



Kişisel Verileri Koruma Hukuku Güncel Gelişmeler

Türkiye'deki Gelişmeler

Veri İhlali Bildirimleri

- **Global Bilgisayar Kontrol Sistemleri San. ve Tic. A.Ş.** tarafından Kişisel Verileri Koruma Kurulu'na ("KVK Kurulu") bildirilen veri ihlali, 22.07.2026 tarihinde Kişisel Verileri Koruma Kurumu'nun ("KVK Kurumu") internet sitesinde yayımlanmıştır.

Veri ihlaline ilişkin kamuoyu duyurusuna [buradan](#) ulaşabilirsiniz.

- **Tamer Tanca Mağazacılık Sanayi Ve Ticaret A.Ş.** tarafından KVK Kurulu'na bildirilen veri ihlali, 05.08.2026 tarihinde KVK Kurumu'nun internet sitesinde yayımlanmıştır.

Veri ihlaline ilişkin kamuoyu duyurusuna [buradan](#) ulaşabilirsiniz.

- **Emsa Enerji Pazarlama ve Dış Ticaret Anonim Şirketi** tarafından KVK Kurulu'na bildirilen veri ihlali, 05.08.2026 tarihinde KVK Kurumu'nun internet sitesinde yayımlanmıştır.

Veri ihlaline ilişkin kamuoyu duyurusuna [buradan](#) ulaşabilirsiniz.

- **Novaform Makine Sanayi ve Ticaret Anonim Şirketi** tarafından KVK Kurulu'na bildirilen veri ihlali, 05.08.2026 tarihinde KVK Kurumu'nun internet sitesinde yayımlanmıştır.

Veri ihlaline ilişkin kamuoyu duyurusuna [buradan](#) ulaşabilirsiniz.

- **Mega Enerji Güç Sistemleri Jeneratör Pazarlama Sanayi ve Ticaret Anonim Şirketi** tarafından KVK Kurulu'na bildirilen veri ihlali, 05.08.2026 tarihinde KVK Kurumu'nun internet sitesinde yayımlanmıştır.

Veri ihlaline ilişkin kamuoyu duyurusuna [buradan](#) ulaşabilirsiniz.

- **Doğanay Ürgüplüoğlu (<https://www.redgalaxygame.space>)** tarafından KVK Kurulu'na bildirilen veri ihlali, 05.08.2026 tarihinde KVK Kurumu internet sitesinde yayımlanmıştır.

Veri ihlaline ilişkin kamuoyu duyurusuna [buradan](#) ulaşabilirsiniz.



Türkiye'deki Gelişmeler

Veri İhlali Bildirimleri

- **Tazemasa Gıda Ürünleri Pazarlama Sanayi ve Ticaret Anonim Şirketi tarafından KVK Kurulu'na bildirilen veri ihlali, 02.09.2026 tarihinde KVK Kurumu internet sitesinde yayımlanmıştır.**

Veri ihlaline ilişkin kamuoyu duyurusuna [buradan](#) ulaşabilirsiniz.

- **Yakupoğlu Tekstil ve Deri Sanayi Ticaret A.Ş. tarafından KVK Kurulu'na bildirilen veri ihlali, 02.09.2026 tarihinde KVK Kurumu'nun internet sitesinde yayımlanmıştır.**

Veri ihlaline ilişkin kamuoyu duyurusuna [buradan](#) ulaşabilirsiniz.

- **Bg Store Mağazacılık A.Ş. tarafından KVK Kurulu'na bildirilen veri ihlali, 02.09.2026 tarihinde KVK Kurumu'nun internet sitesinde yayımlanmıştır.**

Veri ihlaline ilişkin kamuoyu duyurusuna [buradan](#) ulaşabilirsiniz.

- **Coşkun Hazır Giyim Anonim Şirketi tarafından KVK Kurulu'na bildirilen veri ihlali, 02.09.2026 tarihinde KVK Kurumu internet sitesinde yayımlanmıştır.**

Veri ihlaline ilişkin kamuoyu duyurusuna [buradan](#) ulaşabilirsiniz.

