SAYI: 50

MCLEGAL
Metin-Çiçek Avukatlık Ortaklığı
Attorney Partnership

VERİ & TEKNOLOJİ HUKUKU BÜLTENİ

MART 2025

GÜNCEL HABERLER

- KVKK'dan VF Ege Giyim'in Yurt Dışı Veri Aktarımına Onay Verildi
- Mart Ayı İçerisinde Bildirilen Kişisel Veri İhlalleri
- KVKK'dan Güncellenen Rehber: Biyometrik Verilerin İşlenmesine İlişkin Dikkat Edilmesi Gerekenler

GLOBAL GELİŞMELER

- Fransız Rekabet Otoritesinden Apple'a 150 MİlyonEuro'luk Ceza
- Microsoft Advertising, Kullanıcı Onayı Uygulamasını 5 Mayıs 2025'te Zorunlu Hale Getiriyor.
- Avrupa Komisyonu Uzman Grubu, B2B Veri Paylaşımı İçin Rehber Yayınladı
- ICO, Kişisel Verilerin Anonimleştirilmesi Konusunda Yeni Rehber Yayınladı

AB YAPAY ZEKA YASASI YÜRÜRLÜĞE GİRİYOR

Mart 2025'te Avrupa Parlamentosu tarafından onaylanan Yapay Zeka Yasası (AI Act), Avrupa Birliği'nin ilk kapsamlı yapay zekâ düzenlemesi olma niteliğini taşıyor. Yeni yasa, yapay zeka sistemlerini risk temelli bir yaklaşımla dört kategoriye ayırıyor: yasaklı, yüksek riskli, sınırlı riskli ve minimal riskli sistemler. Özellikle yüz tanıma ile kitlesel izleme, sosyal puanlama gibi bireysel hakları ihlal eden uygulamalar tamamen yasaklanırken; sağlık, eğitim, işe alım, finans gibi alanlardaki yüksek riskli sistemler için sert denetim ve şeffaflık yükümlülükleri getiriliyor.

AI Act, tıpkı GDPR gibi sadece AB sınırlarında değil, küresel düzeyde etki yaratacak şekilde tasarlandı. AB vatandaşlarının verisini işleyen, AB pazarına ürün veya hizmet sunan tüm şirketler bu düzenlemelere uyum sağlamakla yükümlü olacak. Bu durum, Türkiye'de faaliyet gösteren teknoloji geliştiricileri, finans kuruluşları ve yapay zeka tabanlı hizmet sunan şirketler açısından da ciddi uyum süreçlerini beraberinde getiriyor. Yasa; insan denetimi, risk analizi ve şeffaflık gibi ilkeleri ön plana çıkarıyor.

Kurumların, yapay zeka sistemlerini gözden geçirmesi ve risk temelli sınıflandırmalar yaparak gerekli teknik ve hukuki önlemleri alması gerekiyor. Yapay zekanın gelişim hızına rağmen etik ve güvenlik eksenli düzenlemeler artık kaçınılmaz hale geliyor. Avrupa'nın bu düzenlemesi, sadece bir mevzuat değil; küresel yapay zeka ekosistemine yön verecek bir çerçeve olarak değerlendiriliyor.

GÜNCEL HABERLER

KVKK'DAN VF EGE GİYİM'İN YURT DIŞI VERİ AKTARIMINA ONAY VERİLDİ

Kişisel Verileri Koruma Kurulu, şirketin üç ayrı taahhütname başvurusunu uygun bularak 12 Mart 2025 tarihinde veri aktarımına izin verdi.

VF Ege Giyim Sanayi ve Ticaret Limited Şirketi tarafından yurtdışına kişisel veri aktarımı yapılması amacıyla Kişisel Verileri Koruma Kurumu'na (KVKK) sunulan üç ayrı taahhütname başvurusu, Kurul tarafından incelendi. 6698 sayılı Kişisel Verilerin Korunması Kanunu'nun 9. maddesi kapsamında yapılan değerlendirmede, başvuruların usul ve esas yönünden eksiksiz olduğu tespit edilerek, 12 Mart 2025 tarihinde söz konusu veri aktarımlarına izin verildi.

