleştirilmiştir.

09/05/2024 tarihinde, Kişisel Verileri Koruma Kurumu ("Kurum") tarafından yayımlanan kamuoyu duyurusu çerçevesinde; söz konusu maddenin mevcut birinci fıkrasının, değiştirilen hali ile 01/09/2024 tarihine kadar uygulanmaya devam edeceği duyurulmuştur.

Kamuoyu duyurusundan sonra merakla beklenen, "Kişisel Verilerin Yurt Dışına Aktarılmasına İlişkin Usul ve Esaslar Hakkında Yönetmelik" 10.07.2024 tarihinde Resmi Gazete'de yayımlanarak yürürlüğe girdi.

Kurumun 9 Mayıs 2024'te taslak olarak paylaşıp 20 Mayıs 2024'e kadar görüşlere açtığı Yönetmelik, çok büyük ölçüde taslak versiyon ile aynı şekilde yayımlandı.
Kanun Değişikliği kapsamında, kişisel verilerin yurt dışına aktarımı bakımından daha detaylı ve sistematik bir yaklaşım benimsenmiş olup Avrupa Birliği Genel Veri Koruma Tüzüğü'ne uyum açısından önemli adımlar atılmıştır. Bu doğrultuda, kişisel verilerin yurt dışına aktarılması bakımından Kanun Değişikliği ile getirilen yeni sistematik şu şekildedir:



- yeterlilik kararına dayalı aktarım,
- uygun güvencelere dayalı aktarım
- arızi durumlara dayalı aktarım.

KVKK'nın mevcut hükümlerinde açıkça ortaya konmamasına karşın uygulamada veri işleyenlerin belirli hukuki sebeplere dayanarak kişisel verileri yurt dışına aktarabildikleri göz önünde bulundurularak Kanun Değişikliği ile veri sorumlularının yanı sıra veri işleyenler de veri aktarımları bakımından önemli aktörler arasında açıkça sayılmış ve veri işleyenler bu doğrultuda KVKK'ya uyumdan sorumlu tutulmuşlardır.

Kanun Değişikliği uyarınca, açık rıza alınması yurt dışına veri aktarımı bakımından tek başına veri işleme şartı olmaktan çıkarılmış ve yalnızca Kurul'un yeterlilik kararının bulunmadığı, taraflarca uygun güvencelerin sağlanamadığı ve arızi aktarımların söz konusu olduğu durumlarda açık rıza alınması hukuki sebebine dayanılabilmesi mümkün kılınmıştır. Ayrıca, yurt dışına veri aktarımına ilişkin potansiyel riskler hakkında ilgili kişilerin bilgilendirilmesine yönelik yükümlülük getirilmiştir.

Kanun Değişikliği kapsamında, kişisel verilerin yurt dışına aktarımı bakımından önem arz eden hususlara buradan ulaşabilirsiniz.

GLOBAL GELİŞMELER

AVRUPA BİRLİĞİ YAPAY ZEKÂ YASASI AB RESMİ GAZETESİNDE YAYIMLANDI

Avrupa Komisyonu tarafından 21 Nisan 2021 tarihinde sunulan ve Yapay Zeka (YZ) sistemlerinin piyasaya arzı, hizmete sunulması ve bazı uygulamaların yasaklanmasına dair kuralları belirleyen "Yapay Zeka Hakkında Uyumlaştırılmış Kurallar Getiren ve Bazı Birlik Yasama Tasarruflarını Değiştiren (AB) 2024/1689 sayılı Tüzük" **("Yapay Zeka Yasası" veya "Yasa")**, 12 Temmuz 2024 tarihinde AB Resmi Gazetesi'nde yayımlanmıştır. Tüzük, 1 Ağustos 2024 tarihinde yürürlüğe girecektir.

AB'nin bu düzenlemesi bir yandan iç pazarın işleyişinin geliştirilmesini, diğer yandan insan odaklı ve güvenilir yapay zeka teknolojilerinin benimsenmesini teşvik etmeyi hedeflemektedir. AB böylece yenilikçiliği desteklerken, yapay zeka sistemlerinin olası zararlı etkilerine karşı sağlığın, güvenliğin, çevrenin yanı sıra demokrasi ve hukukun üstünlüğü dâhil temel hakların korunmasını amaçlamaktadır.