- **Yapı Merkezi İnşaat ve Sanayi Anonim Şirketi tarafından KVK Kurulu'na bildirilen veri ihlali, 02.09.2026 tarihinde KVK Kurumu internet sitesinde yayımlanmıştır.**

Veri ihlaline ilişkin kamuoyu duyurusuna [buradan](#) ulaşabilirsiniz.

- **Canva Pty Ltd tarafından KVK Kurulu'na bildirilen veri ihlali, 16.09.2026 tarihinde KVK Kurumu internet sitesinde yayımlanmıştır.**

Veri ihlaline ilişkin kamuoyu duyurusuna [buradan](#) ulaşabilirsiniz.



Türkiye'deki Gelişmeler

Veri İhlali Bildirimleri

- **Alfa Öncü Global Otomotiv Mobilya San. Tic. Ltd. Şti. tarafından KVK Kurulu'na bildirilen veri ihlali, 16.09.2026 tarihinde KVK Kurumu internet sitesinde yayımlanmıştır.**

Veri ihlaline ilişkin kamuoyu duyurusuna [buradan](#) ulaşabilirsiniz.

- **Desa Deri Sanayi ve Ticaret A.Ş. tarafından KVK Kurulu'na bildirilen veri ihlali, 16.09.2026 tarihinde KVK Kurumu'nun internet sitesinde yayımlanmıştır.**

Veri ihlaline ilişkin kamuoyu duyurusuna [buradan](#) ulaşabilirsiniz.

- **Valmenti Mağazacılık Ticaret Limited Şirketi tarafından KVK Kurulu'na bildirilen veri ihlali, 16.09.2026 tarihinde KVK Kurumu'nun internet sitesinde yayımlanmıştır.**

Veri ihlaline ilişkin kamuoyu duyurusuna [buradan](#) ulaşabilirsiniz.

- **Shule Çanta ve Cüzdan Pazarlama Tic. Ltd. Şti. tarafından KVK Kurulu'na bildirilen veri ihlali, 23.09.2026 tarihinde KVK Kurumu internet sitesinde yayımlanmıştır.**

Veri ihlaline ilişkin kamuoyu duyurusuna [buradan](#) ulaşabilirsiniz.

- **Vergi Müfettişleri Derneği tarafından KVK Kurulu'na bildirilen veri ihlali, 23.09.2026 tarihinde KVK Kurumu internet sitesinde yayımlanmıştır.**

Veri ihlaline ilişkin kamuoyu duyurusuna [buradan](#) ulaşabilirsiniz.

- **Eipom İç ve Dış Tic. Ltd. Şti tarafından KVK Kurulu'na bildirilen veri ihlali, 23.09.2026 tarihinde KVK Kurumu internet sitesinde yayımlanmıştır.**

Veri ihlaline ilişkin kamuoyu duyurusuna [buradan](#) ulaşabilirsiniz.



Türkiye'deki Gelişmeler



Duyurular ve Haberler

KVK Kurumu, üçüncü kişilerden elde edilen iletişim bilgilerinin pazarlama amacıyla kullanımına ilişkin uyarıda bulundu.

Kişisel Verileri Koruma Kurumu ("KVK Kurumu"), 21 Temmuz 2026 tarihinde yayımladığı kamuoyu duyurusuyla, mevcut müşterilerden veya üçüncü kişilerden temin edilen telefon numarası ve e-posta adreslerinin reklam ve pazarlama amacıyla kullanılmasına ilişkin önemli açıklamalarda bulundu.