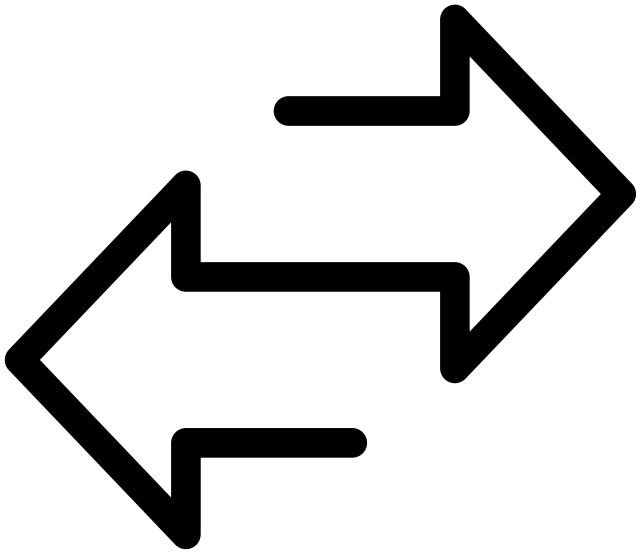
Taahhütname Nedir?

2024 yılında yapılan kanun değişikliğiyle birlikte, kişisel verilerin yurtdışına aktarımı için açık rıza artık tek başına yeterli bir aktarım şartı olmaktan çıkarıldı. Yeni sistemde, aktarımın gerçekleştirilebilmesi için öncelikle verilerin gönderileceği ülkenin Kurum tarafından "yeterli korumaya sahip ülke" olarak ilan edilmesi ya da veri sorumlularının Kurul'a taahhütname sunarak izin alması gerekiyor.

Taahhütname yöntemiyle veri aktarımında, veri sorumlusu ile yurtdışındaki alıcı arasında veri güvenliğine ilişkin teknik ve idari önlemleri içeren taahhütler hazırlanıyor ve Kurul'un onayına sunuluyor. Kurul tarafından onaylanan taahhütname, ilgili şirketin belirlenen kapsamda yurtdışına kişisel veri aktarımı yapabilmesine hukuki zemin sağlıyor.

Bu kapsamda Kurul'un VF Ege Giyim'in başvurularına onay vermesi, şirketin belirli yurt dışı iş ortaklarına hukuka uygun şekilde kişisel veri aktarabileceği anlamına geliyor. Gelişme, yurt dışı ile çalışan tüm veri sorumluları için önemli bir örnek teşkil ediyor.

İlgili kamuoyu duyurusuna buradan ulaşabilirsiniz.



GÜNCEL HABERLER

MART AYI İÇERİSİNDE BİLDİRİLEN KİŞİSEL VERİ İHLALLERİ

Turknet İletişim Hizmetleri A.Ş.

Veri sorumlusu sıfatını haiz Turknet İletişim Hizmetleri A.Ş. tarafından Kurula iletilen veri ihlal bildiriminde özetle;

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

bilgilerine yer verilmiştir.

Konuya ilişkin inceleme devam etmekle birlikte, Kişisel Verileri Koruma Kurulunun 20.03.2025 tarih ve 2025/578 sayılı Kararı ile söz konusu veri ihlal bildiriminin Kurumun internet sayfasında ilan edilmesine karar verilmiştir.

İlgili karara buradan ulaşabilirsiniz.

Nevşehir Hacı Bektaş Veli Üniversitesi

Veri sorumlusu sıfatını haiz Nevşehir Hacı Bektaş Veli Üniversitesi tarafından Kurula iletilen veri ihlal bildiriminde özetle;

- Veri sorumlusunun; İzmir Kâtip Çelebi Üniversitesi (İKÇÜ) tarafından geliştirilen Üniversite Bilgi Yönetim Sistemini (ÜBYS) kullandığı ve PingPong Üniversite Rehberi adlı mobil uygulamanın, İKÇÜ tarafından sağlanan web servisleri aracılığıyla veri sorumlusunun personel ve öğrencilerinin kişisel verilerine eriştiğinin tespit edildiği,
- Tesadüfen bir öğrencinin kişisel verilerine başka bir mobil uygulamadan erişebildiğini ifade etmesi üzerine durumun farkına vardıklarını, mobil uygulamaya sahip firmanın verileri İKÇÜ üzerinden elde ettiğinin tespit edildiği,
- İKÇÜ ile durum hakkında bilgi vermesi için yazışmalar gerçekleştirdiklerini, verilerin İKÇÜ'nün veri sorumlusundan izinsiz paylaştığını tespit edildiği, paylaşım yapılan firmanın kullanıcı sözleşmesi incelendiğinde ise verilerin saklandığı ve işlendiğinin değerlendirildiği,
- İhlalden etkilenen ilgili kişi gruplarının çalışanlar ve öğrenciler olduğu,
- İhlalden etkilenen kişi sayısının tam olarak bilinmediği ancak web serviste kayıtlı 22.960 aktif öğrenci ve personelin bulunduğu

