DL | Avukatlık Bürosu

KİŞİSEL VERİLERİ KORUMA HUKUKU
GÜNCEL GELİŞMELER
TEMMUZ – AĞUSTOS – EYLÜL 2025

TÜRKİYE'DEKİ GELİŞMELER

VERİ İHLALİ BİLDİRİMLERİ

Louis Vuitton Çantacılık Ticaret Anonim Şirketi tarafından Kişisel Verileri Koruma Kuruluna ("KVK Kurulu") bildirilen veri ihlali, 10.07.2025 tarihinde Kişisel Verileri Koruma Kurumunun ("KVK Kurumu") internet sitesinde yayımlanmıştır.

Veri sorumlusu Louis Vuitton Çantacılık Ticaret Anonim Şirketi tarafından KVK Kuruluna veri ihlali ("**Veri İhlali**" veya "**İhlal**") bildirilmiştir. Bildirimde aşağıdaki hususlar belirtilmiştir:

- İhlalin 07.06.2025 tarihinde başladığı ve 02.07.2025 tarihinde tespit edildiği,
- Müşterilere ait kişisel verileri içeren veritabanına yetkisiz erişim sağlanması ile ihlalin gerçekleştiği; üçüncü taraf bir hizmet sağlayıcının yöneticisi tarafından kullanılan bir servis hesabının ele geçirildiğinin belirlendiği,
- İhlalden etkilenen ilgili kişi grubunun müşteri/potansiyel müşteriler olduğu
- İhlalden etkilenen kişisel veri kategorilerinin kimlik ve iletişim verileri olduğu, incelemelerin devam ettiği,
- İhlalden Türkiye'de yerleşik 142.995 kişinin etkilendiği

İlgili kamuoyu duyurusuna buradan ulaşabilirsiniz.

Bold LLC tarafından KVK Kuruluna bildirilen veri ihlali, 24.07.2025 tarihinde KVK Kurumu internet sitesinde yayımlanmıştır.

Veri sorumlusu Bold LLC tarafından KVK Kuruluna veri ihlali bildirilmiştir. Bildirimde aşağıdaki hususlar belirtilmiştir:

- Porto Riko'da çevrimiçi iş arama hizmeti veren veri sorumlusunun kullanıcıların özgeçmişlerini düzenlerken gerçek zamanlı olarak ön izlemelerine olanak tanıyan yeni bir özelliğin yetkisiz erişime açık olduğunun 12.07.2025 tarihinde tespit edildiği,
- Dahili incelemeler sonucunda, olayın 10.03.2023 tarihinde, sunucu ortamının daha hızlı performans için anonimleştirilmiş verileri önbelleğe almak üzere görüntülenebilir hale geldiği, bu açık dolayısıyla sadece 1 defa yetkisiz erişimin gerçekleştiği,
- İhlalden anonim hale getirilmiş isim, iletişim ve özgeçmiş verilerinin etkilendiği, her özgeçmişte yer alan kişisel verilerin niteliği ve kapsamı, kullanıcıların hangi bilgileri ekleyeceğini belirlemesine bağlı olarak önemli ölçüde değişiklik gösterdiği, bazı özgeçmişler yalnızca ad ve soyad gibi temel tanımlayıcılar içerebilirken, diğerleri iletişim bilgileri, istihdam geçmişi, eğitim geçmişi veya bazı durumlarda

fotoğraflar veya gönüllü olarak açıklanan diğer bilgiler gibi ek kişisel bilgiler içerebildiği; gerekli incelemelerin devam ettiği,
- İhlalden etkilenen ilgili kişi gruplarının kullanıcılar ve aboneler/üyeler olduğu,
- İhlalden etkilenen ilgili kişi sayısının 3168 olduğu.

İlgili kamuoyu duyurusuna buradan ulaşabilirsiniz.

Yatırım Finansman Menkul Değerler A.Ş. tarafından KVK Kuruluna bildirilen veri ihlali, 24.07.2025 tarihinde KVK Kurumu internet sitesinde yayımlanmıştır.

Veri sorumlusu Yatırım Finansman Menkul Değerler A.Ş. tarafından KVK Kuruluna veri ihlali bildirilmiştir. Bildirimde aşağıdaki hususlar belirtilmiştir:

- İhlalin 20.07.2025 tarihinde gerçekleştiği ve aynı tarihte tespit edildiği,
- Veri sorumlusunun sunucuları ve istemci bilgisayarlarına, uluslararası ve uzman bir saldırı grubu tarafından fidye yazılımı saldırısı gerçekleştirilmiş olduğu,
- İhlalden etkilenen ilgili kişi sayısı, ilgili kişi grubu ve kişisel veri kategorilerinin henüz tespit edilemediği, bu hususta teknik incelemelerin henüz devam etmekte olduğu,
- İlgili kişilerin, yaşanan bu saldırıyla ilgili veri sorumlusunun tüm şubeleri ve 0 850 723 59 59 numaralı Yatırımcı Destek Hattı üzerinden destek alabileceği

İlgili kamuoyu duyurusuna buradan ulaşabilirsiniz.

Biletal İç ve Dış Ticaret A.Ş. tarafından KVK Kuruluna bildirilen veri ihlali, 14.07.2025 tarihinde KVK Kurumu internet sitesinde yayımlanmıştır.

Veri sorumlusu Biletal İç ve Dış Ticaret A.Ş. tarafından KVK Kuruluna veri ihlali bildirilmiştir. Bildirimde aşağıdaki hususlar belirtilmiştir:

- İhlalin; Bilgi Teknolojileri ve İletişim Kurumu'ndan gelen yazı uyarınca, veri sorumlusu bilişim ekipleri tarafından yürütülen çalışmalar sonucunda 11.08.2025 tarihinde tespit edildiği,
- Veri sorumlusuna ait olduğu bazı kişisel verilerin siber saldırganlar tarafından internet üzerindeki yasadışı platformlarda satışa sunulduğu,
- İhlalden etkilenen kişisel veri kategorilerinin; kimlik, iletişim ve müşteri işlem verileri olduğu,
- İhlalden etkilenen ilgili kişi grubunun müşteriler olduğu,
- Veri ihlalinden etkilenen ilgili kişi sayısının tahmini 7.800 kişi olduğu

İlgili kamuoyu duyurusuna buradan ulaşabilirsiniz.

Türk Tabipler Birliği tarafından KVK Kurumuna bildirilen veri ihlali, 14.07.2025 tarihinde KVK Kurumu internet sitesinde yayımlanmıştır.

Veri sorumlusu Türk Tabipler Birliği tarafından KVK Kuruluna veri ihlali bildirilmiştir. Bildirimde aşağıdaki hususlar belirtilmiştir:

- Belirsiz kaynaklar tarafından veri sorumlusu sistemine 08.08.2025 tarihinde siber saldırı gerçekleştirildiği, ancak siber saldırının nasıl gerçekleştiğinin bilinmediği,
- Siber saldırı neticesinde veri sorumlusu sisteminde yer alan kayıtlı dosyalara erişildiği ve silindiği,
- İhlalden etkilenen ilgili kişi gruplarının çalışanlar, kullanıcılar ve tabip odalarına kayıtlı üyeler olduğu,
- İhlalden etkilenen kişisel veri kategorilerinin kimlik, iletişim, lokasyon, hukuki işlem ve işlem güvenliği olduğu,
- Üye veri tabanına erişilemediğinden ihlalden etkilenen ilgili kişi sayısının henüz bilinmediği ancak muhtemelen etkilenebilecek ilgili kişi sayısının 107.000 olabileceği

İlgili kamuoyu duyurusuna buradan ulaşabilirsiniz.

GÜNCEL KARARLAR

KVK Kurulu tarafından ana faaliyet konusu özel nitelikli kişisel veri işleme olan veri sorumlularının Veri Sorumluları Siciline ("VERBİS") kayıt yükümlülüğüne ilişkin istisna kriteri hakkında 04.09.2025 tarihli ve 2025/1572 sayılı kararı yayımlanmıştır.

KVK Kurulu'nun 04.09.2025 tarihli ve 2025/1572 sayılı kararı 01.10.2025 tarihinde yayımlanmıştır. KVK Kurulu'nun 06.07.2023 tarih ve 2023/1154 sayılı kararı ile değişik 19.07.2018 tarih ve 2018/87 sayılı Kurul kararında yer alan "Yıllık çalışan sayısı 50'den az ve yıllık mali bilanço toplamı 100 milyon Türk lirasından az olan gerçek veya tüzel kişi veri sorumlularından ana faaliyeti konusu özel nitelikli kişisel veri işleme olmayanlar" ifadesinin güncellenmesi suretiyle;

- "Yıllık çalışan sayısı 50'den az ve yıllık mali bilanço toplamı 100 milyon Türk lirasından az olan gerçek veya tüzel kişi veri sorumlularından ana faaliyeti konusu kişisel veri işleme olmakla birlikte yıllık çalışan sayısı 10'dan az ve yıllık mali bilanço toplamı 10 milyon Türk lirasından az olan gerçek veya tüzel kişi veri sorumlularının" şeklinde değiştirilmesine,
- Sonuç olarak yıllık çalışan sayısı 10'dan az ve yıllık mali bilanço toplamı 10 milyon TL'nin altında olan gerçek veya tüzel kişi veri sorumlularının VERBİS'e kayıt yükümlülüğünden muaf tutulmuştur.