Duyuruda, kişisel verilerin üçüncü kişilerden elde edilmiş olmasının, bu verilerin reklam ve pazarlama amacıyla işlenmesi için **tek başına hukuki dayanak** oluşturmadığı vurgulandı. Veri sorumlularının, her somut olay bakımından KVKK'nın 5. maddesinde düzenlenen işleme şartlarını değerlendirmesi ve gerekli hallerde açık rıza alması gerektiği belirtildi. Kurum ayrıca, kişisel verilerin doğrudan ilgili kişiden elde edilmediği durumlarda da **aydınlatma yükümlülüğünün devam ettiğini** hatırlattı. Buna göre ilgili kişi; verilerin elde edilmesinden itibaren makul süre içinde, veriler iletişim amacıyla kullanılacaksa ilk iletişim sırasında ve aktarılacaksa en geç ilk aktarım sırasında bilgilendirilmelidir. Duyuruda ayrıca, kişinin pazarlama görüşmesini sonlandırmaması, bilgi almaya devam etmesi veya SMS'e ret vermemesi gibi davranışların **tek başına açık rıza olarak kabul edilemeyeceği** açıkça belirtildi. Açık rızaya dayalı işlemlerde aydınlatma ile açık rıza alma süreçlerinin birbirinden **ayrı yürütülmesi gerektiği** vurgulandı.

İlgili kamuoyu duyurusuna [buradan](#) ulaşabilirsiniz.

Siber Güvenlik Başkanlığı'nın internet ve iletişim altyapısına ilişkin yetkileri genişletildi.

TBMM'de kabul edilen düzenlemeyle, siber güvenliğin önemli bileşenlerinden olan **internet alan adlarının yönetimi, internet altyapısı ile iletişimin tespiti ve analizi gibi alanlardaki bazı görev ve yetkiler** Siber Güvenlik Başkanlığı bünyesinde toplandı. Düzenleme kapsamında, daha önce BTK'ya ait olan ve Siber Güvenlik Başkanlığı'na devredilen görev ve yetkiler kapsamında kullanılan bilgi işlem altyapıları, sistemler, veri merkezleri ile fiziki ve elektronik ortamdaki kayıt ve dokümanların Başkanlığa devredilmesi öngörüldü. Ayrıca, Başkanlık tarafından ikincil düzenlemeler yapılıncaya kadar mevcut düzenlemelerin uygulanmaya devam edilmesi hükme bağlandı.

Düzenlemeyle birlikte **internet alan adlarına ilişkin strateji ve politikaları belirleme ve düzenleme yapma yetkisi** de Siber Güvenlik Başkanlığı'na verildi. Bu değişiklik, siber güvenlik alanındaki görev ve yetkilerin tek bir kurum altında yeniden yapılandırılması bakımından önem taşımaktadır.

İlgili düzenlemenin tamamına [buradan](#) ulaşabilirsiniz.

Türkiye'deki Gelişmeler



Duyurular ve Haberler

KVK Kurumu, kamu kurumları için KVKK'ya uyum rehberi yayımladı.

KVK Kurumu, kamu kurum ve kuruluşları ile kamu kurumu niteliğindeki meslek kuruluşlarının KVKK uygulamalarına ilişkin farkındalığını artırmak ve uygulamada karşılaşılan tereddütleri gidermek amacıyla “**Kamu Kurum ve Kuruluşları ile Kamu Kurumu Niteliğindeki Meslek Kuruluşları İçin Kişisel Verilerin Korunması Kanununa Uyum Rehberi**”ni yayımladı. Rehberde, kamu kurumlarının kendilerine yöneltilen bilgi ve veri taleplerini yalnızca “KVKK'ya aykırılık” gerekçesiyle kategorik olarak reddetmemesi, taleplerin kişisel verinin niteliği, özel mevzuat hükümleri, hukuki dayanak ve ölçülülük bakımından değerlendirilmesi gerektiği vurgulandı.

Ayrıca, kamu kurumları arasında imzalanan **veri paylaşım protokollerinin tek başına kişisel veri aktarımı için hukuki dayanak oluşturmayacağı**, veri sorumlusunun ise kurum bünyesindeki belirli bir birim veya çalışan değil, kurumun kendisi olduğu açıklandı. Rehberde bunun yanı sıra yurt içi ve yurt dışı veri aktarımları, veri güvenliğine yönelik teknik ve idari tedbirler ile kamu kurumlarına ilişkin KVKK istisnaları da örneklerle ele alındı.

İlgili Rehber [buradan](#) ulaşabilirsiniz.