A) YAPAY ZEKA YASASI'NIN KAPSAMI

Yapay Zeka Yasası'nın Kapsamı ve Etkileri

Yapay Zeka Yasası, AB içinde yapay zeka sistemlerini piyasaya süren veya kullanan sağlayıcılar, AB içinde kurulmuş olsun ya da olmasın, yapay zeka sistemlerinin ithalatçıları ve dağıtıcıları için geçerli olacağını öngörmektedir. Ayrıca, yapay zeka sistemlerinin üreticileri için belirli kriterlerin karşılanması gerekmektedir. Yapay Zeka Yasası'nın kapsamı genişletilerek, yapay zeka sistemleri tarafından üretilen bir çıktının AB içinde kullanılması durumunda, AB dışında bulunan yapay zeka sistemi sağlayıcılarının da mevzuata tabi olacağı düzenlenmiştir. Böylece, Yapay Zeka Yasası dünya çapında birçok paydaşı etkileyen küresel bir etkiye sahip olacaktır.

AB Üye Devletleri veya AB ile adli iş birliği için imzalanan uluslararası anlaşmalar çerçevesinde, AB dışındaki kamu kurum ve kuruluşları ile uluslararası örgütler tarafından yapay zeka sistemlerinin kullanılması, temel hak ve özgürlüklerin korunması için yeterli ve uygun güvencelerin sağlanması kaydıyla Yapay Zeka Yasası'nın kapsamı dışında tutulmuştur. Bu düzenleme, Yapay Zeka Yasası'nın uluslararası düzeyde de belirli istisnalar ve güvenceler ile uygulanmasını öngörmektedir.

Veri Koruma

Yapay Zeka Yasa metninde, kişisel verilerin yapay zeka ile bağlantılı olarak işlendiği tüm süreçlerde kişisel verilerin iletişimin korunması, mahremiyet ve gizliliğine ilişkin AB hukukunun uygulanacağı vurgulanmaktadır. Bu kapsamda, AB Genel Veri Koruma Tüzüğü (GDPR) ve diğer ilgili mevzuatlar, yapay zeka sistemlerinin kişisel veri işlemeleri konusunda bağlayıcı olacaktır.

GLOBAL GELİŞMELER

AVRUPA BİRLİĞİ YAPAY ZEKÂ YASASI AB RESMİ GAZETESİNDE YAYIMLANDI

Yapay Zeka Yasası'nın Gereklilikleri Ne Zaman Uygulanmaya Başlayacak?

Yapay Zeka Yasası 1 Ağustos 2024 tarihinde yürürlüğe girecektir. Buna karşılık uygulamaya konulması bakımından öngörülmüştür.

- **2 Şubat 2025:** Yasaklar, Yapay Zeka okuryazarlığı, genel hükümler
- **2 Ağustos 2025:** Genel amaçlı Yapay Zeka, Üye Devler cezalarına ilişkin hükümler
- **2 Ağustos 2026:** Bağımsız yüksek riskli yapay zeka, özel şeffaflık gereklilikleri, düzenleyici kum havuzları vb.
- **2 Ağustos 2027:** Belirli sektörel mevzuat kapsamında yüksek riskli Yapay Zeka, halihazırda piyasada bulunan genel amaçlı Yapay Zeka modelleri

Ayrıca yürürlüğe farklı tarihlerde girecek bu düzenlemelere ilişkin farklı geçiş dönemleri bulunmaktadır:

- **Para cezaları:** Yasaklar 2 Şubat 2025 tarihinde yürürlüğe girerken, cezalar ve para cezalarına ilişkin hükümler prensipte ancak daha sonra uygulanmaya başlayacaktır. Ayrıca, genel amaçlı Yapay Zeka **("GPAI")** modelleri sağlayıcıları için gereklilikler 2 Ağustos 2025'te uygulanabilir hale gelse de, ilgili para cezaları ilke olarak ancak 12 ay sonra uygulanmaya başlayacaktır.
- **Halihazırda piyasada bulunan sistemler veya modeller:** Mevcut yüksek riskli yapay zeka sistemlerinin operatörleri, Yapay Zeka Yasası kapsamında bu tür sistemler için öngörülen şartların yürürlüğe girdiği tarihten itibaren, tasarımlarının önemli değişikliklere konu olması durumunda bu şartları yerine getirmekle yükümlü olacaktır.

