

Kişisel Verilerin Korunması Bülteni

2026

Birinci Çeyrek

Av. Sevgi Ünsal Özden
Av. Ozan Akman
Av. Gülnur Çakmak Ergene
Av. Elvan Galatalı
Stj. Av. Pelin Mutlu

Türkiye'den Güncel Gelişmeler

Kişisel Verileri Koruma Kurumu, Kamu Kurumlarında Yurt Dışı Menşeli Haberleşme Uygulamaları Kullanımına İlişkin Kamuoyu Duyurusu Yayımladı

Kişisel Verileri Koruma Kurumu (Kurum), Kamu Kurumlarında Yurt Dışı Menşeli Haberleşme Uygulamaları Kullanımına İlişkin Kamuoyu Duyurusu'nda, son dönemde kendisine iletilen ihbar ve başvurulara ilişkin değerlendirmelerini açıkladı. Şikâyetlerde, kamu personelinin idarî iş ve işlemler kapsamında WhatsApp uygulamasını kullanmaya zorlandığı, bu uygulama üzerinden emir ve talimat verildiği ve resmî belge paylaşımı yapıldığı belirtildi.

Kurum, 2019/12 sayılı Cumhurbaşkanlığı Genelgesi'ne atıfla, mobil uygulamalar aracılığıyla gizlilik dereceli veri paylaşımaması ve yerli haberleşme uygulamalarının tercih edilmesi gerektiğini ifade etti. Bu kapsamda, WhatsApp gibi yurt içinde veri merkezi bulunmayan uygulamalar üzerinden gizlilik dereceli ya da kritik ni-

telikteki resmî evrak paylaşımaması gerektiğini vurguladı.

Ayrıca Kurum, bu tür uygulamalar üzerinden kişisel veri içeren paylaşımların, kamu personelinin cep telefonu numaraları da dahil olmak üzere, "kişisel veri işleme faaliyeti" niteliği taşıdığını ve 6698 sayılı Kişisel Verilerin Korunması Kanunu'nun (KVKK) 5 ve 6. maddelerindeki işleme şartlarını karşılamayan faaliyetlerin şikâyet üzerine ya da resen inceleme konusu yapılabileceğini de belirtti. Ayrıca, sorumluluğu tespit edilen kamu personeline disiplin hükümleri çerçevesinde yaptırım uygulanabileceğini de hatırlattı.

Kurum tarafından yayımlanan duyuruya [buradan](#) ulaşabilirsiniz.

Kişisel Verileri Koruma Kurumu, "QR Kodlarla Gelen Risk: 'Quishing'" Başlıklı Bir Duyuru Yayımladı

Kurum, 26.02.2026 tarihinde yayımladığı duyuruda QR kodlar üzerinden gerçekleştirilen ortalama saldırılarına (quishing) karşı uyarıda bulundu.

Duyuruda; sahte veya sonradan değiştirilmiş QR kodlar aracılığıyla kişilerin zararlı sitelere yönlendirilebildiği, kişisel verilerinin ele geçirilebildiği veya cihazlarına kötü amaçlı yazılım yüklenebildiği belirtildi. Özellikle dinamik QR kodların yönlendirme adresinin sonradan değiştirilebilmesi nedeniyle risk taşıdığı vurgulandı.

Kurum; bilinmeyen kaynaklardan gelen, aciliyet içeren QR kodlara karşı dikkatli olunması, yönlendirilen bağlantının kontrol edilmesi, cihaz güvenliğinin güncel tutulması ve çok faktörlü kimlik doğrulama gibi önlemlerin alınması gerektiğini ifade etti.

Kurum'un yayımladığı duyuruya [buradan](#), bu konudaki duyurumuza [buradan](#) ulaşabilirsiniz.

Sadakat Kartlarının Üçüncü Kişilerce Kullanımına İlişkin İlke Kararı Yayımlandı

Kişisel Verileri Koruma Kurulu (Kurul), sadakat kart sahibine ait cep telefonu numarasının veya kart numarasının üçüncü bir kişi tarafından alışveriş sırasında kullanılması konusunda 11.02.2026 tarihli ve 2026/266 sayılı İlke Kararı'nı yayımladı.

Kurul tarafından ilgili kişinin bilgisi ve rızası olmaksızın, herhangi bir doğrulama mekanizması işletilmeksizin sadakat kart üzerinden işlem yapılmasının KVKK m. 5 ile düzenlenen bir işleme şartına dayanmadığı; ilgili kişinin gerçekleştirmediği bir alışverişe ilişkin olarak adına fatura düzenlenmesi veya üyelik hesabına işlenmesinin, "doğru ve gerektiğinde güncel olma" ilkesine aykırılık riski doğurduğu belirtildi. Ayrıca, sözleşmede üçüncü kişilere kullandırmama hükmü bulursa dahi bunun veri sorumlusunun KVKK m. 12 kapsamındaki veri güvenliğini sağlama yükümlülüğünü ortadan kaldırmayaacağı vurgulandı.



Bu çerçevede; doğrulama yapılmaksızın sadakat kart üzerinden işlem yapılmasına imkân tanıyan uygulamaların sonlandırılmasına ve sadakat kart kullanımının ilgili kişinin bilgisi ve onayı dahilinde gerçekleştiğini teyit edecek uygun teknik ve idari tedbirlerin alınması gerektiğine karar verildi. Veri sorumlularına, İlke Kararı'nın Resmî Gazete'de yayımlanmasından itibaren 6 aylık uyum süresi tanındı.

İlke Karar'a [buradan](#) ve bu konudaki duyurumuza [buradan](#) ulaşabilirsiniz.

Neler Yapılabilir?