bilgilerine yer verilmiştir.

Konuya ilişkin inceleme devam etmekle birlikte, Kişisel Verileri Koruma Kurulunun 28.03.2025 tarih ve 2025/634 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

MART AYI İÇERİSİNDE BİLDİRİLEN KİŞİSEL VERİ İHLALLERİ

Bilfen Eğitim Kurumları A.Ş.

Veri sorumlusu sıfatını haiz Bilfen Eğitim Kurumları A.Ş. tarafından Kurula iletilen veri ihlal bildiriminde özetle;

- İhlalin; veri sorumlusunun kullandığı sistemde URL üzerinden sehven erişime açık bırakılan XML dosyalarının saldırganlar tarafından ele geçirilmesiyle gerçekleştiği,
- İhlalin 12.03.2025 tarihinde başladığı ve aynı tarihte veri sorumlusunun Whatsapp hattına siber saldırgan/saldırganlar tarafından gönderilen bir mesaj ile tespit edildiği,
- İhlalden etkilenen veri kategorilerinin; kimlik, iletişim, işlem güvenliği, mesleki deneyim, görsel ve işitsel kayıtlar ile birlikte özel nitelikli kişisel verilerden sağlık bilgileri olduğu,
- İhlalden etkilenen kişi sayısının 24.061 kişi olduğu,
- İhlalden etkilenen ilgili kişilerin; öğrenciler, öğrenci velileri ve çalışanlar olduğu,
- İlgili kişilerin, veri sorumlusuna ait https://bilfen.com/tr internet sitesi vasıtasıyla veri ihlaline ilişkin duyurulara ulaşabilecek ve ayrıca detaylı bilgi için kvkk@bilfen.com e-posta hesabı vasıtasıyla veri ihlali hakkında bilgi alabilecekleri

bilgilerine yer verilmiştir.

Konuya ilişkin inceleme devam etmekle birlikte, Kişisel Verileri Koruma Kurulunun 20.03.2025 tarih ve 2025/573 sayılı Kararı ile söz konusu veri ihlal bildiriminin Kurumun internet sitesinde ilan edilmesine karar verilmiştir.

İlgili karara buradan ulaşabilirsiniz.

Anadolu Anonim Türk Sigorta Şirketi

Veri sorumlusu sıfatını haiz Anadolu Anonim Türk Sigorta Şirketi tarafından Kurula iletilen veri ihlali bildiriminde özetle;

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

bilgilerine yer verilmiştir.

Konuya ilişkin inceleme devam etmekle birlikte, Kişisel Verileri Koruma Kurulunun 06.03.2025 tarih ve 2025/467 sayılı Kararı ile söz konusu veri ihlali bildiriminin Kurumun internet sitesinde ilan edilmesine karar verilmiştir.

İlgili karara buradan ulaşabilirsiniz.

MCLEGAL
Metin-Çiçek Avukatlık Ortaklığı
Attorney Partnership

GÜNCEL HABERLER

KVKK'DAN GÜNCELLENEN REHBER: BİYOMETRİK VERİLERİN İŞLENMESİNE İLİŞKİN DİKKAT EDİLMESİ GEREKENLER

Kişisel Verileri Koruma Kurumu (“Kurum”) tarafından “Biyometrik Verilerin İşlenmesinde Dikkat Edilmesi Gereken Hususlara İlişkin Rehber”, biyometrik verilerin işlenmesinde uyulması gereken temel ilke ve yükümlülükleri ortaya koymaktadır.

Biyometrik Veriler Nedir?