Yapay Zeka Yasası Hangi Teknoloji İçin Geçerlidir?

Yapay Zeka Yasası, geleneksel yazılım ve yaklaşımlarından programlama farklı olarak yapay zeka sistemlerini kapsar ve saf otomasyon uygulamalarını hariç tutar. Yasanın kapsamına giren yapay zeka sistemlerinin temel özellikleri şunlardır:

- **Çıkarım Yapma Yeteneği:** Fiziksel veya sanal ortamları etkileyebilecek çıktılar üretme konusunda çıkarım yapabilme yeteneğine sahip olmaları.
- **Makineler Üzerinde Çalışma:** Yapay zeka sistemlerinin makineler üzerinde çalışması.
- **Bağımsız Eylemler:** Eylemlerin insan müdahalesinden bir dereceye kadar bağımsız olması ve insan müdahalesi olmadan çalışabilme kabiliyetine sahip olması.

GLOBAL GELİŞMELER

AVRUPA BİRLİĞİ YAPAY ZEKÂ YASASI AB RESMİ GAZETESİNDE YAYIMLANDI

Yapay Zeka Yasası Kapsamı Dışında Kalan Sistemler Nelerdir?

Bazı yapay zeka sistemleri veya modelleri, Yapay Zeka Yasası'nın kapsamı dışında kalacaktır. Örneğin, münhasıran askeri, savunma veya ulusal güvenlik amaçları için kullanılan ve piyasaya sürülen yapay zeka sistemleri bu kapsam dışındadır. Aynı şekilde, yalnızca bilimsel araştırma ve geliştirme amacıyla özel olarak geliştirilen ve hizmete sunulan yapay zeka sistemleri ve modelleri de Yasa kapsamına girmemektedir. Ayrıca, ücretsiz ve açık kaynak lisansları altında yayınlanan belirli yapay zeka sistemleri veya yüksek riskli bir yapay zeka sisteminde kullanılan veya entegre edilen araçlar, hizmetler, bileşenler veya süreçler ile ilgili özel istisnalar ve kurallar da bulunmaktadır.

Yapay Zeka Yasası Sadece Avrupa Birliği İşletmelerini mi Etkilemekte?

AB'de Mukim Olanlar:

- AB'de yerleşik olan veya bulunan ve AB'de yapay zeka sistemlerini piyasaya süren veya hizmete sunan ya da GPAI modellerini piyasaya süren sağlayıcılar.
- AB'de kurulmuş veya yerleşik dağıtıcılar.
- Yetkili temsilciler, AB'de kurulmuş veya yerleşik ithalatçılar, vb.

AB'de Mukim Olmayanlar:

- Üçüncü ülke sağlayıcılarının AB'de yapay zeka sistemlerini piyasaya sürmesi veya hizmete sokması ya da GPAI modellerini piyasaya sürmesi
- Kuruluş yeri üçüncü bir ülkede bulunan veya yapay zeka sistemi tarafından üretilen çıktının AB'de kullanıldığı yapay zeka sistemlerinin sağlayıcıları ve dağıtıcıları

Yapay Zeka Yasasından Ne Tür Operatörler Etkilenir?

Yapay Zeka Yasası, yapay zeka değer zincirindeki tüm operatörlere yükümlülükler getirmektedir. Sağlayıcılar, alt tedarikçiler, dağıtıcılar, ithalatçılar ve distribütörler dahil olmak üzere tüm operatörler belirli yükümlülüklere tabidir.

Operatörün Yapay Zeka Yasası kapsamındaki rolü, geçerli kurallar ve sorumlulukların belirlenmesi açısından önemlidir. Dağıtıcılar, distribütörler, ithalatçılar ve diğer üçüncü taraflar, belirli koşullar altında yüksek riskli bir yapay zeka sisteminin sağlayıcısı olarak kabul edilir ve yasal sorumluluklar üstlenirler.