KVK Kurumu, mesai takibinde biyometrik veri kullanımına ilişkin açıklama yayımladı.

KVK Kurumu, 2026/921 sayılı “Mesai Takibi Amacıyla Biyometrik Veri İşlenmesi Hakkında İlke Kararı” sonrasında iletilen görüş talepleri üzerine konuya ilişkin yeni bir kamuoyu duyurusu yayımladı.

Duyuruda, **avuç içi veya parmak izi gibi verilerin matematiksel bir koda dönüştürülerek saklanması biyometrik veri niteliğini ortadan kaldırmadığı** vurgulandı. Kurum tarafından işverenlerin çalışma sürelerini takip etme yükümlülüğü bulunmakla birlikte, bu yükümlülüğün biyometrik sistemlerle yerine getirilmesini öngören açık bir kanuni düzenleme bulunmadığı belirtildi.

Bu kapsamda, yalnızca mesai takibi amacıyla biyometrik veri işlenmesinin KVKK'nın 6. maddesindeki işleme şartlarından herhangi birine dayanmadığı ve **açık rıza alınmış olsa dahi ölçülülük kriterini karşılamayacağı** ifade edildi. Bununla birlikte, yüksek güvenlik riski taşıyan tesislerde biyometrik sistemlerin kritik alanlara erişim ve kimlik doğrulama gibi güvenlik amaçlarıyla kullanılabileceği ancak bu kullanımın gerekli alan ve kişilerle sınırlı olması, alternatif yöntemlerin yetersiz kalması ve somut güvenlik ihtiyacıyla ölçülü olması gerektiği belirtildi.

İlgili kamuoyu duyurusuna [buradan](#) ulaşabilirsiniz.

Türkiye'deki Gelişmeler



Duyurular ve Haberler

KVK Kurumu, avukatların mesleki faaliyetlerinde kişisel verilerin korunmasına ilişkin uygulama rehberi yayımladı.

KVK Kurumu, Türkiye Barolar Birliği'nin görüş ve katkılarıyla hazırlanan “Avukatların Mesleki Faaliyetlerinde Kişisel Verilerin Korunmasına İlişkin Uygulama Rehberi”ni yayımladı.

Rehberde, avukatların mesleki faaliyetleri kapsamında gerçekleştirdiği kişisel veri işleme faaliyetlerine ilişkin hukuki çerçeve ve uygulamada karşılaşılan sorunlara yönelik çözüm önerileri ele alındı. Ayrıca **avukatların, tevkil edilen avukatların, avukat çalışanlarının ve diğer ilgili kişilerin veri sorumlusu/veri işleyen statüleri**, kişisel verilerin işleme şartları, özel nitelikli kişisel verilerin işlenmesi, yurt içi ve yurt dışına veri aktarımı ile veri güvenliği yükümlülüklerine ilişkin değerlendirmelere yer verildi.

Bağımsız çalışan avukatlar, aynı büroda çalışan avukatlar ve avukatlık ortaklıklarının veri koruma mevzuatı bakımından konumları ayrı ayrı değerlendirildi. Rehberin öne çıkan başlıklarından biri de **üretken yapay zeka araçlarının avukatlık faaliyetlerinde kullanımı** oldu. ChatGPT, Claude ve Gemini gibi araçlara müvekkil dosyaları, dava evrakları veya kişisel veri içeren belgelerin yüklenmesinin, kullanılan altyapıya bağlı olarak yurt dışına veri aktarımı sonucunu doğurabileceği belirtildi.

Bu kapsamda kişisel verilerin mümkün olduğunca maskelenmesi veya anonimleştirilmesi, yalnızca gerekli asgari verinin paylaşılması ve özel nitelikli kişisel verilerin bu sistemlere aktarılmasından kaçınılması önerildi. Ayrıca, yapay zeka araçlarının **veri saklama ve model eğitime politikalarının, insan incelemesi süreçlerinin, alt veri işleyenlerin ve güvenlik uygulamalarının** kullanım öncesinde değerlendirilmesi gerektiğine dikkat çekildi.