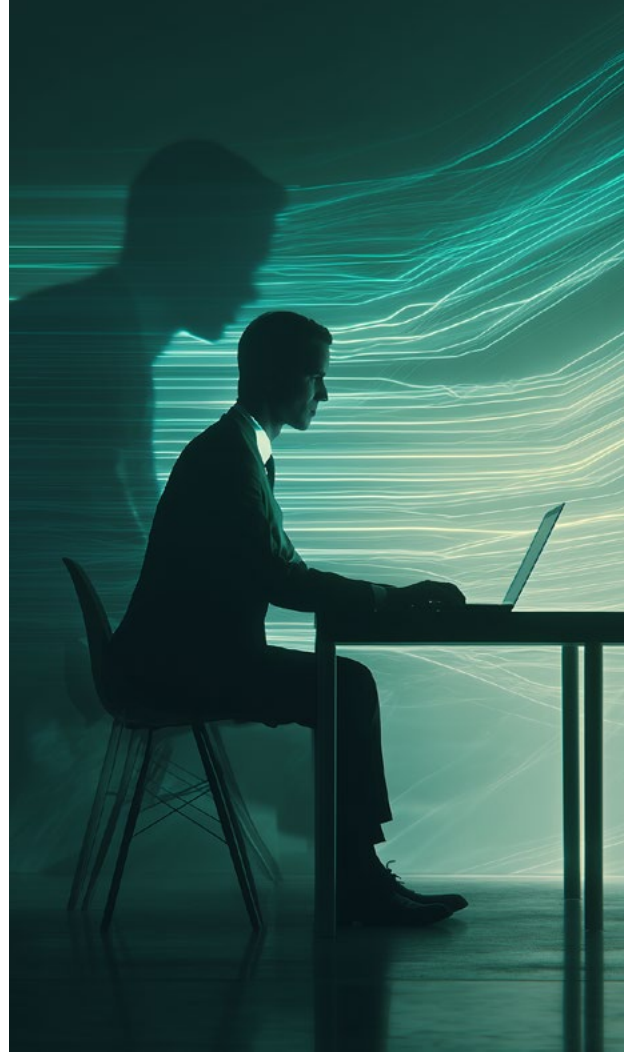
Sadakat kart programına sahip veri sorumluları tarafından; alışveriş sırasında SMS onayı, mobil uygulama doğrulaması, dinamik barkod/QR kod gibi kimlik doğrulama mekanizmaları, kişilerin yaş, eğitim düzeyi, ekonomik durumu, teknoloji okuryazarlığı gibi farklılıkları gözetilerek tesis edilmeli, işlem türü ve risk seviyesine göre kademeli doğrulama süreçleri oluşturulmalı ve üyelik sözleşmeleri, aydınlatma metinleri ve iç politika/prosedürler İlke Kararı doğrultusunda uyum süresi içerisinde revize edilmelidir.

Kurum, “İş Yerlerinde Üretken Yapay Zekâ Araçlarının Kullanımı” Başlıklı Bir Duyuru Yayımladı

Kurum, 05.03.2026 tarihinde, özellikle üçüncü taraflarca sunulan ve kamuya açık olarak erişilebilen üretken yapay zekâ araçlarının iş yerlerinde kullanımına ilişkin farkındalık yaratmak, olası riskleri ortaya koymak ve kurumlar açısından sorumlu kullanım yaklaşımlarına dikkat çekmek amacıyla “İş Yerlerinde Üretken Yapay Zekâ Araçlarının Kullanımı” başlıklı dokümanı yayımladı.

Dokümanda, üretken yapay zekâ araçlarının iş süreçlerinde verimlilik sağlamakla birlikte, özellikle kurumsal politika olmaksızın kullanılan “gölge yapay zekâ” uygulamaları bakımından kişisel verilerin korunması, bilgi güvenliği, fikri mülkiyet ve kurumsal itibar açısından çeşitli riskler doğurabileceği vurgulanmaktadır. Ayrıca veri sorumlularına bu risklerin minimize edilebilmesi için çeşitli öneriler sunulmaktadır.

Dokümana [buradan](#), bu konudaki duyurumuza [buradan](#) ve konuya ilişkin Exlibris makalemize [buradan](#) ulaşabilirsiniz.



Neler Yapılabilir?

Şirketlerde kullanılan yapay zekâ araçları bakımından; veri kullanımında mümkün olduğunca anonimleştirilmiş verilerin tercih edilmesi, açık ve uygulanabilir kurumsal politikaların oluşturulması, çalışanlara yönelik eğitim ve farkındalık çalışmalarının yürütülmesi, ayrıca yapay zekâ tarafından üretilen çıktılar üzerinde insan denetiminin sürdürülmesi önem taşımaktadır.

Kurum, “Etken Yapay Zekâ (Agentic AI)” Başlıklı Bir Doküman Yayımladı

Kurum, etken yapay zekâ sistemlerinin temel özellikleri, kullanılan yapay zekâ ajanları, potansiyel kullanım alanları ve kişisel veriler bakımından doğurabileceği riskleri ele alan “Etken Yapay Zekâ (Agentic AI)” başlıklı bir doküman yayımladı.

Dokümanda, etken yapay zekâ sistemleri; belirli hedeflere ulaşmak amacıyla çevresel koşulları değerlendirebilen, planlama yapabilen ve belirli ölçüde otonom şekilde hareket edebilen yapılar olarak tanımlanmakta; bu sistemlerin araştırma-geliştirme, müşteri hizmetleri, finansal analiz, sağlık ve olay müdahalesi gibi alanlarda kullanım potansiyeli bulunduğu belirtilmektedir.

Bununla birlikte, söz konusu sistemlerin çok adımlı ve hedef odaklı işleyişinin öngörülebilirlik, şeffaflık, açıklanabilirlik, veri minimizasyonu, amaçla sınırlılık ve veri güvenliği bakımından çeşitli riskler doğurabileceği ifade edilmektedir.