MCLEGAL
Metin-Çiçek Avukatlık Ortaklığı
Attorney Partnership

GLOBAL GELİŞMELER

AVRUPA BİRLİĞİ YAPAY ZEKÂ YASASI AB RESMİ GAZETESİNDE YAYIMLANDI

Yapay Zeka Yasası Kapsamında Hangi Uygulamalar Yasaklanmıştır?

Halihazırda sekiz tür yasaklı uygulama bulunmaktadır. Avrupa Komisyonu'nun 2021'deki ilk teklifiyle karşılaştırıldığında, nihai liste, diğer hususların yanı sıra, piyasaya sürme, hizmete alma veya kullanma işlemlerini de kapsayacak şekilde genişletilmiştir:

- Başlangıçta öngörüldüğü gibi yalnızca kamu yetkilileri tarafından veya onlar adına değil, hem kamu hem de özel aktörler tarafından sosyal puanlama için yapay zeka sistemleri.
- İşyeri ve eğitim kurumları alanlarında duyguları tespit etmek için yapay zeka sistemleri.
- Yüz görüntülerinin internetten veya CCTV görüntülerinden hedeflenmemiş bir şekilde toplanması yoluyla yüz tanıma veri tabanları oluşturan veya genişleten yapay zeka sistemleri.
- Yalnızca kişilik özelliklerinin ve karakteristiklerinin profilini çıkarmaya veya değerlendirmeye dayalı olarak gerçek bir kişinin suç işleme riskini değerlendirmek veya tahmin etmekle bağlantılı yapay zeka sistemleri.
- Gerçek kişileri biyometrik verilerine dayanarak ırk, siyasi görüş, sendika üyeliği, dini veya felsefi inanç, cinsel yaşam veya cinsel yönelim gibi çıkarımlarda bulunmak amacıyla kategorize eden biyometrik sınıflandırma sistemleri.

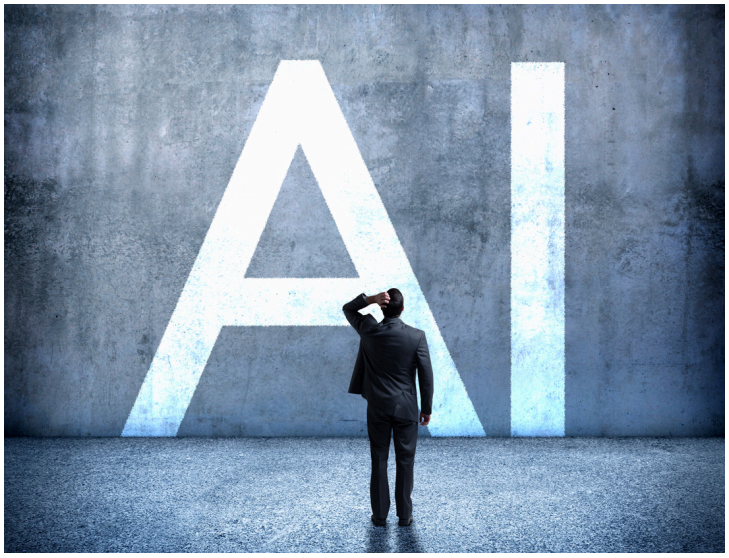
Risk Temelli Yaklaşımlar ve Düzenlemeler

Yapay Zeka Yasası'nın yapay zekadan kaynaklanan risk düzeyine bağlı olarak yapay zeka modellerinin geliştirilmesi, kullanımı, ithalatı, dağıtımı veya üretiminde yer alan tüm tarafların sorumlu olacağı bir dizi kural ortaya koyduğu görülmektedir.

Parlamento'nun kabul ettiği yasa metni, yapay zeka sistemlerini dört ana risk kategorisinde değerlendirmektedir: kabul edilemez risk, yüksek risk, sınırlı risk, minimum risk

Bu kapsamda kanunda; Kabul edilemez risk kategorisinde yer alan uygulamalar tamamen yasaklanmıştır. Örneğin, sosyal kredi puanlama sistemleri gibi vatandaşların temel haklarını ihlal edebilecek sistemler veya bilinçaltı teknikler ve biyometrik tanımlama kullanan uygulamalar bu kategoriye girmektedir.