Rehberde, hukuka aykırı şekilde elde edilen veriler üzerinden kişilerin kimlik ve iletişim bilgilerinin sorgulanmasına imkan sağlayan yazılım ve uygulamaların kullanılmaması gerektiği de açıkça ifade edildi. Rehber, avukatlık faaliyetleri kapsamında işlenen kişisel verilerin hukuki dayanağının belirlenmesi ve özellikle yeni teknolojilerin kullanımında **veri minimizasyonu, veri güvenliği ve yurt dışına veri aktarımı** bakımından dikkat edilmesi gereken hususları somut örneklerle ortaya koyması açısından önem taşımaktadır.

İlgili Rehber [buradan](#) ulaşabilirsiniz.

Türkiye'deki Gelişmeler



Güncel Kararlar

Kişisel Verileri Koruma Kurulu, kaza mağdurlarının kişisel verilerinin hasar danışmanlığı amacıyla hukuka aykırı kullanımına ilişkin önemli ilke kararını açıkladı.

Kişisel Verileri Koruma Kurulu ("KVK Kurulu"), "hasar danışmanlığı", "sigorta takip merkezi" veya benzeri adlarla faaliyet gösteren kuruluşların kaza mağdurlarının kişisel verilerine hukuka aykırı şekilde erişerek mağdurlarla izinsiz iletişime geçtiklerine ilişkin çok sayıda ihbar ve şikayet üzerine **20 Mayıs 2026 tarihli ve 2026/1095 sayılı İlke Kararı'nı** almıştır. Karara ilişkin kamuoyu duyurusu 1 Temmuz 2026 tarihinde yayımlanmıştır.

KVK Kurulu, kaza mağdurlarına ait kişisel verilerin yalnızca kaza sonrası süreçlerin yürütülmesiyle sınırlı olarak ve Kişisel Verilerin Korunması Kanunu'nda ("KVKK") öngörülen **işleme şartlarına uygun şekilde** kullanılabileceğini vurgulamıştır. Sigorta eksperlerinin görevleri kapsamında kişisel veri işleyebileceği belirtilmekle birlikte, **görevleri nedeniyle eriştikleri verileri yetkisiz üçüncü kişilerle paylaşımlarının KVKK'ya aykırılık teşkil edeceği** ve şartları oluştuğunda Türk Ceza Kanunu kapsamında da sorumluluk doğurabileceği ifade edilmiştir. Kararda ayrıca, kaza mağdurlarına ilişkin kişisel verileri işleyen veri sorumlularının asgari yetki prensibine uygun erişim kontrolleri, rol tabanlı yetkilendirme ve loglama/takip mekanizmaları gibi teknik ve idari tedbirleri uygulaması gerektiği belirtilmiştir. Kurul, söz konusu yükümlülöklere aykırı hareket eden veri sorumluları hakkında KVKK'nın 18. maddesi kapsamında idari işlem tesis edilebileceğini hatırlatmıştır. Karar, özellikle sigorta şirketleri, sigorta eksperleri ve hasar yönetimi hizmeti sunan kuruluşlar bakımından, **kişisel verilere erişim yetkilerinin ve üçüncü taraflara veri aktarım süreçlerinin gözden geçirilmesi gerektiğini** ortaya koymaktadır.

İlgili ilke kararının tam metnine [buradan](#) ulaşabilirsiniz.

KVK Kurulu, 10 Ağustos 2026 tarihinde çeşitli kişisel veri işleme faaliyetlerine ilişkin karar özetlerini yayımladı.

KVK Kurulu tarafından 10 Ağustos 2026 tarihinde kişisel verilerin işlenmesine ilişkin çeşitli şikayetler ve veri ihlali bildirimleri kapsamında verdiği kararların özetlerini kamuoyuyla paylaştı. Yayımlanan karar özetleri, izinsiz pazarlama amaçlı ileti gönderimi, ceza infaz kurumlarında kişisel veri işlenmesi, uçak yolculuklarında sunulan internet hizmetlerinde açık rıza uygulamaları, kamera ve ses kayıtları, çerezler, ilgili kişilerin erişim talepleri ve veri ihlalleri gibi farklı konuları kapsamaktadır. Söz konusu kararlar, veri sorumlularının kişisel veri işleme faaliyetlerinde hukuka uygunluk şartlarına, aydınlatma yükümlülüğüne, veri güvenliğine ve ilgili kişilerin haklarına ilişkin uygulamalar bakımından önem taşımaktadır.