Bu itibarla kurul kararı ile muayenehaneler, eczaneler ve laboratuvarlar gibi ana faaliyet konusu özel nitelikli kişisel veriler işlemek olan veri sorumluları, eğer yıllık çalışan sayısı 10'dan az ve yıllık mali bilanço toplamı 10 milyon TL'nin altında ise istisna kapsamına dahil edilmiştir.

İlgili karara buradan ulaşabilirsiniz.

KVKK Kurumu tarafından ana faaliyet konusu özel nitelikli kişisel veri işleme olan ve yıllık çalışan sayısı ile mali bilançosu belirli sınırların altında kalan veri sorumlularının VERBİS'e kayıt yükümlülüğünden istisna tutulmasına karar verildiği 01.10.2025 tarihinde kamuoyuna duyurulmuştur.

KVK Kurulu'nun Kanun'un 16'ncı maddesi uyarınca, veri sorumlularının VERBİS kayıt yükümlülüğü bulunduğu; Kurul'un belirleyeceği objektif kriterler çerçevesinde istisnalar tanınabileceği belirtilmiştir. Daha önce 2018/87 sayılı ve 2023/1154 sayılı Kurul kararları ile yıllık çalışan sayısı ve mali bilanço tutarı kriterlerine göre ana faaliyet konusu özel nitelikli kişisel veri işleme olmayan veri sorumlularının istisna kapsamına alınmış olduğu hatırlatılmıştır. Gelinen aşamada, mikro işletme niteliğindeki veri sorumlularının sınırlı personel ve mali kaynakla faaliyet gösterdiği, hukuki ve teknik imkânlarının kısıtlı olduğu ve sınırlı sayıda kişisel veri işledikleri dikkate alınarak, ana faaliyet konusu özel nitelikli kişisel veri işleme olan veri sorumluları için de yeni bir değerlendirme yapılması gerektiği vurgulanmıştır. Bu kapsamda, 04.09.2025 tarih ve 2025/1572 sayılı Kurul Kararı ile; ana faaliyet konusu özel nitelikli kişisel veri işleme olan ancak yıllık çalışan sayısı 10'dan az ve yıllık mali bilanço toplamı 10 milyon Türk Lirasından az olan gerçek veya tüzel kişi veri sorumlularının da Sicile kayıt ve bildirim yükümlülüğünden istisna tutulmasına karar verildiği duyurulmuştur.

İlgili kamuoyu duyurusuna buradan ulaşabilirsiniz.

DUYURULAR VE HABERLER

KVK Kurumu tarafından okul döneminde çocukların kişisel verilerinin korunmasına ilişkin ebeveynlere tavsiyeler yayımlanmıştır.

KVK Kurumunun LinkedIn okul döneminde çocukların kişisel verilerinin korunmasına ilişkin ebeveynlere bazı tavsiyeler yayımlanmıştır.

- Çocukların kullandığı akıllı cihazların gizlilik ve güvenlik ayarlarının düzenlenmesi.
- Gizlilik ve güvenlik ayarlarının, internet tarayıcısı ayarlarının ve uygulama izinlerinin periyodik olarak kontrol edilmesi.
- Ölçülü ve bilinçli kullanımı teminen ebeveyn kontrolü gibi imkânlardan yararlanılması.
- Sosyal ağlardaki sahte hesaplara karşı çocukların bilgilendirilmesi ve kötü niyetli kişilerin kimliklerini gizleyebileceği konusunda uyarılması.
- Çocuklara, tehdit oluşturabileceğini düşündükleri kullanıcıları engelleyebileceklerinin hatırlatılması ve dijital ortamda da yalnız bırakılmamaları.
- Çocuklara, karşılaştıkları şüpheli içerik veya mesajları ebeveynleriyle paylaşmaları gerektiğinin hatırlatılması.
- Çocuklara ilişkin okul bilgisi, adres, ders notu, ses, fotoğraf veya video gibi kişisel verilerin herkese açık şekilde paylaşılmaması.
- Çocukları yaş grubuna uygun olmayan içeriklerden ve zararlı olduğu bilinen oyunlardan koruyacak tedbirlerin alınması.
- Oyun bağımlılığı ve olumsuz etkilerine karşı oyun oynama sürelerinin sınırlandırılması.
- Siber zorbalık veya benzeri tehditler karşısında gerekli durumlarda ilgili kamu kurum ve kuruluşlarından destek alınması.

İlgili tavsiyelere buradan ulaşabilirsiniz.

KVK Kurumu tarafından yapay zekâ alanında kişisel verilerin korunmasına dair tavsiyeler yayımlanmıştır.

KVK Kurumunun LinkedIn hesabından yapay zekâ alanında kişisel verilerin korunmasına dair tavsiyeler yayımlanmıştır.

Yapay zekâ alanında kişisel verilerin korunmasına dair tavsiyeler aşağıdaki şekilde belirtilmiştir:

- Tasarımda, ulusal ve uluslararası düzenleme ve/veya belgelerle tutarlı olarak kişisel veri mahremiyetini esas alan bir yaklaşım gözetilmelidir.
- Temel hak ve özgürlükler üzerindeki muhtemel olumsuz sonuçlar gözetilerek, uygun risk önleme ve azaltma tedbirlerine dayalı ihtiyatlı bir yaklaşım benimsenmelidir.
- Veri toplama da dâhil olmak üzere veri işlemenin her aşamasında, temel hak ve özgürlükler gözetilerek, ilgili kişiler üzerinde meydana gelebilecek ayrımcılık riski veya diğer olumsuz etkiler ve ön yargılar önlenmelidir.
- Kullanılan kişisel verilerin kalitesi, niteliği, kaynağı, miktarı, kategori ve içeriği değerlendirilerek asgari veri kullanımına gidilmeli; geliştirilen modelin doğruluğu sürekli izlenmelidir.
- Bağlamından koparılmış algoritma modelleri, bireyler ve toplum üzerinde olumsuz etkilere sebep olma riski açısından dikkatle değerlendirilmelidir.

- İnsan hakları temelli, etik ve sosyal yönelimli yapay zekâ uygulamalarının tasarlanmasına ve potansiyel önyargıların tespit edilmesine katkıda bulunabilecek akademik kurumlarla irtibata geçilmeli; şeffaflık ve paydaş katılımının zor olabileceği alanlarda tarafsız uzman kişi ve kuruluşların görüşü alınmalıdır.
- Bireylere, görüşlerini ve kişisel gelişimlerini etkileyen teknolojilere dayalı işlemelerle ilgili itiraz hakkı tanınmalıdır.
- Yapay zekâ sistemlerinin kişisel verileri analiz etme ve kullanma gücü göz önüne alındığında, kişisel verilerin işlenmesinde, ilgili kişilerin ulusal ve uluslararası mevzuattan doğan hakları korunmalıdır.
- Uygulamalardan özellikle etkilenmesi muhtemel olan bireylerin ve grupların aktif katılımına dayalı risk değerlendirmesi teşvik edilmelidir.
- Bireylerin münhasıran kendi görüşleri dikkate alınmaksızın otomatik işlemeye dayalı olarak kendilerini etkileyecek bir karara maruz kalmamalarını sağlayacak ürün ve hizmetler tasarlanmalıdır.
- Üretimde kişilik haklarına daha az müdahale eden alternatifler de sunulmalı, kullanıcıların seçim yapma özgürlüğü güvence altına alınmalıdır.
- Ürün ve hizmetlerin tasarımından başlayarak yaşam döngüsü boyunca kişisel verilerin korunması hukukuna uygunluk açısından tüm paydaşlar için hesap verebilirliği sağlayacak algoritmalar benimsenmelidir.
- Kullanıcının veri işleme faaliyetini durdurabilme hakkı tanınmalı ve kullanıcılara ait verilerin silinmesi, yok edilmesi veya anonim hale getirilmesi imkânı tasarlanmalıdır.
- Uygulama ile iletişime giren kişiler, kişisel veri işleme faaliyetinin gerekçeleri, kişisel verilerin işlenmesinde kullanılan yöntemlerin detayları ile muhtemel sonuçları hakkında aydınlatılmalı ve gerekli haller için etkili bir veri işleme onay mekanizması tasarlanmalıdır.

İlgili tavsiyelere buradan ulaşabilirsiniz.

KVK Kurumu tarafından 16.11.2023 – 17.11.2023 tarihleri arasında düzenlenen II. Uluslararası Kişisel Verileri Koruma Kongresi kitaplaştırılarak kullanıma sunulmuştur.

KVK Kurumu ve Bilkent Üniversitesi Hukuk Fakültesi iş birliği ile 16.11.2023 – 17.11.2023 tarihleri arasında düzenlenen II. Uluslararası Kişisel Verileri Koruma Kongresi kapsamında kişisel verilerin korunmasıyla ilgili 32 farklı konuda sunulan metinler derlenerek kitaplaştırılmıştır.

İlgili kitaba buradan ulaşabilirsiniz.

KVK Kurumu tarafından alacaklı vekillerinin borçlu yakınlarının telefon numaralarına erişerek borç bilgisi paylaşımının KVKK'ya aykırılık teşkil edebileceği kamuoyuna duyurulmuştur.