Yüksek risk kategorisindeki sistemler, sağlık, güvenlik ve kritik altyapılar gibi alanlarda kullanıldığından sıkı düzenlemelere tabidir ve bu sistemler için güvenlik, şeffaflık ve insan denetimi zorunludur.



GLOBAL GELİŞMELER

AVRUPA BİRLİĞİ YAPAY ZEKÂ YASASI AB RESMİ GAZETESİNDE YAYIMLANDI

Yüksek Riskli Yapay Zeka Sistemleri Nelerdir?

Birincisi, belirli sektörel mevzuat kapsamına giren ve piyasaya sürülmek veya hizmete sunulmak amacıyla bu Yasa uyarınca üçüncü taraf uygunluk değerlendirmesine tabi olan ürünler veya ürünlerin güvenlik bileşenleri olan yapay zeka sistemlerini ifade eder.

İkinci kategori, mevcut sekiz alandan birine giren 'bağımsız' yüksek riskli yapay zeka sistemlerinin bir listesini ifade etmektedir:

- İK amaçları
- Kredi değerliliğinin değerlendirilmesi veya kredi puanı oluşturulması
- Gerçek kişilerle ilgili risk değerlendirmesi ve fiyatlandırma hayat ve sağlık sigortası.
- Uzaktan biyometrik tanımlama, hassas veya korunan özelliklere göre biyometrik kategorizasyon
- Eğitim ve mesleki eğitim
- Kritik tesislerin yönetimi ve işletilmesinde güvenlik bileşenleri ve dijital altyapı.

Yüksek Riskli Yapay Zeka Sistemleri İçin Öngörülen Yükümlülükler Nelerdir?

Yüksek riskli yapay zeka sistemleri için belirli yükümlülükler geçerlidir ve bunlar operatörün rolüne göre farklılık gösterir.

Örneğin, yüksek riskli yapay zeka sistemlerinin sağlayıcıları, risk ve kalite yönetimi, önyargıyı önlemek de dahil olmak üzere veri yönetişimi, dokümantasyon ve kayıt tutma, şeffaflık, kayıt, insan gözetimi, doğruluk, sağlamlık ve siber güvenlik ve uygunluk değerlendirmeleri açısından geniş bir dizi şarta tabidir. Bunlar şu şekilde özetlenebilir:

- Veri yönetişimi önlemlerinin uygulanması ve veri kümelerinin kalitesinin sağlanması
- Risk ve kalite yönetim sistemlerinin uygulanması
- Uygun insan gözetiminin sağlanması
- Kullanım talimatlarına uyma
- İnsan gözetiminin uygun şekilde atanması
- Yapay zeka sisteminin izlenmesi
- Etkilenen kişilere bilgi sağlanması
- Girdi verilerinin uygunluğunun sağlanması

GPAI Modelleri İçin Hangi Kurallar Geçerlidir?

Yapay Zeka Yasası GPAI modellerinin düzenlenmesi için özel bir çerçeve sunmaktadır. Tüm GPAI modellerinin sağlayıcıları için bir dizi şartlar ve sistemik risk taşıyan sağlayıcılar için ek şartlar içermektedir. Bu, Avrupa Komisyonu'nun 2021'deki ilk teklifine kıyasla en önemli gelişmelerin görüldüğü alanlardan biridir.

MCLEGAL
Metin-Çiçek Avukatlık Ortaklığı
Attorney Partnership

GLOBAL GELİŞMELER

AVRUPA BİRLİĞİ YAPAY ZEKÂ YASASI AB RESMİ GAZETESİNDE YAYIMLANDI

Sistemik Risk İçeren GPAI Modelleri İçin Ek Kurallar

- Sistemik riskleri tanımlamak ve azaltmak için modelin rakip testleri de dahil olmak üzere en son teknolojiyi yansıtan standartlaştırılmış protokoller ve araçlar uyarınca model değerlendirmesi yapmak
- Kaynakları da dahil olmak üzere AB düzeyinde olası sistemik riskleri değerlendirmek ve azaltmak
- Ciddi olayları ve ilgili düzeltici önlemleri izlemek ve ilgili makamlara raporlamak
- Model ve fiziksel altyapısı için yeterli siber güvenlik korumasının sağlanması

Tüm GPAI Modelleri İçin Kurallar

GPAI modellerinin sağlayıcılarının belirli gerekliliklere uyması gerekecektir.