Bu nedenle etken yapay zekâ kullanımında insan gözetimi, açıklanabilirlik, veri doğruluğu, rol ve sorumlulukların açık şekilde belirlenmesi ile tasarımdan itibaren mahremiyet (privacy by design) yaklaşımının benimsenmesinin önem taşıdığı vurgulanmaktadır.

Dokümana [buradan](#) ve bu konudaki duyurumuza [buradan](#) ulaşabilirsiniz.

İş Ortaklığı, Konsorsiyum ve Adi Ortaklıklarda İşlenen Kişisel Verilerin VERBİS'e Bildirimi Hakkında Kamuoyu Duyurusu Yayımlandı

Kurum, iş ortaklığı, konsorsiyum ve adi ortaklık gibi yapılar nezdinde yürütülen faaliyetler kapsamında işlenen kişisel verilerin Veri Sorumluları Sicil Bilgi Sistemi'ne (VERBİS) bildirim bakımından uygulamada ortaya çıkan tereddütleri gidermek amacıyla bir kamuoyu duyurusu yayımladı.

Duyuruda, anılan yapıların ayrı bir tüzel kişiliğe sahip olmamaları nedeniyle VERBİS'e kendi adlarına kayıt yaptırmamaları gerektiği, kayıt yükümlülüğünün ise ortaklığı oluşturan taraflar bakımından ayrıca değerlendirilmesi gerektiği belirtildi.

Kurum'un yayımladığı duyuruya [buradan](#) ve bu konudaki duyurumuza [buradan](#) ulaşabilirsiniz.

Neler Yapılabilir?

İş ortaklığı, konsorsiyum ve adi ortaklık gibi yapılar bakımından, öncelikle ortakları oluşturan tarafların VERBİS'e kayıt yükümlülüğü bulunup bulunmadığı tespit edilmelidir. Kayıt yükümlülüğü bulunan tarafların ise VERBİS bildirimlerinde, kendi veri işleme faaliyetlerine ilave olarak ortaklık faaliyetleri kapsamında işlenen kişisel verilere de yer vermesi gerekmektedir.

Ceza Muhakemesi Kanunu'nda Yer Alan Genetik Verilere İlişkin Düzenlemeler Anayasa Mahkemesi Tarafından İptal Edildi

18.03.2026 tarihli ve 33200 sayılı Resmî Gazete'de yayımlanan Anayasa Mahkemesi'nin 25.12.2025 tarihli ve 2025/141 E., 2025/274 K. sayılı kararı ile, 5271 sayılı Ceza Muhakemesi Kanunu'nun genetik inceleme sonuçlarının saklanması ve imhasına ilişkin bazı hükümleri, kişisel verilerin korunmasına yönelik yeterli güvenceleri içermediği gerekçesiyle iptal edildi.

Kararda, genetik verilerin saklanma süresi, imha usulleri, veri sahiplerinin hakları ve başvuru yollarına ilişkin hususların

yönetmelik yerine kanun düzeyinde açıkça düzenlenmesi gerektiği belirtildi.

İptal kararının, Resmî Gazete'de yayımlanmasından itibaren dokuz ay sonra yürürlüğe girmesine karar verildi. Bu süre zarfında ilgili mevzuatın Anayasa'ya uygun şekilde yeniden düzenlenmesi beklenmektedir.

Karara [buradan](#) ve bu konudaki duyurumuza [buradan](#) ulaşabilirsiniz.

Açık Rıza ve Aydınlatma Metinlerinin Ayrı Düzenlenmesine İlişkin İlke Kararı Yayımlandı

Kurul'un 18.02.2026 tarihli ve 2026/347 sayılı "Veri Sorumluları Tarafından Açık Rıza ve Aydınlatma Metinlerinin Ayrı Ayrı Düzenlenmesi Gerektiği Hakkında İlke Kararı", 24.03.2026 tarihli ve 33203 sayılı Resmî Gazete'de yayımlandı.

Kararda, veri sorumlularının açık rıza ve aydınlatma yükümlülüklerini yerine getirirken uymaları gereken esaslar açıklanmaktadır. Ayrıca, veri sorumlularının açık rıza ve aydınlatma yükümlülüklerini yeri-

ne getirmelerine ilişkin iyi ve kötü uygulama örneklerine karar ekinde yer verilmektedir. Son olarak, bu hususlara uygun hareket edilmediğinin tespiti hâlinde ilgili veri sorumluları hakkında KVKK m. 18 hükümleri gereği işlem tesis edileceği de ifade edilmektedir.

Karara [buradan](#) ve bu konudaki duyurumuza [buradan](#) ulaşabilirsiniz.

Neler Yapılabilir?

Aydınlatma ve açık rıza metinleri, kararda ortaya konulan esaslar doğrultusunda gözden geçirilerek yeniden düzenlenmelidir. Bu kapsamda, aydınlatma ve açık rıza metinlerinin birbirinden ayrı hazırlanması, sade ve anlaşılır bir dil kullanılması, açık rıza gerektirmeyen hallerde ayrıca rıza talep edilmemesi ve kullanılan metinlerin her veri sorumlusunun kendi veri işleme faaliyetlerine özgü şekilde oluşturulması önem taşımaktadır.