KVK Kurumunun internet sitesinde yayımlanan duyuru kapsamında;

- Kuruma ulaşan ihbarlarda, alacaklı vekillerinin borçlu kişilerin yakınlarının telefon numaralarına erişerek borç bilgilerini içeren arama ve mesajlar gerçekleştirdiği belirtilmiştir.
- 6698 sayılı Kişisel Verilerin Korunması Kanunu'nun ("**6698 sayılı Kanun**") çerçevesinde kişisel verilerin ancak hukuka uygun, belirli ve açık amaçlar için, doğru ve güncel olarak ve ölçülü biçimde işlenebileceği; açık rıza bulunmadıkça veya kanunda öngörülen işleme şartlarından biri mevcut olmadıkça veri işlenemeyeceği vurgulanmıştır.
- 6698 sayılı Kanun'un 12. maddesi uyarınca veri sorumlularının kişisel verilerin hukuka aykırı işlenmesini ve erişimini önlemek için gerekli teknik ve idari tedbirleri almakla yükümlü olduğu, aksi halde 15.000 TL ile 1.000.000 TL arasında idari para cezası uygulanacağı duyurulmuştur.

- Açık rıza veya başka bir işleme şartı olmaksızın borçlu kişilerin yakınlarının bilgilerine erişilmesinin ve borç bilgilerinin paylaşılmasının 6698 sayılı Kanun'a aykırılık teşkil edebileceği; alacaklı vekillerinin borç tahsil işlemlerinde hem borçluların hem de ilgisi olmayan üçüncü kişilerin kişisel verilerini işlerken Kanun'a uygun hareket etmesi gerektiği belirtilmiştir.

İlgili duyuruya buradan ulaşabilirsiniz.

6698 sayılı Kanun'un GDPR ile uyumlaştırılmasına yönelik çalışmaların 2026 üçüncü çeyrekte tamamlanacağı Resmi Gazete'de yayımlanan "Orta Vadeli Program" kapsamında belirtildi.

2026–2028 dönemine ilişkin Orta Vadeli Program'da, 6698 sayılı Kanun'un GDPR ile tam uyumlu hale getirilmesine yönelik çalışmaların tamamlanacağı ifade edilirken, ulusal mevzuatın Avrupa Birliği Tüzüğü doğrultusunda güncellenmesinin de hedeflendiği açıklanmıştır.

İlgili program metnine buradan ulaşabilirsiniz.

KVK Kurumu tarafından 11.09.2025 tarihinde Haziran – Ağustos aylarına ilişkin sosyal medyada kişisel verilerin korunmasını ele alan 9 sayılı bülten yayımlanmıştır.

Kamu kurumlarına yönelik kurumsal sosyal medya kullanım rehberi, sosyal medyada kişisel verilerin korunmasına ilişkin araştırmalar, mobil uygulamalarda kişisel verileri işleyen taraflara yönelik tavsiyeler, sosyal medyada öne çıkan platform türleri, ebeveyn paylaşımları *(sharenting),* çocukların sosyal medya kullanımında ebeveynlere yönelik tavsiyeler ve daha güvenli bir sosyal medya kullanımına ilişkin önerileri içeren 9 sayılı bülten yayınlanmıştır.

İlgili bültene buradan ulaşabilirsiniz.

DÜNYADAKİ GELİŞMELER

DUYURULAR VE HABERLER

Avrupa Komisyonu, Dijital Hizmetler Tüzüğü ("DSA") kapsamında küçüklerin çevrim içi ortamda korunmasına yönelik hazırlanan rehberin son halini yayımladı.

DSA kapsamında çocuklar ve gençlerin çevrim içi güvenliğini artırma konusunda bir dönüm noktası olarak nitelendirilen Rehber'de sunulan temel tavsiyeler arasında;

- Reşit olmayanların kişisel bilgilerinin, verilerinin ve sosyal medya içeriklerinin, bağlantıda olmadıkları kişiler tarafından görülmesini önlemek ve yabancılarla istenmeyen temas riskini azaltmak amacıyla, bu kullanıcıların hesaplarının varsayılan olarak gizli hale getirilmesi,
- Platformların öneri sistemlerinin, çocukların zararlı içeriklerle karşılaşma veya belirli içerik döngülerine takılı kalma riskini azaltacak şekilde değiştirilmesi ve bu doğrultuda çocukların kendi içerik akışları üzerinde daha fazla kontrol sahibi olmaları konusunda teşvik edilmeleri,
- Çocuklara, herhangi bir kullanıcıyı engelleme veya sessize alma imkânı tanınması, açık rızaları olmaksızın gruplara eklenmelerinin önüne geçilmesi ve bu sayede siber zorbalığın önlenmesine katkı sunulabilmesi,
- Reşit olmayan kullanıcıların paylaştığı içeriklerin indirilmesinin veya ekran görüntüsünün alınmasının yasaklanması; bu sayede cinsel içerikli veya mahrem içeriklerin istenmeyen biçimde yayılması ve cinsel istismar amacıyla kullanılmasının önlenmesine katkı sağlanabilmesi,
- Özellikle etkileşimi artırmaya yönelik tasarlanmış ikna edici tasarım özelliklerinin kaldırılması ve çevrim içi platformlara entegre edilen yapay zekâ sohbet robotlarına yönelik güvenlik önlemleri getirilmesi,

- Çocukların ticari okuryazarlık eksikliklerinin istismar edilmemesinin sağlanması ve onları manipülatif olabilecek, istenmeyen harcamalara yol açabilecek veya bağımlılık yaratabilecek davranışlara neden olabilecek ticari uygulamalardan (bazı sanal para birimleri veya ganimet kutuları gibi) koruyacak önlemlerin alınması,
- İçerik denetleme ve şikâyet mekanizmalarının iyileştirilmesini, hızlı geri bildirim sağlanmasını ve ebeveyn denetim araçları için asgari gerekliliklerin getirilmesini içeren tedbirlerin uygulanması gibi hususlar yer almaktadır.

İlgili rehbere buradan ulaşabilirsiniz.

Fransa Veri Koruma Otoritesi ("CNIL"), kullanıcı rızasına tâbi olmadan uygulanabilecek hedef kitle ölçüm çözümlerinin belirlenmesine yardımcı olmak amacıyla bir öz değerlendirme aracı yayımladı.

CNIL, *"Informatique et Libertés"* Yasası'nın 82. maddesi uyarınca bazı çerezlerin (özellikle ölçüm ve analiz çerezlerinin) kullanıcı onayına gerek olmaksızın kullanılabileceğini belirtmiştir.

Bu istisnadan yararlanmak için çerezlerin:

- Yalnızca site veya uygulamanın performans ölçümü, teknik optimizasyonu veya hata tespiti gibi seyirci ölçümüne (audience measurement) yönelik amaçlarla kullanılması,
- Yalnızca istatistiksel ve anonim veriler üretmesi,
- Üçüncü taraflarla veri paylaşımı veya kullanıcıların farklı sitelerde izlenmesi gibi faaliyetlere yol açmaması gerekmektedir.

CNIL ayrıca şu hususlara dikkat çekmiştir:

- Kullanıcıların bu çerezlerin kullanımından gizlilik politikası aracılığıyla bilgilendirilmesi,
- Çerezlerin azami 13 ay, toplanan verilerin ise azami 25 ay süreyle saklanması,
- Bu sürelerin periyodik olarak gözden geçirilmesi önerilmektedir.

İlgili değerlendirmeye buradan ulaşabilirsiniz.

Avrupa Veri Koruma Kurulu ("EDPB") ile Avrupa Veri Koruma Denetçisi ("EDPS"), AB Genel Veri Koruma Tüzüğü ("GDPR") kapsamında özellikle kayıt tutma yükümlülüklerinin basitleştirilmesi önerisine ilişkin olarak kabul edilen ortak görüş metnini yayımladı.

EDPB ile EDPS, GDPR'nin 30. maddesinde öngördüğü kayıt tutma yükümlülüklerinin basitleştirilmesine yönelik değişiklik teklifine ilişkin ortak görüş metnini yayımladı.

Söz konusu teklif, özellikle küçük ve orta ölçekli işletmeler (KOBİ) ile small mid-cap (SMC) şirketler için idari yüklerin hafifletilmesini amaçlıyor. Bu kapsamda, kayıt tutma yükümlülüğünden muafiyet sınırının 250 çalışandan 750 çalışana çıkarılması ve yalnızca yüksek riskli veri işleme faaliyetleri için bu muafiyetin uygulanmaması öngörülüyor.

EDPB ve EDPS, genel olarak değişiklik teklifini olumlu karşılasa da, düzenlemenin orantılılık ilkesine uygun olarak netleştirilmesi, kamu kurumlarının kapsam dışında tutulması ve genişletilen muafiyetin gerekçesinin daha ayrıntılı açıklanması gerektiğini vurguladı.

İlgili açıklamaya buradan ulaşabilirsiniz.

Avrupa Komisyonu, çocuklar ve gençler için daha güvenli bir çevrim içi dünya oluşturma yönündeki kapsamlı çalışmaların bir parçası olarak, 2026 yılının başlarında yayımlanması beklenen siber zorbalığa karşı eylem planının geliştirilmesini desteklemek amacıyla, siber zorbalık konusunda kamuoyu görüşüne başvurulduğunu duyurdu.