- Teknik dokümantasyon
- GPAI modelini yapay zeka sistemlerine entegre etmeyi amaçlayan yapay zeka sistemleri sağlayıcılarına sunulacak bilgiler ve modelin yeteneklerini anlamalarını sağlamak
- Telif hakkı ve ilgili haklara ilişkin AB hukukuna saygı gösterme politikası
- Yapay Zeka Ofisi tarafından sağlanacak bir şablona dayalı olarak modelin eğitimi için kullanılan içeriğe ilişkin ayrıntılı bir özet
- ilgili makamlarla işbirliği. Ayrıca, sağlayıcının AB dışında yerleşik olduğu durumlarda, özellikle GPAI modelleriyle ilgili olarak yetkili temsilcilerin atanmasına ilişkin özel hükümler bulunmaktadır

Özel Şeffaflık Gereksinimleri

Genel amaçlı AI (GPAI) sistemleri ve bunların dayandığı GPAI modelleri, AB telif hakkı yasasına uyum ve eğitim için kullanılan içeriğin ayrıntılı özetlerinin yayınlanması gibi belirli şeffaflık gerekliliklerini karşılamalıdır.

Sistemsel riskler oluşturabilecek daha güçlü GPAI modelleri, model değerlendirmeleri yapma, sistemsel riskleri değerlendirme ve azaltma ve olaylar hakkında raporlama gibi ek şartlarla karşı karşıya kalacaktır.

Ayrıca, yapay veya değiştirilmiş görüntü, ses veya video içeriklerinin ("deepfake") açıkça etiketlenmesi gerekecektir.

Şeffaflık gereksinimlerine ilişkin hükümler, özellikle ilgili içeriğin yapay olarak üretilmiş veya manipüle edilmiş olarak tanımlanmasını veya tespit edilebilmesini sağlamak için üretken yapay zeka dahil olmak üzere yeni gereklilikler getirecek şekilde genişletilmiştir.

MCLEGAL
Metin-Çiçek Avukatlık Ortaklığı
Attorney Partnership

GLOBAL GELİŞMELER

AVRUPA BİRLİĞİ YAPAY ZEKÂ YASASI AB RESMİ GAZETESİNDE YAYIMLANDI

GPAI sistemleri de dahil olmak üzere, sentetik ses, görüntü, video veya metin içeriği üreten yapay zeka sistemlerinin sağlayıcıları, yapay zeka sisteminin çıktılarının makine tarafından okunabilir bir formatta işaretlenmesini ve yapay olarak üretildiğinin veya manipüle edildiğinin tespitini mümkün kılacaktır.

Benzer şekilde, Kamu yararını ilgilendiren konularda kamuoyunu bilgilendirmek amacıyla yayınlanan bir metni üreten veya manipüle eden bir yapay zeka sisteminin dağıtıcıları ile kamu yararını ilgilendiren bir içeriği oluşturan, üreten veya manipüle eden bir yapay zeka sisteminin dağıtıcıları sahte metnin/içeriğin yapay olarak oluşturulduğunu veya manipüle edildiğini (deepfake) açıklamak zorunda kalacaktır

Yapay Zeka Yasası Nasıl Uygulanacak? Hangi Para Cezaları Uygulanacak?

Ulusal düzeyde ve ayrıca AB düzeyinde güçlü bir uygulama ve denetim çerçevesi oluşturulmuştur. Kilit organlar ve yetkililer arasında ulusal yetkili makamlar, Avrupa Komisyonu bünyesinde kurulan Yapay Zeka Ofisi, Yapay Zeka Kurulu, bağımsız uzmanlardan oluşan bilimsel panel ve danışma forumu yer almaktadır.

Yapay Zeka Yasası'nın ihlallerine yönelik cezalar ve diğer yaptırım türlerine ilişkin kuralları, Yapay Zeka Yasası'nda öngörülenlere ve Avrupa Komisyonu tarafından çıkarılabilecek kılavuz ilkelere uygun olarak belirlemek AB Üye Devletlerinin görevidir.