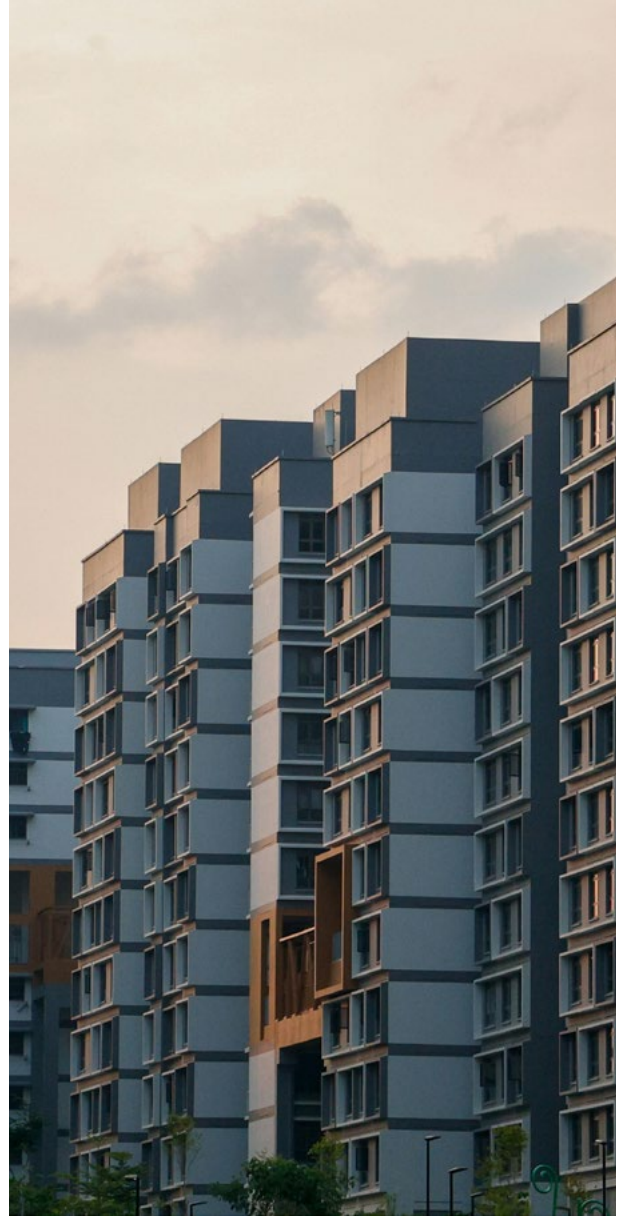
Toplu Yapılarda Kişisel Veri İçeren Borç Bilgilerinin Ortak Alanlarda Paylaşılmasına İlişkin İlke Kararı Yayınlandı

Kurul'un 18.02.2026 tarihli ve 2026/348 sayılı "Toplu Yapılarda Apartman/Site Sakinlerine Ait Borç Bilgilerinin Ortak Yerlere Asılması Hakkında İlke Kararı", 31.03.2026 tarihli ve 33210 sayılı Resmî Gazete'de yayımlandı.

Kararda, apartman ve site yönetim süreçlerinde aidat, avans ve benzeri borç bilgilerine ilişkin duyuruların ortak alanlarda ilan edilmesi, kişisel verilerin korunması hukuku bakımından değerlendirilmekte ve bu konuda uyulması gereken esaslar ortaya konulmaktadır.

Kurul, borç bilgilerine ilişkin bilgilendirmenin tamamen yasak olmadığını; ancak bu bilgilendirmenin, ölçülülük ilkesi ve veri güvenliği yükümlülüklerine uygun yöntemlerle yapılması gerektiğini, aksi takdirde bu uygulamanın hukuka aykırı bir kişisel veri işleme faaliyeti teşkil edeceğini belirtmektedir. Bu kapsamda; kapalı e-posta grupları, sınırlı erişimli mesajlaşma grupları veya yalnızca ilgili kişilerin erişebileceği dijital sistemler gibi daha güvenli yöntemlerin tercih edilmesi önerilmektedir.

Karara [buradan](#) ve bu konudaki duyurumuza [buradan](#) ulaşabilirsiniz.



Mobil Uygulamalar Üzerinden Gönderilen Anlık Bildirilere İlişkin Kamuoyu Duyurusu Yayınlandı

Kurum, mobil uygulamalar üzerinden gönderilen anlık bildirimlere ilişkin şikâyetler kapsamında yaptığı incelemeler sonucunda 14.01.2026 tarihinde bir kamuoyu duyurusu yayınladı. Duyuruda, mobil uygulama sağlayıcılarının veri sorumlusu sıfatıyla gerçekleştirdikleri veri işleme faaliyetlerinin KVKK'nın genel ilkeleri ve işleme şartlarına uygun olması gerektiği vurgulandı. Bu kapsamda, anlık bildirimlerin kullanıcıdan alınan izinlere dayandığı belirtildi.

Ayrıca Kurum, duyuruda incelediği somut bir olaya yer vererek, bir mobil uygulamanın yüklenme aşamasında kullanıcılara sunulan anlık bildirim onayı kapsamında ilgili kişilerden birden fazla kişisel veri işleme amacını aynı anda kapsayan tek bir rıza alındığını ve kullanıcıların hizmete erişebilmek için pazarlama bildirimlerini de kabul etmek zorunda bırakıldığını belirtti.

Bu kapsamda Kurul, ilgili veri sorumlusu tarafından sunulan onay mekanizmasında "kampanyalardan haberdar olmak" ve "sipariş durumunu anlık takip etmek" amaçlarının birleştirildiğini; bu itibarla, veri sahibi kullanıcıların, sipariş takibi gibi hizmetin doğal bir parçası olan operasyonel bildirimleri alabilmek için kampanya ve reklam içerikli bildirimleri kabul



etmek zorunda bırakıldığını ve bu durumun, açık rızanın özgür iradeyle verilmesi unsurunu zedeleyebileceği ifade edildi.

Bu itibarla, Kurul "parçalı açık rıza" ilkesine dikkat çekerek, her bir veri işleme amacı bakımından ayrı rıza alınması gerektiğini, birden fazla veri işleme amacının söz konusu olduğu durumlarda veri sahiplerine her bir veri işleme amacı için ayrı ve bağımsız bir seçim hakkı sunulmasının zorunlu olduğunu; ayrıca kullanıcılara bildirim tercihlerini yönetebilecekleri seçenekler sunulmasının önem taşıdığını vurgulamıştır. Bu kapsamda veri sorumlularına, rıza mekanizmalarını gözden geçirmeleri ve bildirim amaçlarını ayırtmalarını tavsiye edildi.