Avrupa Komisyonu tarafından, 2026 yılı başında açıklanması beklenen "AB Siber Zorbalıkla Mücadele Eylem Planı"nın hazırlanmasına yönelik olarak bir kamuoyu istişaresi ve görüş çağrısı başlatıldığı duyurulmuştur.

Komisyon Başkan Yardımcısı Virkkunen tarafından yapılan açıklamada, çocuk ve gençlerin çevrimiçi ortamlarda giderek daha fazla siber zorbalığa maruz kaldığı, bu nedenle çevrimiçi dünyanın güvenli ve güçlendirici bir ortam haline getirilmesinin hedeflendiği belirtilmiştir. Komisyon Üyesi Micallef tarafından ise, internetin herkes için güvenli bir alan olması gerektiği, siber zorbalığın Avrupa Birliği içinde yeri olmayan bir tehdit olduğu ifade edilmiştir.

Hazırlanacak eylem planının, çocukların korunmasına, cinsiyet temelli risklere ve 29 yaş altı gençlerin kırılganlık durumuna odaklanacağı açıklanmıştır. Ayrıca, planın DSA kapsamındaki çocuk koruma rehberleri, uygulama önlemleri ve yaş doğrulama sistemi taslağıyla uyumlu şekilde geliştirileceği bildirilmiştir.

Kamuoyu istişaresi ve görüş toplama sürecinin 29 Eylül 2025 tarihine kadar devam edeceği; ayrıca Eylül ayında çocuklara özel bir danışma platformunun faaliyete geçirileceği belirtilmiştir.

İlgili duyuruya buradan ulaşabilirsiniz.

Avrupa Parlamentosu Araştırma Servisi ("EPRS"), yapay zekâ ile üretilen sahte içeriklerin çocuklar üzerindeki etkilerinin ele alındığı "Çocuklar ve Deepfake" başlıklı bir çalışma yayımladı.

EPRS tarafından hazırlanan çalışmada deepfake teknolojisinin gelişimi, yaygınlaşması ve toplumsal etkilerinin yanı sıra bu teknolojinin dolandırıcılık, manipülasyon, veri gizliliği ihlalleri ve siber zorbalık gibi kötü amaçlı kullanımları ile risklerin azaltılmasına yönelik alınabilecek tedbirler gibi hususlar incelenmektedir.

İlgili çalışmaya buradan ulaşabilirsiniz.

ABD'de "Yarışı Kazanmak: Amerika'nın Yapay Zekâ Eylem Planı" başlığını taşıyan kapsamlı bir eylem planı yayımlandı.

Beyaz Saray, Başkan Donald Trump'ın "Yapay Zekâ Alanında Amerikan Liderliğinin Önündeki Engellerin Kaldırılması"na ilişkin başkanlık kararnamesi doğrultusunda hazırlanan "Yarışı Kazanmak: Amerika'nın Yapay Zekâ Eylem Planı" başlıklı eylem planını yayımladığını duyurmuştur. Planın, insan refahı, ekonomik rekabet gücü ve ulusal güvenlik alanlarında "yeni bir altın çağ" başlatacağı ifade edilmiştir.

Eylem planı, Yeniliği Hızlandırmak, Amerikan Yapay Zekâ Altyapısını Güçlendirmek ve Uluslararası Diplomasi ve Güvenlikte Liderlik olmak üzere üç temel sütunda 90'dan fazla federal politika eylemi içermektedir. Başlıca politika adımları arasında; Amerikan yapay zekâ teknolojilerinin müttefik ülkelere güvenli şekilde ihracı, veri merkezleri ve yarı iletken tesislerinin hızlı biçimde inşasının teşvik edilmesi, yeniliği engelleyen düzenlemelerin kaldırılması ve büyük dil modellerinde ifade özgürlüğünün korunması yer almaktadır.

Beyaz Saray Bilim ve Teknoloji Politikaları Ofisi Direktörü Michael Kratsios, söz konusu planın ABD'nin küresel yapay zekâ liderliğini pekiştirmeyi hedeflediğini belirtmiştir. Planın, yenilik, altyapı ve uluslararası işbirliği temelinde ABD'nin ekonomik ve askeri üstünlüğünü koruma stratejisini ortaya koyduğu ifade edilmiştir. Dışişleri

Bakanı ve Ulusal Güvenlik Danışmanı Marco Rubio tarafından yapılan açıklamada ise, "Yapay zekâ yarışını kazanmanın ABD için müzakere edilemez bir zorunluluk olduğu" vurgulanmıştır.

İlgili eylem planına buradan ulaşabilirsiniz.

Avrupa Komisyonu, genel amaçlı yapay zekâ modelleri sağlayıcılarının DSA kapsamındaki yükümlülüklerini yerine getirmelerine yardımcı olmak amacıyla hazırlanan ve genel amaçlı yapay zekâ uygulama kurallarını tamamlayan rehberi yayımladı.

Avrupa Komisyonu tarafından, 2 Ağustos 2025 tarihinde yürürlüğe girecek AI Act kapsamındaki yükümlülüklerin uygulanmasına destek olmak amacıyla, genel amaçlı yapay zekâ modelleri sağlayıcılarına yönelik kılavuzların yayımlandığı belirtilmiştir.

Kılavuzlarda, söz konusu yükümlülüklerin kapsamının açıklığa kavuşturularak AI ekosistemindeki tüm paydaşlar için hukuki belirlilik sağlanmasının ve Genel Amaçlı Yapay Zekâ Uygulama Kuralları belgesiyle uyumun güçlendirilmesinin hedeflendiği ifade edilmiştir.

Komisyon Başkan Yardımcısı Henna Virkkunen tarafından yapılan açıklamada, kılavuzların AI Act'in etkin ve uyumlu şekilde uygulanmasını destekleyeceği, bu sayede yenilikçiliğin güvenli, şeffaf ve Avrupa değerleriyle uyumlu biçimde sürdürülebileceği belirtilmiştir.

Kılavuzlarda, genel amaçlı yapay zekâ modellerinin, 10^23 işlem gücünü aşan hesaplama kaynaklarıyla eğitilen ve metin, ses, görüntü veya video üretebilen sistemler olarak tanımlandığı ifade edilmiştir. Ayrıca, "sağlayıcı" ve "piyasaya arz" kavramlarının kapsamı açıklığa kavuşturulmuş; şeffaflık koşullarını karşılayan açık kaynak lisanslı modellerin belirli yükümlülüklerden muaf tutulacağı belirtilmiştir.

Son olarak, kılavuzlarda temel haklara, güvenliğe veya model üzerindeki kontrolün kaybedilmesine yönelik sistemik riskler taşıyan ileri düzey yapay zekâ modellerine ilişkin olarak, bu risklerin değerlendirilmesi ve azaltılması yönünde özel yükümlülükler getirileceği ifade edilmiştir.

İlgili rehbere buradan ulaşabilirsiniz.

Kanada Mahremiyet Komisyonerliği Ofisi ("OPC"), konuya ilişkin alınan görüşlerin ardından, kamu ve özel sektör kuruluşlarınca biyometrik verilerin işlenmesinde gizliliğin korunmasına yönelik yeni bir rehber yayımladı.

Kanada Gizlilik Komiseri tarafından, yüz tanıma ve parmak izi tarama gibi biyometrik teknolojilerin kimlik doğrulama ve hizmet sunumunda giderek daha yaygın hale geldiği dikkate alınarak, biyometrik girişimlerde gizliliğin korunmasına ilişkin yeni bir rehber yayımlandı.

Söz konusu rehberin, hem kamu hem özel sektör kuruluşları için hazırlandığı ve OPC tarafından yürütülen bir kamu istişaresi sürecini takiben oluşturulduğu ifade edilmiştir. Rehberde, biyometrik verilerin kişinin bedeniyle doğrudan bağlantılı, genellikle benzersiz ve zamanla değişme olasılığı düşük olduğu; bu nedenle sağlık durumu, ırk veya cinsiyet gibi hassas bilgileri ortaya çıkarabileceği belirtilmiştir.

Rehberde, biyometrik teknolojilere ilişkin projelerin planlanması ve uygulanmasında dikkate alınması gereken temel hususların belirlendiği; veri toplama, kullanma ve paylaşma amaçlarının uygunluğunun, risklerin orantılılık ilkesine göre değerlendirilmesinin ve açıklık, veri güvenliği ve doğruluk gibi unsurların sağlanmasının önemine

vurgu yapıldığı ifade edilmiştir. Ayrıca, rehberin biyometrik uygulamalarda açık rıza koşullarını netleştireceği belirtilmiştir.

Kasım 2023 – Şubat 2024 döneminde yürütülen kamu istişaresi kapsamında 34 yazılı görüşün alındığı ve 31 kuruluşla toplantılar gerçekleştirildiği açıklanmıştır. İstişare süreci sonrasında rehberin, paydaş geri bildirimleri doğrultusunda güncellendiği; bu kapsamda tanımların netleştirildiği, yasal gerekliliklerle uyumun güçlendirildiği, teknik standartların ve en iyi uygulamaların detaylandırıldığı belirtilmiştir.