Öte yandan ve daha da önemlisi, GPAI modellerine ilişkin hükümleri denetlemek ve uygulamak, bu tür modellerin sağlayıcılarına para cezası uygulamak da dahil, münhasıran Avrupa Komisyonu'nun yetkisinde olacaktır. Yasa uyarınca, kademeli para cezaları şu şekilde olacaktır:

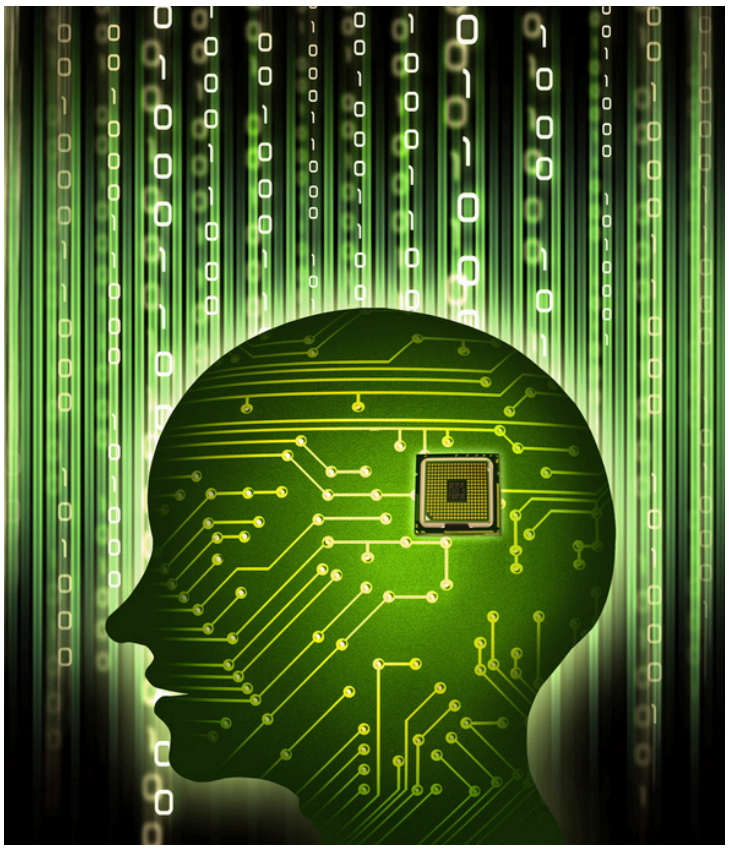
- **Yasaklanmış Uygulamalar:** 35.000.000 Avro ve %7'sinden yüksek olanına kadar teşebbüsün küresel yıllık cirosu.

- **Yüksek Riskli Yapay Zeka ve Özel şeffaflık Gereksinimleri:** 15.000.000 Avro ve %3'ünden yüksek olanına kadar teşebbüsün küresel yıllık cirosu.

- **GPAI Modelleri:** 15.000.000 Avro ve %3'ünden yüksek olanına kadar sağlayıcının küresel yıllık cirosu

.

- **Yanlış, Eksik veya Yanıltıcı Bilgiler:** 7.500.000 Avro ve %1'inden yüksek olanına kadar teşebbüsün küresel yıllık cirosu.



GLOBAL GELİŞMELER

AVRUPA KOMİSYONU, META'NIN "ÖDE VEYA KABUL ET" REKLAM MODELİNİN DİJİTAL PAZARLAR YASASI'NA (DMA) UYGUN OLMADIĞINI BELİRTEN ÖN BULGULARINI META'YA BİLDİRDİ

Avrupa Komisyonu, META'nın "öde veya kabul et" reklam modelinin Dijital Pazarlar Yasası'na (DMA) uygun olmadığını belirten ön bulgularını META'ya bildirdi. Komisyona göre, bu ikili seçenek, kullanıcıları kişisel verilerini birleştirmeyi kabul etmeye zorlamakta ve kişiselleştirilmemiş ama eşdeğer bir META sosyal ağı versiyonu sunmamaktadır.

AB'deki mevzuat değişikliklerine cevaben META, Kasım 2023'te Facebook ve Instagram'ın AB kullanıcılarının **(i)** bu sosyal ağların reklamsız bir versiyonuna aylık bir ücret karşılığında abone olmayı veya **(ii)** bu sosyal ağların kişiselleştirilmiş reklamlara sahip ücretsiz bir versiyonu seçmeyi içeren ikili bir "öde veya onay ver" teklifini uygulamaya koymuştur.