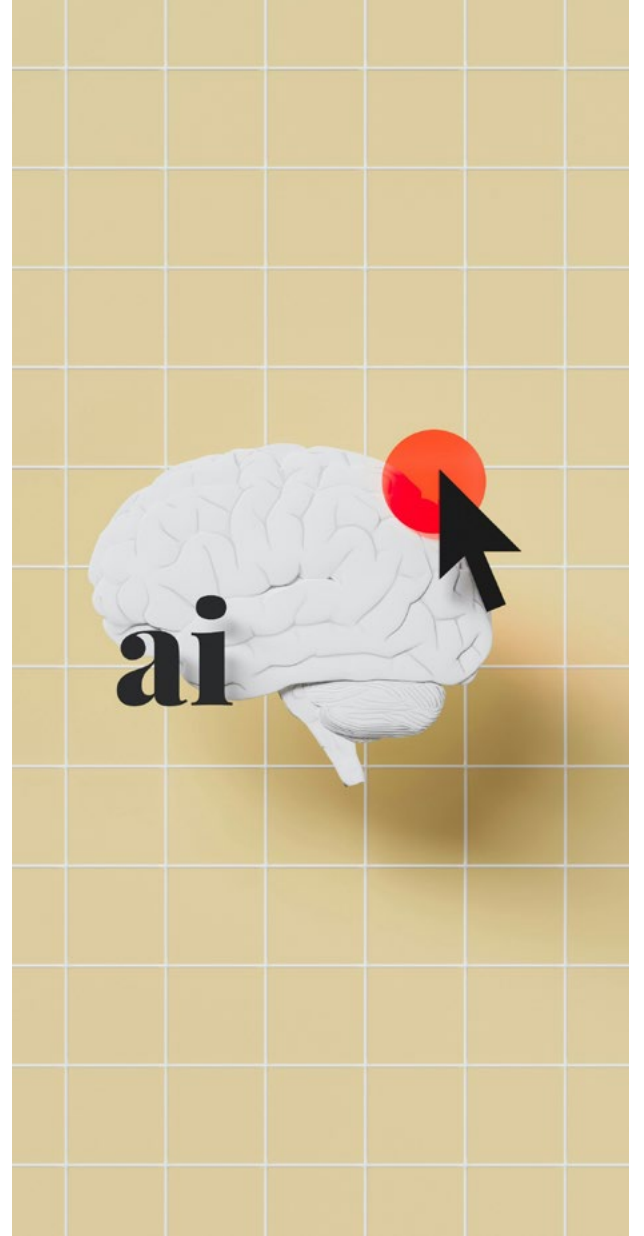
Kurum tarafından yayımlanan duyuruya [buradan](#) ve bu konudaki duyurumuza [buradan](#) ulaşabilirsiniz.

Dünya'dan Güncel Gelişmeler

Avrupa Konseyi İnsan Hakları ve Yapay Zekâ El Kitabı Yaymlandı

Avrupa Konseyi, İnsan Hakları Yönlendirme Komitesi (CDDH) tarafından Avrupa Konseyi üye devletleri için pratik bir referans aracı olarak geliştirilen İnsan Hakları ve Yapay Zekâ El Kitabı'nı yayımladı. El Kitabı, Avrupa İnsan Hakları Sözleşmesi (AİHS) ve Avrupa Sosyal Şartı'nda güvence altına alınan temel hak ve özgürlükler etrafında yapılandırılmış olup her bir hakkın yapay zekâ sistemlerinin tasarımı, geliştirilmesi ve kullanımından nasıl etkilenebileceğini ele almaktadır. Bu kapsamda; adil yargılanma hakkı, ifade özgürlüğü, mahremiyet hakkı, ayrımcılık yasağı ile sosyal ve ekonomik haklar gibi konular incelenmekte ve her bir alanda yapay zekâ kaynaklı risklere ilişkin somut örnekler sunulmaktadır.

El Kitabı ayrıca, Avrupa Konseyi Yapay Zekâ ve İnsan Hakları, Demokrasi ve Hukukun Üstünlüğü Çerçeve Sözleşmesi'ni (CETS No. 225) de dikkate almakta; politika yapıcılar ve kamu otoritelerinin yapay zekâ sistemlerine ilişkin insan hakları etki değerlendirmesi gerçekleştirmelerine yardımcı olmak üzere kontrol listeleri ve yol gösterici sorular gibi pratik araçlar içermektedir. Adalet, kolluk faaliyetleri, sağlık, eğitim ve istihdam gibi çeşitli alanlara yönelik sektöre özgü rehberlik sunulmakta; yapay zekâ sistemlerinin kamu veya özel sektör tarafından kullanılması fark etmeksizin, devletlerin şeffaflık, anlamlı insan gözetimi, hesap verebilirlik ve etkili başvuru yollarına erişimi güvence altına alma yönündeki yükümlülüklerine özellikle vurgu yapılmaktadır.



El Kitabı'nın İngilizce metnine [buradan](#) ulaşabilirsiniz.

OECD Sorumlu Yapay Zekâ İçin Durum Tespiti Rehberi Yayımladı

Ekonomik İşbirliği ve Kalkınma Teşkilatı (OECD), 2026 tarihli Sorumlu Yapay Zekâ İçin Durum Tespiti Rehberi'ni yayımladı. Söz konusu rehber, çok uluslu şirketlerin yapay zekâ kaynaklı riskleri sorumlu iş davranışı ilkeleri doğrultusunda yönetmelerine yönelik pratik bir çerçeve sunmaktadır. OECD Çok Uluslu Şirketler Rehberi temel alınarak hazırlanan rehber, sektör ve yapay zekâ sisteminden bağımsız, esnek bir yaklaşım benimsemektedir. Bu kapsamda, kuruluşların yapay zekâ sistemlerinin yaşam döngüsü boyunca ortaya çıkabilecek olumsuz etkileri tespit etmelerine, değerlendirmelerine ve ele almalarına yardımcı olmayı amaçlamaktadır.