Kanada Gizlilik Komiseri Philippe Dufresne, açıklamasında kuruluşların biyometrik verileri kullanırken gizliliği merkeze alan bir yaklaşım benimsemeleri gerektiğini, bu şekilde gizliliğe öncelik verilmesinin hem yeniliği destekleyeceğini hem de daha güvenli bir dijital toplumun oluşumuna katkı sağlayacağını ifade etmiştir.

İlgili rehbere buradan ulaşabilirsiniz.

CNIL, kişisel verilerin sızdırılması ve özellikle IBAN bilgisinin çalınması durumunda bireylerin karşılaşabileceği riskler ile alınabilecek önlemlere ilişkin bir bilgilendirme metni yayımladı.

CNIL tarafından, veri ihlallerinin kişisel verilerin sızdırılması, çalınması veya kaybedilmesi şeklinde gerçekleşebileceği ve bu durumların hem kazara hem de kötü niyetli eylemlerden kaynaklanabileceği belirtilmiştir. Bu tür ihlallerin, verilerin internet ortamında satışa sunulması veya diğer veri sızıntılarıyla birleştirilmesi gibi riskler doğurabileceği ifade edilmiştir.

CNIL tarafından, veri ihlallerinin mağdurlarına yönelik olarak dikkatli olunması, parola güncellenmesi ve çok faktörlü kimlik doğrulamanın kullanılması gibi önlemlerin alınması gerektiği belirtilmiştir. Özellikle IBAN hırsızlığı, kimlik hırsızlığı, SIM kart dolandırıcılığı ve oltalama saldırıları gibi yöntemlerle kişisel bilgilerin kötüye kullanılabileceği ifade edilmiştir.

Ayrıca, veri ihlali yaşayan kuruluşların, ihlali CNIL'e bildirme ve etkilenen kişileri bilgilendirme yükümlülüğünün bulunduğu, CNIL'in de bu kuruluşlara ihlalin etkilerini azaltma ve siber güvenlik duruşlarını geliştirme konusunda rehberlik sağlayacağı belirtilmiştir.

CNIL'in 2024 yılı verilerine göre, 5629 veri ihlali bildirimi alındığı, bunun 2023 yılına kıyasla %20 artış anlamına geldiği; ayrıca 87 yaptırım kararından 12'sinin veri güvenliği eksikliğine ilişkin olduğu ifade edilmiştir.

İlgili metne buradan ulaşabilirsiniz.

Birleşik Krallık Veri Koruma Otoritesi ("ICO"), kamuya açıklanacak veya kişilere iletilecek belgelerde yer alan gizli kişisel bilgilerin istemsiz şekilde ifşa edilmesi riskinin en aza indirilmesine yardımcı olmak üzere bir rehber yayımladı.

ICO tarafından, kamuya açıklanacak veya kişilerle paylaşılacak belgelerde yer alan gizli kişisel bilgilerin istemsiz biçimde ifşa edilmesi riskini azaltmaya yönelik bir rehber yayımlandığı belirtilmiştir. Rehberin, belge paylaşım süreçlerinin güvenli şekilde yürütülmesine yardımcı olmak amacıyla kontrol listeleri ve uygulamalı "nasıl yapılır" videolarına erişim bağlantıları içerdiği ifade edilmiştir.

Rehber kapsamında; açıklanacak belgelerde uygun formatın seçilmesi, gizli satır, sütun, meta veri ve filtrelerin tespit edilmesi, verilerin basit formatlara dönüştürülürken gizli bilgilerin açığa çıkmamasının sağlanması, ve veri güvenliği açısından etkisiz yöntemlerin kullanılmaktan kaçınılması gerektiği vurgulanmıştır.

Ayrıca, gizli bilgilerin tespiti için özel yazılım araçlarının kullanılması, benzer ihlallerin tekrarının önlenmesi için süreçlerin gözden geçirilmesi ve kişisel bilgilerin etkili biçimde çıkarılması veya uygun yöntemlerle karartılması gerektiği belirtilmiştir.

İlgili rehbere buradan ulaşabilirsiniz.

ABD Ulusal Standartlar ve Teknoloji Enstitüsü ("NIST"), dijital kimliğe ilişkin güncellenmiş yönergeleri (NIST SP 800-63-4) yayımladı.

NIST tarafından hazırlanan yeni rehberde, kamu bilgi sistemleriyle ağlar üzerinden etkileşime giren kullanıcıların (örneğin çalışanlar, yükleniciler veya bireyler) kimlik doğrulama, kimlik kanıtlama ve federasyon süreçlerine ilişkin teknik gerekliliklerin belirlendiği belirtilmiştir.

Rehberde; kimlik kanıtlama, kayıt süreçleri, kimlik doğrulayıcılar, yönetim prosedürleri, kimlik doğrulama protokolleri, federasyon ve buna ilişkin beyanlara dair teknik gereksinimlerin tanımlandığı ve bu alanlarda uygulamaya yönelik teknik tavsiyelerin sunulduğu ifade edilmiştir. Ayrıca, belgenin bu amaç dışında kalan standartların geliştirilmesini kısıtlamayı hedeflemediği, ancak kamu kurumlarında güvenli dijital kimlik doğrulama altyapısının güçlendirilmesine katkı sağlayacağı belirtilmiştir.

Yeni rehberin, önceki NIST Special Publication (SP) 800-63-3 dokümanının yerini alacağı ifade edilmiştir.

İlgili yönergeye buradan ulaşabilirsiniz.

Birleşik Krallık Hukuk Komisyonu, yapay zekâ ve hukuk üzerine bir çalışma belgesi yayımladı.

İngiltere Hukuk Komisyonu tarafından, yapay zekâya ilişkin hukuki meseleler hakkında farkındalığı artırmak, konunun kapsamlı biçimde tartışılmasını sağlamak ve hukuk reformuna ihtiyaç duyulan alanların belirlenmesine zemin hazırlamak amacıyla bir tartışma belgesi yayımlandığı belirtilmiştir.

Belgede, yapay zekânın ne olduğu ve nasıl işlediğinin açıklanacağı, ayrıca özel hukuk, kamu hukuku ve ceza hukuku alanlarında doğurabileceği hukuki meselelerin "yapay zekânın özerkliği ve uyarlanabilirliği", "yapay zekâ ile etkileşim ve bağımlılık" ile "yapay zekâ eğitimi ve veri kullanımı" başlıkları altında ele alınacağı ifade edilmiştir. Söz konusu belgenin, herhangi bir yasa reformu önerisi içermediği, ancak ileride yapılacak düzenlemelere yön verecek bir farkındalık adımı olarak hazırlandığı belirtilmiştir.

Komisyonun, daha önce otonom araçlar ve yapay zekâ destekli "deepfake" görüntüler gibi alanlarda çalışmalar yürüttüğü; ayrıca havacılıkta otonomi ve ürün sorumluluğu konularında devam eden projelerinin bulunduğu ifade edilmiştir. Yapay zekânın toplumsal yaşam üzerindeki etkilerinin hızla artmaya devam edeceği ve bu nedenle İngiltere ve Galler hukuk sisteminin bu gelişmelere uyum sağlayacak biçimde evrilmesinin gerekeceği vurgulanmıştır.

Hukuk Komisyonu Başkanı Sir Peter Fraser tarafından yapılan açıklamada, belgenin amacının yapay zekânın hukuk üzerindeki etkilerine dair farkındalığı artırmak ve gerekli görülmesi hâlinde gelecekteki hukuk reformlarına temel oluşturmak olduğu belirtilmiştir.

İlgili belgeye buradan ulaşabilirsiniz.

Kaliforniya Yargı Konseyi, yargısal faaliyetlerde üretken yapay zekânın kullanımına yönelik kural ve standartları kabul etti.

Yeni düzenleme ile, üretken yapay zekâ kullanımını yasaklamayan tüm mahkemelerin, 15 Aralık 2025 tarihine kadar bu konuda bir politika benimsemekle yükümlü olacağı belirtilmiştir. Bu yükümlülüğün, ilk derece, temyiz ve Yüksek Mahkeme dâhil olmak üzere tüm yargı mercileri için geçerli olacağı ifade edilmiştir.

Benimsenecek politikalarda, gizliliğin korunacağı, ayrımcılığın önleneceği, çıktıların doğruluğunun teyit edileceği, önyargı ve zararlı içeriklerin giderileceği, yapay zekâ kullanımının kamuya açıklanacağı ve etik kurallara tam uyum sağlanacağı belirtilmiştir.

İlgili rapora buradan ulaşabilirsiniz.

Avrupa Komisyonu, genel amaçlı yapay zekâ uygulama kurallarını imzalayanların listesini yayımladı ve bu listenin sürekli bir şekilde güncellenmeye devam edileceğini duyurdu.

Genel Amaçlı Yapay Zekâ Uygulama Kuralları, AI Act kapsamında genel amaçlı yapay zekâ modelleri sağlayıcılarının güvenlik, şeffaflık ve telif hakkı yükümlülüklerine uyum sağlamalarına yardımcı olacak gönüllü bir araç olarak tasarlandığı belirtilmiştir. Söz konusu dokümanın, bağımsız uzmanlar tarafından çok paydaşlı bir süreçle hazırlandığı ve 10 Temmuz 2025 tarihinde yayımlandığı ifade edilmiştir.