Komisyon, META'nın bu modelinin, DMA'nın 5(2) maddesinde belirtilen gereksinimleri karşılamadığı için DMA ile uyumlu olmadığı ön görüşünü benimsemektedir. Özellikle META'nın modeli;

- Kullanıcıların kişisel verilerini daha az kullanan ancak "kişiselleştirilmiş reklamlar" tabanlı hizmetle eşdeğer olan bir hizmeti tercih etmelerine izin vermemektedir.
- Kullanıcıların kişisel verilerinin birleştirilmesine özgürce rıza gösterme haklarını kullanmalarına izin vermemektedir.
- DMA ile uyumluluğun sağlanması için, rıza göstermeyen kullanıcıların, bu durumda reklamların kişiselleştirilmesi için kişisel verilerini daha az kullanan eşdeğer bir hizmete erişebilmeleri gerekmektedir.

GLOBAL GELİŞMELER

AVRUPA KOMİSYONU, AMAZON'A DİJİTAL HİZMETLER YASASI (DSA) KAPSAMINDA BİR BİLGİ TALEBİ GÖNDERDİ

Avrupa Komisyonu, Amazon'dan, DSA (Dijital Hizmetler Yasası) yükümlülüklerine uygunluğunu açıklayan daha ayrıntılı bilgi talep etmektedir.

Özellikle, Amazon'un öneri sistemlerinin şeffaflığı, bu sistemlerin girdi faktörleri, özellikler, sinyaller, bilgi ve meta veriler ile kullanıcıların profil oluşturmadan çıkma seçenekleri hakkında bilgi sağlaması istenmektedir.

Ayrıca, Amazon'un; Amazon Store'un Reklam Kütüphanesi'nin çevrimiçi arayüzünün tasarımı, geliştirilmesi, uygulanması, test edilmesi ve bakımı ile ilgili bilgileri ve risk değerlendirme raporuyla ilgili destekleyici belgeleri de sunması gerekmektedir.

Amazon'un bu bilgileri 26 Temmuz 2024'e kadar sağlaması beklenmektedir. Komisyon, yanıtları değerlendirdikten sonra, yasal işlemler başlatabilecek ve yanlış, eksik ya da yanıltıcı bilgi sunulması durumunda para cezası uygulayabilecektir. Ayrıca, yanıt verilmezse, düzenli cezalar uygulanabilecektir.

LİTVANYA VERİ KORUMA OTORİTESİ, VİNTED İSİMLİ ÇEVRİMİÇİ İKİNCİ EL KIYAFET ALIM SATIM PLATFORMUNA 2.385.276 EURO PARA CEZASI KESTİ

2 Temmuz 2024'te Litvanya Veri Koruma Otoritesi, Vinted adlı çevrimiçi ikinci el kıyafet alım satım platformuna 2.385.276 Euro para cezası uygulanmasına karar verdi. Ceza, Fransız ve Polonyalı denetim makamlarının şikayetleri üzerine, Genel Veri Koruma Tüzüğü'nün (GDPR) yasallık, adillik ve şeffaflık ilkelerine, hesap verebilirlik ilkesine ve veri sahiplerinin haklarıyla ilgili şeffaf bilgi sağlama yükümlülüklerine aykırı hareket ettiği tespit edilen Vinted'e verildi. Şikayetlerde, Vinted'in "unutulma hakkı" ve "erişim hakkı" taleplerine uygun şekilde yanıt vermediği, kişisel verileri "gölge engelleme" yöntemiyle işlediği ve hesap verebilirlik ilkesini yerine getirecek teknik ve organizasyonel önlemleri almadığı belirtildi. Cezanın belirlenmesinde, işlem kapsamı, etkilenen veri sahiplerinin sayısı ve ihlalin süresi gibi faktörler dikkate alındı.

MCLEGAL
Metin-Çiçek Avukatlık Ortaklığı
Attorney Partnership

P: +90 212 264 50 00
info@mclegal.com.tr | mclegal.com.tr
Nisbetiye Mah. Nisbetiye Cad. No:32/9
Beşiktaş / İSTANBUL