Rehberde, altı aşamalı sürekli bir durum tespiti süreci öngörülmektedir. Bunlar; politika ve yönetim mekanizmalarının oluşturulması, risklerin belirlenmesi, olumsuz etkilerin giderilmesi, sonuçların izlenmesi, alınan önlemlerin raporlanması ve gerektiğinde telafi mekanizmalarının işletilmesidir. Rehberin, inovasyonu desteklediği, mevcut yönetim çerçeveleriyle uyum sağladığı ve farklı yapay zekâ risk yönetimi çerçeveleri arasında uyumlu bir uygulama yaklaşımının geliştirilmesini desteklediği ifade edilebilir.

OECD tarafından yayımlanan rehberin İngilizce metnine [buradan](#) ulaşabilirsiniz.

Birleşik Krallık Veri Koruma ve Gizlilik Mevzuatında Reformlar Yürürlüğe Girdi

Şubat 2026 itibarıyla Birleşik Krallık'ta, Data (Use and Access) Act 2025 (DUAA) kapsamında veri koruma alanında önemli reformlar yürürlüğe girdi. Söz konusu reformlar, AB veri koruma rejiminden belirli ölçüde ayrılmaya işaret etmektedir. Yapılan değişiklikler; çerez kullanımına ilişkin esneklik, otomatik karar alma süreçlerinin (ADM) güvencelerle genişletilmesi ve araştırma amaçlı veri işleme faaliyetlerine açıklık getirilmesi gibi alanlarda kolaylıklar sağlarken özellikle çocuk verilerinin korunması ve Information Commissioner's Office'in (ICO) denetim ve yaptırım yetkilerinin güçlendirilmesi suretiyle uyum yükümlülüklerini de artırmaktadır.

Başlıca yenilikler arasında; çerezler bakımından yeni istisnalar, veri sahibi başvurularında (DSAR) "süre durdurma" mekanizması, ADM'nin belirli güvencelerle genişletilmesi, ticari araştırmaları da kapsayan daha net araştırma tanımları ve meşru menfaatlere ilişkin belirli kategorilerin tanımlanarak denge testine olan ihtiyacın azaltılması yer almaktadır. Genel olarak reformlar, veri koruma çerçevesinin modernize edilmesini amaçlamakta olup, bir yandan uyum süreçlerinde esneklik sağlarken diğer yandan düzenleyici denetimin artmasına yol açmaktadır. Bu kapsamda, ICO tarafından ek rehberlerin yayımlanması beklenmektedir.

DUAA'nın İngilizce metnine [buradan](#) ulaşabilirsiniz.

Kritik Bilgi İletişim Teknolojileri Hizmet Sağlayıcılarının Sınır Ötesi Denetimine İlişkin AB-Birleşik Krallık Mutabakat Zaptı İmzalandı

2026 yılı ocak ayında, Avrupa Birliği (AB) ve Birleşik Krallık finansal düzenleyici otoriteleri, Dijital Operasyonel Dayanıklılık Tüzüğü (DORA) ve Birleşik Krallık kritik üçüncü taraf (CTP) rejimi kapsamında kritik bilgi ve iletişim teknolojisi üçüncü taraf hizmet sağlayıcılarının (CTPP) sınır ötesi denetimini güçlendirmek amacıyla bir Mutabakat Zaptı (Mutabakat) imzaladı. Mutabakat kapsamında; başta bulut bilişim hizmetleri, veri depolama ve veri merkezi altyapıları, ödeme sistemleri altyapıları, siber güvenlik çözümleri ve finansal yazılım hizmetleri sağlayan şirketler olmak üzere, finans sektörünün operasyonel sürekliliği bakımından kritik öneme sahip teknoloji sağlayıcıları hedef alınmaktadır. Söz konusu Mutabakat, düzenleyici otoriteler arasında sistematik bilgi paylaşımı, koordineli denetimler ve ortak gözetim faaliyetlerini içeren geliştirilmiş bir iş birliği çerçevesi oluştur-

makta; bu suretle denetim boşluklarının azaltılması ve operasyonel dayanıklılığın artırılmasını hedeflemektedir.

Mutabakat ayrıca, otoriteler arasındaki bilgi paylaşımının gizlilik yükümlülüklerine tabi olacağını, ancak hukuken gerekli hallerde paylaşılabilirliğini de açıklığa kavuşturmuştur. Bu gelişme; Amazon Web Services, Microsoft Azure, Google Cloud gibi kritik üçüncü taraf hizmet sağlayıcıları bakımından daha sıkı düzenleyici denetim, yargı alanları arasında daha entegre bir gözetim yaklaşımı ve AB ile Birleşik Krallık düzenleyici süreçleri arasında uyum, dokümantasyon ve kurum içi koordinasyonun güçlendirilmesi gerekliliği anlamına gelmektedir.

Duyurunun İngilizce metnine [buradan](#) ulaşabilirsiniz.

AB Adalet Divanı, EDPB Bağlayıcı Kararlarının Yargısal Denetimine İlişkin Emsal Niteliğinde Bir Karar Verdi

AB Adalet Divanı (CJEU), 10.02.2026 tarihinde şirketlerin Avrupa Veri Koruma Kurulu'nun (EDPB) bağlayıcı kararlarına karşı, yetkili denetim otoritesi tarafından nihai bir karar alınmadan önce dahi, Avrupa Birliği'nin İşleyişi Hakkında Antlaşma (ABİHA) m. 263 kapsamında AB mahkemeleri nezdinde iptal davası açabileceğini teyit eden emsal bir karar verdi.