Rehber kapsamında biyometrik veriler; bireylere özgü fiziksel, fizyolojik veya davranışsal özelliklerin teknik yöntemlerle işlenmesi sonucunda elde edilen, kişinin kimliğini belirlemeye yarayan veriler olarak tanımlanmıştır. Parmak izi, yüz tanıma, retina/iris taraması, avuç içi damar haritası, ses ve davranış analizleri (örneğin imza) biyometrik veri örnekleri arasında sayılmaktadır.

Özel Nitelikli Kişisel Veri

Biyometrik veriler, 6698 sayılı Kişisel Verilerin Korunması Kanunu (“Kanun”) kapsamında özel nitelikli kişisel veri olarak değerlendirilmektedir. Bu doğrultuda, söz konusu verilerin işlenmesi sıkı şartlara bağlanmıştır.

Açık Rıza ve Alternatif Sunma Yükümlülüğü

Rehber, biyometrik verilerin işlenmesinde açık rıza alınmasının kural olduğunu ve bu rızanın özgür iradeyle, ilgili kişiyi bilgilendirerek alınması gerektiğini vurgulamaktadır. Ayrıca, veri sorumlularının mümkün olduğu ölçüde alternatif bir doğrulama yöntemi sunmaları gerektiği ifade edilmektedir. Bu yükümlülük, açık rızanın gerçekten özgür iradeyle verilip verilmediğinin güvencesidir.

Gereklilik ve Orantılılık İlkesi

Biyometrik veri işleme faaliyetinin amaçla sınırlı, ölçülü ve gerçekten gerekli olması gerekmektedir. Yalnızca kolaylık, hız ya da alışkanlık gibi gerekçelerle biyometrik veri kullanılmasının hukuka uygunluğu bulunmamaktadır.

Veri Güvenliği Tedbirleri

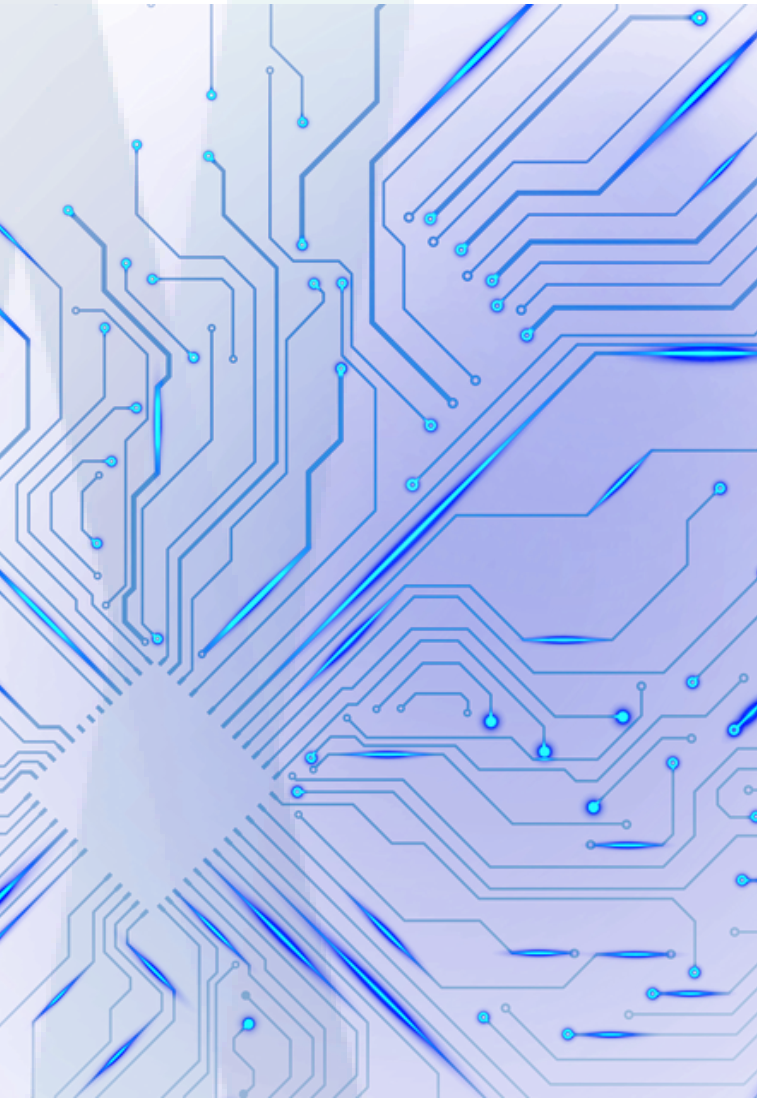
Biyometrik veriler, teknik açıdan yeniden üretilebilir nitelikte olduğu için daha güçlü güvenlik tedbirlerinin uygulanması gerekmektedir. Rehberde, kriptografik yöntemlerle koruma, erişim kontrolleri, şifreleme ve güvenli saklama gibi teknik ve idari önlemlerin hayata geçirilmesi gerektiği açıkça belirtilmiştir.