KVK Kurulu tarafından yayımlanan karar özetlerine ve bu kararlara ilişkin değerlendirmelerimize dair detaylı bilgi için DL'den Notlar serisi kapsamında yayımladığımız yazımızı [buradan](#) inceleyebilirsiniz.

Türkiye'deki Gelişmeler



Güncel Kararlar

KVK Kurulu, izinsiz pazarlama SMS'i gönderen tasarruf finansman şirketine 1 milyon TL ceza verdi.

KVK Kurulu tarafından bir kişinin açık rızası ve bilgisi olmaksızın pazarlama amaçlı SMS gönderilmesi ve telefon numarasının hukuka aykırı şekilde işlenmesi nedeniyle bir tasarruf finansman şirketine **1 milyon TL idari para cezası** uygulanmasına karar verildi.

Olayda, ilgili kişinin telefon numarasının başka bir müşteri tarafından sisteme eklendiği ve bu numaraya pazarlama amaçlı SMS gönderildiği, sonrasında ise sesli aramalar gerçekleştirildiği belirtildi. Şirket, şikayet üzerine ilgili kişiye ait verilerin sistemden silindiğini ve numaranın SMS gönderim panellerinde engellendiğini savundu. KVK Kurulu, açık rızanın veri işleme faaliyetinden önce, belirli bir konuya ilişkin, bilgilendirmeye dayalı ve özgür iradeyle alınması gerektiğini vurguladı. Ayrıca, **telefon numarasının üçüncü bir kişi aracılığıyla temin edilerek işlenmesini ve ilgili kişinin onayı olmaksızın ticari elektronik ileti gönderilmesini hukuka aykırı** buldu. Kararda, 6563 sayılı Elektronik Ticaretin Düzenlenmesi Hakkında Kanun ve İleti Yönetim Sistemi düzenlemelerine de atıf yapıldı. Karar, özellikle **pazarlama faaliyetlerinde kullanılan iletişim verilerinin kaynağının ve hukuki işleme şartının doğrulanmasının** ve ticari elektronik ileti süreçlerinin KVKK ile 6563 sayılı Kanun bakımından birlikte değerlendirilmesinin önemini ortaya koymaktadır.

İlgili habere [buradan](#) ulaşabilirsiniz.

KVK Kurulu, kamu kurumlarının internet sitelerinde kişisel veri paylaşımına ilişkin ilke kararını yayımladı.

KVK Kurulu 27 Temmuz 2026 tarihinde yayımladığı kamuoyu duyurusuyla, belediyeler, üniversiteler ve diğer kamu tüzel kişiliğini haiz veri sorumlularının internet sitelerinde kişisel veri paylaşımına ilişkin önemli değerlendirmelerde bulundu. Kurul, internet sitelerinde **T.C. kimlik numarası, adres, telefon numarası, sınav ve KPSS puanları, aday/öğrenci numarası ve benzeri kişisel verilerin** yayımlanmasının, verilerin üçüncü kişiler tarafından erişilebilir hale gelmesi nedeniyle KVKK kapsamında bir veri işleme faaliyeti olduğunu vurguladı.

İnternet ortamında kişisel veri paylaşımının geçerli bir işleme şartına dayanması ve **amaçla bağlantılı, sınırlı ve ölçülü** olması gerektiğini belirten Kurul, gerekli olmayan verilerin paylaşılmaması, gerektiğinde maskeleye uygulanması ve içeriklerin belirlenen süre sonunda kaldırılması gerektiğini açıkladı. Sınav ve kura sonuçları gibi duyurularda ise mümkün olduğunca yalnızca ilgili kişinin erişebileceği güvenli yöntemlerin tercih edilmesi gerektiği belirtildi. Kurul ayrıca mevcut internet içeriklerinin gözden geçirilmesi, gerekli teknik ve idari tedbirlerin alınması ve ilgili personele düzenli eğitim verilmesi gerektiğini hatırlattı.