Uygulama Kurallarının, Komisyon tarafından yayımlanan genel amaçlı yapay zekâ kavramlarına ilişkin kılavuzları tamamlayacağı ve Komisyon ile Yapay Zekâ Kurulu tarafından AI Act'e uyumu göstermek için uygun bir gönüllü araç olarak değerlendirildiği belirtilmiştir. Kuralların onaylanmasının ardından, belgeyi gönüllü olarak imzalayan model sağlayıcılarının, AI Act yükümlülüklerine uyumlarını bu kurallar aracılığıyla gösterebilecekleri, bu sayede idari yüklerinin azalacağı ve hukuki belirliliklerinin artacağı ifade edilmiştir.

Uygulama Kurallarının üç bölümden oluştuğu, bunların "Şeffaflık", "Telif Hakkı" ve "Güvenlik & Emniyet" başlıklarını içerdiği belirtilmiştir. Şeffaflık ve Telif Hakkı bölümlerinin, AI Act'in 53. maddesi kapsamındaki yükümlülüklerin yerine getirilmesine yardımcı olacağı; Güvenlik ve Emniyet bölümünün ise yalnızca AI Act'in 55. maddesi uyarınca sistemik risk taşıyan ileri düzey modeller için geçerli olacağı ifade edilmiştir.

İlgili duyuruya buradan ulaşabilirsiniz.

ICO, yasal düzenlemelerin çerezler veya takip pikselleri gibi depolama ve erişim teknolojilerine uygulanmasına ilişkin olarak yaygın şekilde karşılaşılan yanlış anlaşılmaların giderilmesine yönelik bir içerik yayımladı.

ICO tarafından, çerezler ve benzeri izleme teknolojilerine ilişkin güncellenmiş rehberin yayımlandığı ve bu kapsamda işletmelere hukuki belirlilik ve sorumlu yenilik imkânı sağlayacak yeni bir uygulama yaklaşımının tanıtıldığı belirtilmiştir.

Rehberde, PECR kurallarının yalnızca kişisel verileri değil, cihazlarda depolanan tüm bilgileri kapsayacağı, "kesinlikle gerekli" istisnasının yalnızca kullanıcının talep ettiği hizmetin sağlanmasıyla sınırlı olacağı ve rızaya dayalı veri işleme sonrası meşru menfaat gerekçesine geçilemeyeceği ifade edilmiştir.

ICO'nun amacının, takip teknolojilerinin gizlilik dostu, şeffaf ve kullanıcıya kontrol imkânı tanıyacak şekilde kullanılmasını sağlamak olduğu belirtilmiştir.

İlgili içeriğe buradan ulaşabilirsiniz.

EDPB, DSA ile GDPR arasındaki etkileşime ilişkin bir rehber yayımladı.

EDPB tarafından, Dijital Hizmetler Yasası DSA ile GDPR arasındaki etkileşimi açıklığa kavuşturmak amacıyla yeni kılavuzların yayımlandığı belirtilmiştir.

Kılavuzların, DSA kapsamında çevrim içi aracı hizmet sağlayıcıları tarafından gerçekleştirilen kişisel veri işleme faaliyetlerinin GDPR hükümleriyle uyumlu şekilde uygulanmasını sağlamayı amaçladığı ifade edilmiştir. Bu çerçevede, yasadışı içerik bildirimi sistemleri, öneri algoritmaları, çocukların gizliliği ve reklam güvenliği, reklam şeffaflığı ve özel nitelikli verilere dayalı reklamların yasaklanması gibi düzenlemelerin GDPR hükümleriyle kesiştiği alanların ele alındığı belirtilmiştir.

EDPB'nin, yetkili otoriteler arasında iş birliği ve koordinasyonun güçlendirilmesine yönelik pratik rehberlik sağlayacağı ve böylece hizmet sağlayıcılara hukuki belirlilik kazandırılacağı ifade edilmiştir.

Kılavuzların, paydaşların görüş ve önerilerini sunabilmeleri amacıyla kamu istişaresine açılacağı, ayrıca EDPB'nin benzer şekilde DSA ve AI Act ile GDPR arasındaki ilişkiye dair ortak kılavuzlar üzerinde çalışmaya devam edeceği belirtilmiştir.

İlgili rehbere buradan ulaşabilirsiniz.

İtalya, DSA'yı tamamlayıcı nitelikte ulusal bir yasayı onaylayan ilk AB üyesi ülke oldu.

İtalya Senatosu tarafından 17 Eylül 2025 tarihinde onaylanan ulusal yapay zekâ yasasıyla, ülkenin AI Act tamamlayıcı nitelikte bir düzenlemeyi yürürlüğe koyan ilk AB üyesi ülke olduğu belirtilmiştir.

Yasanın, yapay zekâ teknolojilerinin çalışma, sağlık ve adalet gibi alanlarda kullanımını düzenleyeceği, reşit olmayanların korunmasına yönelik hükümler getireceği ve yapay zekâ kaynaklı zararlara ilişkin cezai yaptırımlar öngöreceği ifade edilmiştir.

Yeni yasanın, veri işleme, güvenlik ve denetim alanlarında sorumlulukları paylaşacak ulusal otoriteler oluşturacağı, bu kapsamda Dijital İtalya Ajansı (AgID) ile Ulusal Siber Güvenlik Ajansı'nın (ACN) yetkili otoriteler olarak belirleneceği belirtilmiştir.

Ayrıca, yapay zekâ sistemlerinin AB dışındaki sunucularda barındırılabileceği, ancak kamu kurumlarının stratejik verilerin İtalya'daki veri merkezlerinde işlenmesine öncelik vereceği düzenlenmiştir.

Sağlık alanında, bilimsel araştırmalarda kişisel verilerin ikincil kullanımına izin verileceği ve ikincil rıza aranmaksızın anonimleştirilmiş sağlık verilerinin araştırma amacıyla yeniden kullanılabileceği ifade edilmiştir.

Yasa kapsamında, 14 yaş altı çocuklara ait kişisel verilerin yalnızca ebeveyn onayıyla işlenebileceği ve yapay zekâ ile oluşturulmuş sahte görsellerin paylaşılması hâlinde hapis cezası uygulanacağı belirtilmiştir.

İlgili metne buradan ulaşabilirsiniz.

Singapur Adalet Bakanlığı, hukukçular için üretken yapay zeka kullanımıyla ilgili taslak bir rehber yayımladı.

Singapur Adalet Bakanlığı tarafından hukuk sektöründe üretken yapay zekânın güvenli, etik ve sorumlu kullanımını teşvik etmek amacıyla hazırlanan taslak rehbere ilişkin kamuoyu görüşü alınacağı belirtilmiştir.

1–30 Eylül 2025 tarihleri arasında yürütülecek istişare süreci kapsamında yayımlanan rehber ile, hukuk profesyonellerinin yapay zekâ araçlarını mesleki sorumluluklarla uyumlu şekilde kullanmalarının hedeflendiği düzenlenmiştir. Rehber kapsamında, yapay zekâ kullanımında mesleki etik, gizlilik ve şeffaflık ilkelerinin korunmasının esas olduğu, hukukçuların yapay zekâdan yararlanırken müvekkil verilerini korumak, doğru bilgilendirme yapmak ve nihai sorumluluklarını yerine getirmekle yükümlü oldukları hükme bağlanmıştır. Ayrıca, Rehber'de yapay zekâ benimseme sürecine ilişkin olarak ihtiyaç analizi, araç seçimi, uygulama, eğitim ve sürekli iyileştirme aşamalarını içeren adım adım bir yol haritası öngörülmüştür. Bu kapsamda, rehberin hukuk sektörünün dijital dönüşüm sürecinde etik standartların korunmasına katkı sağlamasının amaçlandığı belirtilmiştir.

İlgili rehbere buradan ulaşabilirsiniz.

GÜNCEL KARARLAR

Avrupa Birliği Adalet Divanı ("ABAD") C-413/23 sayılı kararında, psödönim verilerin üçüncü taraflara aktarılması bağlamında "kişisel veri" kavramının kapsamına açıklık getirdi.

ABAD tarafından, psödönim verilerin üçüncü taraflara aktarımı bağlamında "kişisel veri" kavramının kapsamına ilişkin önemli bir karar verildiği belirtilmiştir.

Karar, Banco Popular Español'un tasfiyesi sürecinde, Tek Tasfiye Kurulu'nun ("**SRB**") hissedar ve alacaklıların görüşlerini psödönim biçimde Deloitte'a aktarması üzerine yapılan şikâyetlere ilişkindir. EDPS, SRB'yi bilgilendirme yükümlülüğünü ihlal ettiği yönündeki kararının, Genel Mahkeme tarafından kısmen iptal edilmesi üzerine, konu ABAD önüne taşınmıştır.

ABAD, Genel Mahkemenin hatalı hukuki değerlendirmede bulunduğunu, kişisel görüşlerin bireyin düşüncesini yansıttığı için doğası gereği kişisel veri olarak kabul edilmesi gerektiğini ve veri öznesinin tanımlanabilirliğinin, verinin toplandığı anda ve veri sorumlusunun bakış açısından değerlendirilmesi gerektiğini belirtmiştir.

Ayrıca, psödönim verilerin her durumda kişisel veri olarak değerlendirilemeyeceği, bunun somut olayın koşullarına ve veriyi işleyen kişinin veri öznesini tanımlama imkânına sahip olup olmamasına bağlı olarak değişeceği ifade edilmiştir.