GLOBAL GELİŞMELER

FRANSIZ REKABET OTERİTESİNDEN APPLE'A 150 MİLYON EURO'LUK CEZA

Fransız Rekabet Otoritesi (Autorité de la concurrence), Apple'a 150 milyon euro tutarında bir ceza verdiğini duyurdu. Bu karar, Apple'ın uygulama mağazası politikalarının rekabeti engelleyici olduğu ve piyasa hakimiyetini kötüye kullandığı iddialarına dayanıyor.

Otorite, Apple'ın App Store üzerinden uygulama geliştiricilere yönelik getirdiği kısıtlamaların, rekabeti bozucu ve tüketici seçeneklerini sınırlayıcı nitelikte olduğunu belirtti. Özellikle, Apple'ın kendi uygulamalarına avantaj sağladığı ve üçüncü taraf geliştiricilerin dezavantajlı duruma düşürüldüğü ifade edildi.



Apple ise cezaya itiraz edeceğini açıkladı. Şirket, App Store'un hem geliştiriciler hem de kullanıcılar için güvenli, istikrarlı ve yüksek kaliteli bir dijital ekosistem sunduğunu savunarak, uyguladığı kuralların rekabeti sınırlamak değil, platform güvenliğini sağlamak amacıyla tasarlandığını belirtti. Apple ayrıca, geliştiricilere küresel ölçekte erişim sağladığını ve kullanıcıların güvenini korumak için sıkı içerik denetim süreçlerinin sürdürüldüğünü vurguladı.

Bu gelişme, Avrupa genelinde teknoloji devlerine yönelik artan regülasyon baskısının bir yansıması olarak değerlendiriliyor. Fransa'nın kararı, özellikle dijital platformların piyasa gücünü nasıl kullandığına dair artan endişelerin somut bir örneği oldu.

Uzmanlar, bu tür yüksek profilli davaların sadece Apple değil, Google, Meta, Amazon gibi diğer büyük oyuncular için de emsal niteliğinde olabileceğini ve Avrupa'da teknoloji hukukunun seyrini değiştirecek nitelikte bir dönemin başladığını ifade ediyor.

MCLEGAL
Metin-Çiçek Avukatlık Ortaklığı
Attorney Partnership

GLOBAL GELİŞMELER

MICROSOFT ADVERTISING, KULLANICI ONAYI UYGULAMASINI 5 MAYIS 2025'TE ZORUNLU HALE GETİRİYOR

Microsoft Advertising, dijital reklamcılıkta kullanıcı gizliliğine verdiği önemi artırarak, 5 Mayıs 2025 tarihinden itibaren reklam verenlerin kullanıcı onayı sinyalleri sağlamasını zorunlu kıldığını duyurdu.

Neden Önemli?

Bu adımın arkasındaki temel nedenler şunlardır:

- Gizlilik Düzenlemeleriyle Uyum: Kullanıcı onayı sinyalleri, GDPR gibi gizlilik yasalarıyla uyum sağlamaya yardımcı olur ve olası cezaların önüne geçer.
- Kullanıcı Güveni: Kullanıcıların gizlilik tercihlerine saygı göstermek, markalara olan güveni artırır.
- Reklam Performansı: Onaylı verilerle, reklam kampanyalarının etkinliğini ölçmek ve optimize etmek daha mümkün olur.

Onay Modu Nedir?