İlgili ilke kararına [buradan](#) ulaşabilirsiniz.

Türkiye'deki Gelişmeler

Mevzuat Gündemi

Kişisel Sağlık Verileri Yönetmeliği'nde değişiklik: Geçmiş tanıların işe giriş süreçlerinde kullanımına yeni düzenleme getirildi.

4 Temmuz 2026 tarihli Resmî Gazete'de yayımlanan değişiklikle, Kişisel Sağlık Verileri Hakkında Yönetmeliğe "kişisel sağlık verilerinin yeniden değerlendirilmesi" başlıklı yeni bir madde eklendi. Düzenleme uyarınca, kişiler geçmişte konulmuş tanıların mevcut sağlık durumları çerçevesinde yeniden değerlendirilmesi talebiyle sağlık hizmeti sunucularına başvuruda bulunabilir. Yeniden değerlendirme sonucunda tanının kişinin güncel durumunda bulunmadığına ilişkin sağlık kurulu raporu düzenlenmesi halinde, ilgili mevzuattaki özel hükümler saklı kalmak üzere, **başta işe giriş süreçleri olmak üzere geçmiş tanıların yerine güncel sağlık kurulu raporu esas alınacaktır.** Düzenleme, özellikle işverenler bakımından **özel nitelikli kişisel veri niteliğindeki sağlık verilerinin işe giriş ve istihdam süreçlerinde işlenmesi** açısından önem taşımaktadır.

Düzenleme, işe alım ve istihdam süreçlerinde geçmiş sağlık kayıtlarının güncel sağlık durumunu her zaman doğru şekilde yansıtmayabileceğini dikkate alması bakımından önem taşımaktadır. Bu kapsamda, işverenlerin adayların veya çalışanların sağlık durumlarına ilişkin değerlendirmelerinde geçmiş tanıları tek başına belirleyici kabul etmek yerine, **ilgili mevzuat çerçevesinde güncel sağlık kurulu raporlarını esas almaları** gerekebilir. Bununla birlikte, sağlık verilerinin özel nitelikli kişisel veri olması nedeniyle, işe giriş ve istihdam süreçlerinde bu verilerin işlenmesi bakımından KVKK'da öngörülen hukuki şartların ayrıca değerlendirilmesi gerekmektedir. İşverenlerin yalnızca ilgili pozisyonun gereklilikleri ve mevzuattan doğan yükümlülükleri kapsamında ihtiyaç duyulan sağlık verilerini işlemesi; bu verilere erişimi görev ve yetki esasına göre sınırlandırması ve uygun teknik ve idari güvenlik tedbirlerini uygulaması önem taşımaktadır. Dolayısıyla değişiklik, yalnızca geçmiş tanıların yeniden değerlendirilmesine ilişkin bir imkan sunmakla kalmayıp, sağlık verilerinin işe alım kararlarında nasıl dikkate alınacağı ve bu süreçlerde veri koruma ilkelerine nasıl uyulacağı bakımından da işverenlerin mevcut uygulamalarını gözden geçirmelerini gerektirebilir niteliktedir.

İlgili Yönetmeliğe ilişkin değişikliğin tam metnine [buradan](#) ulaşabilirsiniz.





Dünyadaki Gelişmeler

Duyurular ve Haberler

AB-ABD veri aktarım mekanizmasına yönelik yeni hukuki süreç gündemde.

Avrupa'daki veri koruma alanındaki çalışmalarıyla bilinen noyb, [EU-US Data Privacy Framework \(DPF\)](#) kapsamında AB'den ABD'ye gerçekleştirilen kişisel veri aktarımlarına ilişkin yeni bir hukuki süreç başlatmaya hazırlanmaktadır.