Sonuç olarak, SRB'nin bilgilendirme yükümlülüğünün, veriler üçüncü bir tarafa aktarılmadan önce ve bu verilerin Deloitte açısından kişisel veri sayılıp sayılmadığından bağımsız olarak geçerli olacağı belirtilmiştir.

İlgili karara buradan ulaşabilirsiniz.

Avusturya Federal İdare Mahkemesi, Der Standard gazetesinin internet sitesinde uyguladığı "öde veya rıza göster" modelinin GDPR'ye aykırılık teşkil ettiğine karar verdi.

Avusturya Federal İdare Mahkemesi tarafından, Der Standard gazetesinin internet sitesinde uyguladığı "Öde ya da Kabul Et" modelinin GDPR'ye aykırı olduğuna karar verildiği belirtilmiştir.

Bu model kapsamında, kullanıcıların ya aylık 9,90 Euro ödeyerek siteye reklamsız erişim sağlayacakları ya da hedefli reklam amacıyla kişisel verilerinin işlenmesine onay vermek zorunda kalacakları ifade edilmiştir. Mahkeme, uygulamanın yalnızca genel bir onay veya reddetme seçeneği sunduğu için GDPR'de öngörülen "özgür iradeye dayalı açık rıza" ilkesini ihlal ettiğini belirtmiştir.

Gazete, bölünmüş rıza sisteminin bu modelde teknik olarak uygulanamayacağını ileri sürmüş olsa da, mahkeme Avusturya Veri Koruma Kurumu'nun 2023 tarihli kararını onaylayarak uygulamanın AB veri koruma kurallarına uygun olmadığını hükme bağlamıştır.

Kararın, Avusturya Yüksek İdare Mahkemesi'ne ve büyük olasılıkla Avrupa Birliği Adalet Divanı'na taşınacağı belirtilmiştir.

Benzer bir kararda, Avrupa Komisyonu'nun Nisan 2025'te Meta'ya, Dijital Piyasalar Yasası'nı ihlal eden "Öde ya da Kabul Et" modelinden dolayı 200 milyon Euro idari para cezası uyguladığı ifade edilmiştir.

İlgili karara ilişkin habere buradan ulaşabilirsiniz.

CNIL, La Samaritaine mağazasında çalışanların gizli şekilde izlenmesi nedeniyle Samaritaine SAS'a 100.000 Euro tutarında idari para cezası uygulanmasına karar vermiştir.

CNIL, La Samaritaine mağazasının işletmecisi Samaritaine SAS'a, çalışanların görüntü ve seslerini gizli şekilde kaydeden "duman dedektörü görünümlü kameralar" nedeniyle 100.000 Euro para cezası verdi. Otorite, bu uygulamanın çalışanların makul şekilde beklemeyeceği gizli izleme niteliğinde olduğunu, ses kaydı alınmasının veri minimizasyonu ilkesini ihlal ettiğini, ayrıca veri ihlali (SD kartların çalınması) konusunda zamanında bildirim yapılmadığını ve Veri Koruma Görevlisi'nin sürece dahil edilmediğini tespit etti.

İlgili karara buradan ulaşabilirsiniz.

İspanya Veri Koruma Otoritesi ("AEPD"), kişisel verilerin korunmasına yönelik teknik ve organizasyonel önlemleri yeterli şekilde uygulamaması ve veri işleme sözleşmesinin GDPR'ye uygun olmaması nedeniyle Sociedad De Gestión De Activos Procedentes De La Reestructuración Bancaria, S.A. (Sareb) adlı şirkete 180.000 Euro tutarında idari para cezası uygulanmasına karar vermiştir.

AEPD, bir danışmanlık şirketinde yaşanan veri ihlali sonucunda yaklaşık 360 çalışanın kimlik bilgilerinin yetkisiz erişime maruz kalması üzerine başlattığı incelemede, Sareb'in veri sorumlusu sıfatıyla GDPR'nin 5(1)(f) ve 28. maddelerini ihlal ettiğini tespit etmiştir. Otorite, şirketin veri güvenliği önlemlerinin yetersiz olduğunu, veri işleme sözleşmesinde saklama süresi gibi zorunlu unsurların yer almadığını ve yükleniciye ilişkin güvenlik önlemlerinin somut biçimde tanımlanmadığını belirlemiştir. Başlangıçta 300.000 Euro olarak belirlenen para cezası, şirketin sorumluluğunu kabul etmesi ve gönüllü ödeme indiriminden yararlanmasıyla 180.000 Euro olarak kesinleşmiştir.

İlgili karara buradan ulaşabilirsiniz.

CNIL, Gmail hizmetinde kullanıcı rızası olmaksızın tanıtım e-postaları gösterilmesi ve reklam çerezlerine ilişkin geçersiz rıza mekanizması nedeniyle Google LLC'ye 200 milyon Euro, Google Ireland Limited'e ise 125 milyon Euro olmak üzere toplam 325 milyon Euro tutarında idari para cezası uygulanmasına karar vermiştir.

CNIL, yapılan şikayet üzerine başlattığı incelemede, Google tarafından Gmail kullanıcılarına "Tanıtımlar" sekmesinde gösterilen tanıtım e-postalarının, önceden alınmış açık rıza bulunmaksızın doğrudan pazarlama iletişimi niteliğinde olduğunu tespit etmiştir. Ayrıca, Google hesap oluşturma sürecinde kişiselleştirilmiş reklam ve çerez tercihlerinin kabul edilmesinin reddedilmesine kıyasla çok daha kolay olması nedeniyle kullanıcı rızasının özgür iradeye dayanmadığı sonucuna varılmıştır. Bu nedenle CNIL, şirketlerin ePrivacy Direktifi'nin 5(3). maddesini ve Fransız Posta ve Elektronik Haberleşme Kanunu'nun L.34-5 maddesini ihlal ettiğine hükmetmiştir.

Otorite, Fransa'daki 74 milyondan fazla hesabın etkilendiğini, bunlardan 53 milyonunun izinsiz reklam gösterimine maruz kaldığını belirterek, Google'ın çevrimiçi reklamcılık pazarındaki hakim konumunu da dikkate almıştır. CNIL ayrıca, Google'a altı ay içinde kullanıcı rızası olmadan reklam göstermeyi sonlandırması ve geçerli rıza mekanizması kurması talimatını vermiş, aksi halde her gecikme günü için 100.000 Euro para cezası uygulanacağını hükme bağlamıştır.

İlgili karara buradan ulaşabilirsiniz.

AEPD, veri sahibinin erişim talebine yanıt vermemesi ve Kurum kararına uymaması nedeniyle TRIVE CREDIT SPAIN, S.L. adlı şirkete ceza uygulamıştır.

AEPD, bir veri sahibinin erişim talebine yanıt verilmediği gerekçesiyle yaptığı şikayet üzerine yürüttüğü incelemede, şirketin Kurum tarafından Mart 2024'te verilen "erişim talebine 10 iş günü içinde cevap verme" kararına uymadığını tespit etmiştir. Şirket, veri sahibinin taleplerinin kötüye kullanıldığını ve daha önce veri silme talebinin yerine getirildiğini savunsa da, Kurum bu savunmayı kabul etmemiştir. AEPD, şirketin GDPR'nin 58(2)(c) maddesini ihlal ettiğine, ayrıca hesap verebilirlik yükümlülüğü (madde 5(2)) kapsamında uyumu ispat etme sorumluluğunu da yerine getirmediğine hükmetmiştir. İhlalin süresinin uzunluğu ve Kurum kararına uyulmaması dikkate alınarak ceza önce 225.000 Euro olarak belirlenmiş, ancak şirketin gönüllü ödeme indiriminden yararlanmasıyla 180.000 Euro olarak kesinleşmiştir. Ayrıca, Kurum şirketin erişim talebine yanıt vermesini emretmiştir.

İlgili karara buradan ulaşabilirsiniz.

İtalya Veri Koruma Otoritesi (Garante), kimlik hırsızlığı sonucu üçüncü bir kişiye ait sahte erişim talepleri üzerine kişisel verileri yanlışlıkla ifşa etmesi ve veri ihlalini süresinde bildirmemesi nedeniyle Poste Vita S.p.A.'ya para cezası uygulanmasına karar vermiştir.

Garante, 2021–2023 yılları arasında bir kişinin veri sahibini taklit ederek şirketten bilgi talep etmesi üzerine, şirketin yeterli kimlik doğrulama prosedürü uygulamadan kişisel verileri üçüncü kişiye aktardığını tespit etmiştir. Bu durumun, veri sahibinin adil işlenme, bütünlük ve gizlilik ilkeleri kapsamında GDPR'nin 5(1)(a) ve 5(1)(f) maddelerinin ihlaline yol açtığı belirtilmiştir. Ayrıca, veri ihlalinin fark edilmesinden itibaren 72 saat içinde bildirim yapılması gerekirken, şirketin iç soruşturmanın tamamlanmasını bekleyerek gecikmeli bildirim yaptığı ve bu nedenle GDPR'nin 33. maddesini ihlal ettiği sonucuna varılmıştır. Otorite, şirketin sonradan kimlik doğrulama süreçlerini güçlendirmesini cezayı hafifletici unsur olarak değerlendirmiştir.