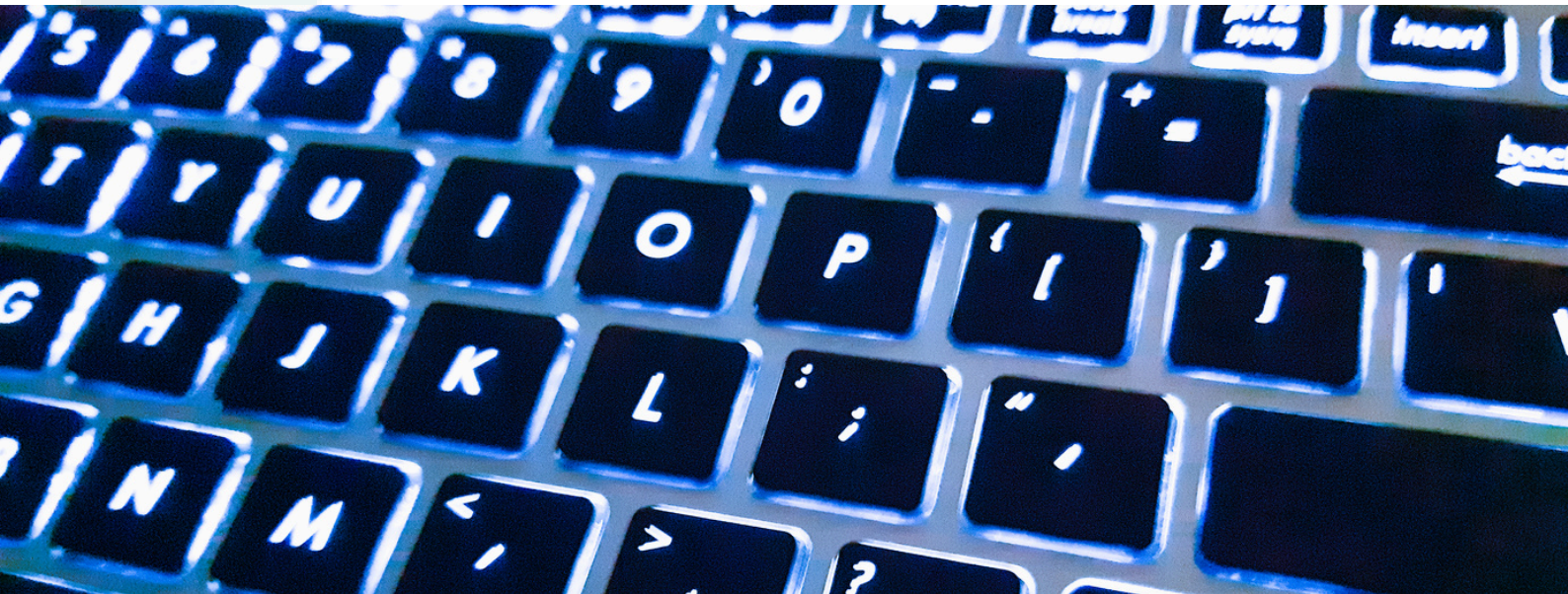
Onay Modu, Microsoft Advertising'in, kullanıcı gizliliği tercihlerini ve gizlilik düzenlemelerini dikkate alarak veri toplama ve reklam izleme işlemlerini düzenleyen bir özelliktir. Bu özellik, reklam verenlerin kullanıcıların izleme onay durumuna göre çerez erişimini ayarlamalarına olanak tanır.

Nasıl Uygulanır?

Reklam verenler, kullanıcı onayı sinyallerini iletmek için şu yöntemlerden birini kullanmalıdır:
Doğrudan Entegrasyon: UET, Evrensel Piksel, Segment veya Dönüşüm pikseli üzerinden Onay Modu'nu uygulamak.
IAB Onay ve Şeffaflık Çerçevesi (TCF): TCF 2.0 dizesi veya tercihinize bağlı olarak bir Onay Yönetim Platforması (CMP) aracılığıyla onay sinyalleri göndermek.
Üçüncü Taraf Araçlarıyla Entegrasyon: Örneğin, Google Tag Manager gibi araçlarla Microsoft'un Onay Modu'nu entegre etmek.

Önemli Tarihler:

- 24 Temmuz 2023: Microsoft Advertising, IAB TCF v2.0 desteğini başlattı.
- 31 Mart 2025: Kullanıcı onayı sinyalleri gerekliliği duyuruldu.
- 5 Mayıs 2025: Uygulama zorunluluğu başlayacak.