Dava, İrlanda Veri Koruma Komisyonu'nun WhatsApp'ın şeffaflık yükümlülüklerine uyumuna ilişkin yürüttüğü inceleme kapsamında ortaya çıktı. Bu sürecin ardından EDPB, birden fazla Avrupa Birliği Genel Veri Koruma Tüzüğü (GDPR) ihlali tespit ederek 225 milyon avro tutarında idari para cezası uygulanmasını öngören bağlayıcı bir karar verdi. CJEU, söz konusu kararın ulusal denetim otoritelerine takdir yetkisi bırakmaksızın ilgili şirketler bakımından doğrudan bağlayıcı hukuki sonuçlar doğurduğunu tespit etti ve bu nitelikteki EDPB kararlarının AB mahkemeleri nezdinde doğrudan denetlenebilir işlemler olduğuna hükmetti.

Bu karar, EDPB'nin bağlayıcı kararlarının AB mahkemeleri önünde doğrudan denetlenebilmesinin önünü açmakta; EDPB kararlarına karşı AB yargısı nezdinde yürütülen süreçler ile ulusal uygulama kararlarına karşı ulusal mahkemeler nezdinde açılan davaların paralel veya kesişen biçimde ilerlemesi ihtimalini gündeme getirmektedir.



Kararın İngilizce metnine [buradan](#) ulaşabilirsiniz.

Avrupa Komisyonu, Yapay Zekâ Tarafından Üretilen İçeriklere İlişkin Davranış Kuralları Taslağını Güncelledi

Avrupa Komisyonu, 05.03.2026 tarihinde, AB Yapay Zekâ Tüzüğü'nün (Yapay Zekâ Tüzüğü) 50. maddesi kapsamında öngörülen şeffaflık yükümlülüklerine uyumu desteklemek amacıyla, yapay zekâ tarafından üretilen içeriklerin işaretlenmesi ve etiketlenmesine ilişkin Davranış Kuralları Taslağı'nın ikinci versiyonunu yayımladı. Güncellenen taslak, önceki versiyona kıyasla daha esnek ve uygulamaya yönelik bir yaklaşım benimsemekte; yapay zekâ sistemlerinin sağlayıcıları ve dağıtıcıları bakımından uyum süreçlerinin sadeleştirilmesini hedeflemektedir. Taslak, yapay zekâ tarafından üretilen veya manipüle edilen içeriklerin

işaretlenmesi ve etiketlenmesine ilişkin rehberlik sunmakta; özellikle "deepfake" içeriklerin ve belirli türde yapay zekâ üretimi içeriklerin açık şekilde etiketlenmesine yönelik gereklilikler öngörmektedir. 30.03.2026 tarihinde sona eren kamuoyu istişare sürecinin ardından, nihai versiyonun Haziran 2026'da yayımlanması beklenmektedir. Yapay Zekâ Tüzüğü kapsamındaki ilgili şeffaflık yükümlülüklerinin ise 02.08.2026 tarihinde uygulanmaya başlanması öngörülmektedir.

Avrupa Komisyonu tarafından yayımlanan taslağın İngilizce metnine [buradan](#) ulaşabilirsiniz.

AB Siber Dayanıklılık Tüzüğü Kapsamında Taslak Rehber Yayımlandı

Avrupa Komisyonu, 03.03.2026 tarihinde, AB Siber Dayanıklılık Tüzüğü'nün (CRA) uygulanmasına açıklık getirmek ve paydaşların uyum yükümlülüklerini daha iyi anlamalarını sağlamak amacıyla bir taslak rehber yayımladı. Taslak rehber, CRA'nın kapsamı ve uygulanma alanına ilişkin ilave açıklamalar sunmakta; özellikle donanım ve yazılım ürünleri dâhil olmak üzere dijital unsurlar içeren ürünler bakımından yükümlülükleri netleştirmektedir. Ayrıca, risk değerlendirmesi, zafiyet yönetimi, olay bildirim yükümlülükleri ve ürün yaşam döngüsü boyunca uygulanması gereken siber güvenlik gereklilikleri gibi temel uyum alanlarına ilişkin yönlendirmeler içermektedir. Taslak

rehberde ayrıca, açık kaynak yazılımlar, uzaktan veri işleme çözümleri ve ürünlere ilişkin destek süreleri gibi uygulamada önem arz eden konular ele alınmakta; özellikle küçük ve orta ölçekli işletmeler bakımından uyum süreçlerinin kolaylaştırılması hedeflenmektedir.

Taslak rehber, 31.03.2026 tarihinde sona eren bir kamuoyu istişare sürecine tabi tutuldu. Nihai rehberin, CRA'nın uygulanmasına yön vermesi beklenmekte olup, zafiyet yönetimi ve siber olay bildirimine ilişkin bazı yükümlülüklerin 11.09.2026 tarihinde uygulanmaya başlaması öngörülmektedir. Rehber, nihai hâliyle dahi bağlayıcı nitelik taşımayacaktır.

Taslak rehberin İngilizce metnine [buradan](#) ulaşabilirsiniz.

CJEU, Veri Sahibi Erişim Taleplerinin Hangi Durumlarda “Aşırı” Sayılabileceğine Açıklık Getirdi

19.03.2026 tarihinde CJEU, GDPR kapsamında veri sahibi erişim taleplerinin hangi durumlarda GDPR'ın 12/5'inci maddesi kapsamında “açıkça dayanaksız veya aşırı” sayılabileceğine açıklık getirdi. Divan, taleplerin sayısının tek başına belirleyici olmadığını; asıl incelemenin talebin bir hakkın kötüye kullanımı teşkil edip etmediğiyle ilgili olduğunu belirtti. Bu kapsamda, veri koruma hakkının kullanılmasından ziyade tazminat talebine zemin hazırlamak amacıyla yapılan baş-

vuruların, ilk talep dahi olsa “aşırı” olarak değerlendirilebileceği ifade edildi. Kararda ayrıca, talebin reddi veya ücret talep edilmesinin istisnai olduğu, ispat yükünün veri sorumlusunda bulunduğu ve kamuya açık bilgilerin tek başına ret gerekçesi oluşturamayacağı vurgulandı.