İlgili karara buradan ulaşabilirsiniz.

Belçika Veri Koruma Otoritesi (APD), öğrenci yurdunda yer alan güvenlik kameralarının hukuka aykırı biçimde kullanılması, gereksiz alanların görüntülenmesi ve gerekli teknik-idari önlemlerin alınmaması nedeniyle yurt sahibi kişiye para cezası uygulanmasına karar vermiştir.

APD, 8 odalı bir öğrenci yurdunda ortak mutfak, teras, bahçe ve bina girişi gibi alanlarda yer alan dört güvenlik kamerasının hukuka uygun bir işleme temeline dayanmadan kullanılmasını tespit etmiştir. Kurum, mülkün korunması amacının meşru kabul edilebileceğini, ancak bu amaca ulaşmak için daha az müdahaleci yöntemler bulunabileceğini belirterek GDPR'nin 5(1)(a) ve 6(1)(f) maddelerinin ihlal edildiğine hükmetmiştir. Ayrıca, kameralarla kamuya açık yolun ve komşu mülklerin bir kısmının da kayda alınması nedeniyle veri minimizasyonu ilkesinin (madde 5(1)(c)) ihlal edildiği; kameralarla yapılan işlemlere ilişkin kayıt tutulmaması sebebiyle de madde 30 kapsamında yükümlülüklerin yerine getirilmediği tespit edilmiştir. Veri sorumlusunun herhangi bir düzeltici veya hafifletici önlem almaması da cezayı artırıcı unsur olarak değerlendirilmiştir.

İlgili karara buradan ulaşabilirsiniz.

Polonya Veri Koruma Otoritesi (UODO), kimlik belgelerinin gereksiz ve ayrım yapılmaksızın taranması nedeniyle ING Bank Śląski S.A.'ya para cezası uygulanmasına karar vermiştir.

UODO'nun incelemesi sonucunda, bankanın 2019–2020 yılları arasında müşterilerinin ve potansiyel müşterilerinin kimlik belgelerini her durumda zorunlu olarak tarattığı, bu uygulamanın kara para aklama ve terörün finansmanı ile mücadele (AML) mevzuatına dayandırıldığı ancak bireysel risk değerlendirmesi yapılmadan gerçekleştirildiği tespit edilmiştir. Otorite, kimlik belgelerinin tamamının taranmasının kimlik doğrulama için gerekli olandan fazla veri içerdiğini belirleyerek veri minimizasyonu ve hukuka uygunluk ilkelerinin ihlal edildiğine hükmetmiştir. Bu kapsamda, bankanın GDPR'nin 5(1)(a), 5(1)(b), 5(1)(c) ve 6(1) maddelerini ihlal ettiği kabul edilmiş ve 18.416.400 PLN (yaklaşık 4,3 milyon Euro) tutarında idari para cezası uygulanmıştır. Ayrıca, kimlik belgelerinin özel nitelikli veri sayılmadığı ancak işlenmesinin yüksek risk taşıdığı vurgulanmıştır.

İlgili karara buradan ulaşabilirsiniz.

İtalya Veri Koruma Otoritesi (Garante), Venedik Belediyesi'nin turist vergisi muafiyet sisteminde kişisel verilerin gereksiz ve aşırı şekilde işlenmesi ile veri güvenliği açıkları nedeniyle para cezası uygulanmasına karar vermiştir.

Garante'nin re'sen başlattığı incelemede, Venedik Belediyesi'nin turist vergisinden muaf kişilerin (örneğin şehir sakinleri, öğrenciler, engelliler veya sağlık hizmeti alan kişiler) muafiyet durumunu doğrulamak için kullandığı üç aşamalı sistemin gereksiz veri toplama içerdiği tespit edilmiştir. Özellikle, ilk aşamada kişisel verilerin toplanarak QR kod oluşturulmasının sonraki aşamalarda kullanılmadığı, bu nedenle veri işleme amacına hizmet etmediği ve orantısız olduğu değerlendirilmiştir. Ayrıca, şehir genelinde bulunan ödeme kiosklarında tarayıcı ayarlarının değiştirilmesine ve önceden girilmiş kişisel verilerin diğer kullanıcılar tarafından görüntülenmesine imkân veren bir güvenlik açığı bulunduğu belirlenmiştir. Bu nedenlerle otorite, belediyenin GDPR'nin 5, 6, 25 ve 32. maddelerini ihlal ettiğine hükmetmiş ve 10.000 Euro tutarında idari para cezası uygulanmasına karar vermiştir.

İlgili karara buradan ulaşabilirsiniz.

Yunanistan Veri Koruma Otoritesi (HDPA), veri sahibinin erişim talebini yerine getirmemesi nedeniyle NN Hellas'a para cezası uygulanmasına karar vermiştir.

HDPA, bir sigorta müşterisinin "Dental Care NN Hellas" kapsamında yürütülen diş tedavisine ilişkin çağrı merkezi kayıtlarına erişim talebinin reddedilmesi üzerine yaptığı şikayet sonucunda, söz konusu çağrı merkezi kayıtlarının işlenmesinde NN Hellas'ın veri sorumlusu konumunda olduğuna hükmetmiştir. İnceleme sonucunda, NN Hellas'ın çağrı merkezinin işleyişine ilişkin açık talimatlar verdiği, kayıtların alınması, dosyalanması ve aylık raporlanması süreçlerini belirlediği, ayrıca tüm kişisel verilerin NN Hellas'a ait olduğunu sözleşmede düzenlediği tespit edilmiştir. Bu kapsamda, NN Hellas'ın veri sahibinin erişim talebini karşılamayarak GDPR'nin 15(1) ve 15(3) maddelerini ihlal ettiği belirtilmiş ve 20.000 Euro tutarında idari para cezası uygulanmıştır. Ayrıca, Mediadent'in Kurumun talep ve duruşma çağrılarına yanıt vermemesi nedeniyle GDPR'nin 31. maddesini ihlal ettiği değerlendirilmiş ve 2.000 Euro tutarında ek ceza uygulanmıştır.

İlgili karara buradan ulaşabilirsiniz.

AEPD, Real Sociedad de Fútbol kulübüne yönelik siber saldırı sonucu kişisel verilerin gizliliği ve bütünlüğünün ihlal edilmesi ve yeterli güvenlik önlemlerinin bulunmaması nedeniyle idari para cezası uygulanmasına karar vermiştir.

Kulübün sistemlerine yönelik fidye yazılımı saldırısı sonucunda 60.000 kişiye ait kimlik, iletişim, finansal, biyometrik ve sağlık verileri etkilenmiştir. AEPD, kulübün GDPR'nin 5(1)(f) ve 32. maddelerini ihlal ettiğini tespit etmiş ve toplam 110.000 Euro tutarındaki cezayı, kulübün gönüllü ödeme ve sorumluluk kabulü nedeniyle 66.000 Euro olarak kesinleştirmiştir. Kulübe ayrıca üç ay içinde uygun teknik ve idari güvenlik önlemleri alma yükümlülüğü getirilmiştir.

İlgili karara buradan ulaşabilirsiniz.

Hollanda Devlet Konseyi, ebeveynlerin erişim talebinin üçüncü kişilerin (yetişkin oğullarının) gizliliğini ihlal edeceği gerekçesiyle reddedilmesini hukuka uygun bulmuştur.

Almere Belediyesi, ebeveynlerin yetişkin oğullarına ait "Sosyal Destek Dosyası"ndaki kişisel verilerine erişim talebini, üçüncü kişilerin mahremiyetini koruma gerekçesiyle kısmen reddetmiştir. Konsey, GDPR Madde 15 uyarınca erişim hakkının mutlak olmadığını, veri sorumlusunun erişim talebi ile üçüncü kişilerin gizlilik haklarını menfaat dengesi çerçevesinde değerlendirmesi gerektiğini belirtmiştir. Ayrıca, davanın makul sürede sonuçlanmaması nedeniyle Avrupa İnsan Hakları Sözleşmesi'nin 6. maddesinin ihlal edildiği tespit edilmiş ve toplam 2.500 Euro tazminat ödenmesine hükmedilmiştir.

İlgili karara buradan ulaşabilirsiniz.

İrlanda Yüksek Mahkemesi, veri ihlali nedeniyle yaşanan stres ve endişe gibi manevi zararların "kişisel yaralanma" kapsamında değerlendirilemeyeceğine ve Kişisel Zararlar Değerlendirme Kurulu ("PIAB") onayına tabi olmadığına karar vermiştir.

Bir sigorta şirketi, poliçe sahibine ait kişisel ve mali bilgileri içeren bazı mektupları 2008–2020 yılları arasında yanlışlıkla üçüncü kişilere göndermiştir. Veri sahibi, bu durumun kendisine stres, kaygı ve rahatsızlık verdiğini ileri sürerek GDPR ve İrlanda Veri Koruma Yasaları uyarınca tazminat talebiyle dava açmıştır.

Yüksek Mahkeme, alt mahkemelerin aksine, bu tür manevi zararların "tıbben tanınan psikiyatrik bir rahatsızlık" oluşturmadığı sürece PIAB onayı gerektirmediğine hükmetmiştir.

İlgili karara buradan ulaşabilirsiniz.