GLOBAL GELİŞMELER

AVRUPA KOMİSYONU UZMAN GRUBU, B2B VERİ PAYLAŞIMI İÇİN REHBER YAYINLADI

Avrupa Komisyonu'na bağlı bir uzman grubu, işletmeler arası (B2B) veri paylaşımı ve bulut bilişim sözleşmeleri konularında rehber niteliğinde bir rapor yayımladı. Bu rapor, gönüllü veri paylaşımının hukuki hakları nasıl koruyabileceğine dair detaylı bilgiler sunuyor.

Ana Noktalar:

- Veri Paylaşımının Teşviki: Raporda, işletmeler arasındaki veri paylaşımının artırılması gerektiği vurgulanıyor. Bu durumun, inovasyonu desteklemesi ve ekonomik büyümeye katkı sağlaması bekleniyor.
- Hukuki Çerçeve: Veri paylaşımı sırasında tarafların hukuki haklarının korunması için öneriler sunuluyor. Özellikle, gönüllü veri paylaşımının nasıl güvence altına alınacağına dair rehberlik sağlanıyor.
- Bulut Bilişim Sözleşmeleri: Raporda, bulut bilişim hizmet sağlayıcıları ile müşterileri arasındaki sözleşmelerin şeffaf ve adil olmasına yönelik tavsiyeler bulunuyor. Bu sayede, veri güvenliği ve erişilebilirliği konularında netlik sağlanması hedefleniyor.

Önemi:

Bu rehber, Avrupa'daki işletmelerin veri paylaşımı ve bulut bilişim hizmetleri konularında daha bilinçli ve hukuki açıdan güvenli adımlar atmasına olanak tanıyacak. Ayrıca, veri ekonomisinin gelişimine katkıda bulunarak, dijital dönüşüm süreçlerini hızlandırması bekleniyor.

GLOBAL GELİŞMELER

ICO, KİŞİSEL VERİLERİN ANONİMLEŞTİRİLMESİ KONUSUNDA YENİ REHBER YAYINLADI

İngiliz Bilgi Komiserliği (ICO), kişisel verilerin anonimleştirilmesi ve takma adlandırılması konularında kapsamlı bir rehber yayımladı. Bu rehber, veri paylaşımları ve bulut bilişim hizmetleri sunan tüm kuruluşlara, anonimleştirme tekniklerini etkili ve güvenli bir şekilde kullanma konusunda yol göstermeyi amaçlıyor.

Rehberin Öne Çıkan Noktaları:

- Anonimleştirme ve Takma Adlandırma Tanımları: Rehber, anonimleştirme ve takma adlandırma kavramlarını net bir şekilde tanımlayarak, bu tekniklerin veri koruma hukukundaki yerini açıklıyor.
- Etkin Anonimleştirme İçin Kriterler: Verilerin anonimleştirilmesinin etkin olabilmesi için hangi kriterlerin göz önünde bulundurulması gerektiği detaylandırılıyor.
- Hukuki Yükümlülükler ve Sorumluluklar: Anonimleştirme ve takma adlandırma uygulamalarının, veri koruma yasaları çerçevesindeki etkileri ve kuruluşların bu konudaki yükümlülükleri ele alınıyor.
- İyi Uygulama Önerileri: Veri anonimleştirme süreçlerinde izlenmesi gereken en iyi uygulamalar ve teknikler paylaşılıyor.
- Teknik ve İdari Önlemler: Verilerin anonimleştirilmesi sırasında alınması gereken teknik ve idari önlemlerle ilgili tavsiyeler sunuluyor.

ICO'nun yayımladığı bu rehber, özellikle veri paylaşımında ve kişisel verilerin işlenmesinde güvenliği artırmayı hedefleyen kuruluşlar için büyük önem taşıyor. Anonimleştirme, kişisel verilerin kimliği tanımlanabilir olmaktan çıkarılması sürecini ifade eder ve bu, özellikle büyük veri analitiği ve araştırma projelerinde yaygın olarak kullanılır. ICO, anonimleştirme tekniklerinin doğru uygulanmaması durumunda kişisel verilerin hala tespit edilebilir olabileceğine dikkat çekerek, kuruluşları bu süreçte dikkatli olmaya çağırıyor. Rehber, aynı zamanda GDPR kapsamında veri sorumlularının uyum sağlamalarına yardımcı olmak amacıyla pratik çözümler sunuyor.