Kararın İngilizce metnine [buradan](#) ulaşabilirsiniz.

Avrupa Komisyonu, TikTok'un Bağımlılık Yaratan Tasarımının Dijital Hizmetler Tüzüğü'ne Aykırı Olabileceğini Değerlendirdi

Avrupa Komisyonu, 06.02.2026 tarihinde yayımladığı ön bulgularında, TikTok'un bağımlılık yaratan tasarım özellikleri nedeniyle Dijital Hizmetler Tüzüğü'nü (DSA) ihlal ettiğini ön değerlendirme aşamasında tespit ettiğini açıkladı. Söz konusu ön bulgular; sonsuz kaydırma, otomatik oynatma, anlık bildirimler ve kişiselleştirilmiş öneri sistemlerine odaklanmaktadır. Komisyon, anılan özelliklere ilişkin risklerin TikTok tarafından yeterince değerlendirilmediğini ve bu riskleri gidermeye yönelik etkili önlemlerin alınmadığını ifade etti. Bu çerçevede Komisyon, bazı tasarım özelliklerinin sınırlandırılması ve kullanıcı kontrollerinin güçlendirilmesi gerekebileceğini belirtmektedir. Ön bulgular nihai nitelikte olmamakla birlikte ihlalin tespiti hâlinde şirketin küresel cirosunun %6'sına kadar idari para cezası uygulanabilecektir.



Komisyon'un basın açıklamasının İngilizce metnine [buradan](#) ulaşabilirsiniz.

İşe Alım Süreçlerinde Otomatik Karar Alma Rehberi Yayınlandı

Birleşik Krallık'ın veri koruma otoritesi ICO, 31.03.2026 tarihinde yayımladığı rehberde, işe alım süreçlerinde ADM ve yapay zekâ kullanımına ilişkin önemli açıklamalarda bulundu. ICO, işverenlerin CV tarama, aday değerlendirme ve başvuru eleme süreçlerinde giderek daha fazla otomatik araçlardan yararlandığını; bu tür uygulamaların verimlilik sağlamakla birlikte şeffaflık, adillik ve ayrımcılık riski bakımından çeşitli endişeler doğurabileceğini belirtti.

Rehberde, işe alım süreçlerinde ADM kullanımının ancak uygun güvencelerin sağlanması hâlinde mümkün olabileceği ifade edildi. Bu kapsamda; adayların otomatik araçların kullanımı hakkında açık şekilde bilgilendirilmesi, karar alma süreçlerinde şeffaflığın sağlanması ve bireylere kararlara itiraz ederek insan incelemesi talep etme imkânı tanınması gerektiği vurgulandı. ICO ayrıca, kuruluşların bu tür teknolojileri kullanırken işe alım uygulamalarını gözden geçirmeleri ve veri koruma mevzuatına uyumu sağlamaları gerektiğini belirtti.

ICO tarafından yayımlanan rehberin İngilizce metnine [buradan](#) ulaşabilirsiniz.

Neler Yapılabilir?

İşe alım süreçlerinde ADM ve yapay zekâ araçlarından yararlanan şirketler bakımından; öncelikle kullanılan otomatik araçların hangi aşamalarda devreye girdiğinin (CV tarama, puanlama, eleme gibi) tespit edilerek adaylara bu süreçlerin açık ve anlaşılır bir dille bildirilmesi, otomatik değerlendirme sonucunda elenen adaylara kararın gerekçesini öğrenme ve bu karara itiraz ederek bir insan tarafından yeniden değerlendirilme talep etme imkânının tanınması, kullanılan algoritmaların özellikle yaş, cinsiyet, engellilik durumu ve etnik köken gibi korunan özellikler bakımından ayrımcı sonuçlar üretip üretmediğinin düzenli aralıklarla test edilmesi, otomatik eleme eşiklerinin ve puanlama kriterlerinin belgelenecek periyodik olarak gözden geçirilmesi ve mevcut işe alım süreçlerine ilişkin veri koruma etki değerlendirmelerinin yapılarak gerekli teknik ve idari tedbirlerin alınması önem taşımaktadır.

İlgili Kişiler



Sevgi Ünsal Özden
Yönetici Avukat ve Arabulucu

sevgiunsal@erdem-erdem.com



Ozan Akman
Kıdemli Avukat

ozanakman@erdem-erdem.av.tr

Yasal Uyarı

Bu bültende yer alan bilgi, belge ve değerlendirmeler sadece bilgilendirme amaçlı olup Erdem & Erdem Ortak Avukatlık Bürosu tarafından hazırlanmıştır. Reklam amacıyla veya Avukatlık Meslek Kuralları'na aykırı olan başka bir amaçla kullanılamaz. Erdem & Erdem tarafından açıkça yazılı olarak izin verilmediği müddetçe bu içeriğe bağlantı verilemez, kaynak gösterilerek alıntı yapılamaz, kısmen veya tamamen kullanılamaz. Bu bülten kapsamındaki tüm bilgi, belge ve değerlendirmelerin fikri mülkiyet hakları Erdem & Erdem'e aittir ve tüm hakları saklıdır.

ERDEM
&
ERDEM



İSTANBUL

Ferko Signature

Büyükdere Caddesi, No. 175 Kat. 3
34394, Esentepe - Şişli, İstanbul

+90 212 291 73 83
+90 212 291 73 82

istanbul@erdem-erdem.av.tr

İZMİR

1476 Sokak, No. 2, D. 27, Aksoy
Plaza Alsancak, İzmir

+90 232 464 66 76
+90 232 466 01 21

izmir@erdem-erdem.com

AMSTERDAM

Office 4.31, Strawinskylaan 457,
1077 XX Amsterdam

+31 (0)20 747 1113

amsterdam@erdem-erdem.nl

www.erdem-erdem.av.tr