Gelişme, ABD Yüksek Mahkemesi'nin 29 Haziran 2026 tarihli kararının ardından gündeme geldi. Karar sonrasında noyb, Avrupa Komisyonu'na DPF kapsamında ABD'nin veri koruma denetim mekanizmalarına ilişkin yeterlilik değerlendirmesinin yeniden ele alınması ve ABD'ye ilişkin yeterlilik kararının geri çekilmesi çağrısında bulundu. Kuruluş, özellikle ABD Federal Trade Commission'ın ("FTC") bağımsızlığına ilişkin gelişmelerin DPF'in dayandığı denetim yapısı bakımından önem taşıdığını savunmaktadır. Noyb ayrıca önümüzdeki dönemde DPF'e karşı yeni bir hukuki süreç başlatmaya hazırlandığını açıkladı. Bu gelişme, daha önce [Safe Harbor ve Privacy Shield'in Avrupa Birliği Adalet Divanı tarafından geçersiz kılınmasına](#) yol açan Schrems I ve Schrems II süreçlerinin ardından, AB-ABD veri aktarımlarına ilişkin yeni bir yargısal inceleme ihtimalini gündeme getirmektedir. Gelişme, özellikle [ABD merkezli bulut, SaaS ve teknoloji hizmet sağlayıcılarına veri aktarımı gerçekleştiren kuruluşlar açısından](#), DPF'in geleceğine ilişkin gelişmelerin ve alternatif aktarım mekanizmalarının takip edilmesinin önemini ortaya koymaktadır.

İlgili gelişmeye ilişkin açıklamalara [buradan](#) ulaşabilirsiniz.

AB Komisyonu, yapay zeka kaynaklı siber tehditlere karşı yeni eylem planı açıkladı.

Avrupa Birliği Komisyonu, gelişmiş yapay zeka modellerinin siber saldırıları daha hızlı ve etkili hale getirmesiyle ortaya çıkan risklere karşı "[Siber Güvenlik ve Yapay Zeka Eylem Planı](#)"nı 7 Temmuz 2026 tarihinde açıkladı.

Eylem planı kapsamında, yapay zekanın güvenlik açıklarını tespit etmek ve siber saldırıları otomatikleştirmek amacıyla kötüye kullanımından kaynaklanan risklere karşı AB'nin dijital altyapısının güçlendirilmesi hedeflenmektedir. Bu kapsamda üye ülkeler, sektör temsilcileri ve AB kurumlarının iş birliği içinde çalışması öngörülmektedir. Plan kapsamında ayrıca, [AB Yapay Zeka Yasası](#) çerçevesinde gelişmiş yapay zeka modellerinin piyasaya sunulmadan önce güvenlik riskleri bakımından değerlendirilmesi ve risk azaltıcı önlemlerin incelenmesi planlanmaktadır. AB Komisyonu, 2027 yılında faaliyete geçmesi hedeflenen bağımsız bir yapay zeka değerlendirme kapasitesi oluşturmayı da planlanmaktadır. Bunun yanı sıra Avrupa Siber Güvenlik Ajansı ("ENISA") ve AB Komisyonu tarafından kritik sektörlerde kullanılacak yapay zeka sistemlerinin güvenli şekilde test edilmesine yönelik çalışmalar yürütülmesi öngörülmektedir. Eylem planı, [yapay zeka sistemlerinin geliştirilmesi ve kullanımında risk yönetimi, siber hijyen ve "tasarım aşamasında güvenlik"](#) yaklaşımlarının güçlendirilmesini öngörmesi bakımından önem taşımaktadır.

İlgili eylem planına ilişkin habere [buradan](#) ulaşabilirsiniz.



Dünyadaki Gelişmeler

Duyurular ve Haberler

Almanya’da yapay zeka destekli arama hizmetleri medya hukuku denetimi kapsamına alınacaktır.

Almanya’daki 14 eyalet medya otoritesini temsil eden Lisanslama ve Denetim Komisyonu (“ZAK”), [Google’ın AI Overviews özelliği ile Perplexity AI’nın Alman medya hukukuna tabi olduğunu](#) açıkladı.

Karar, yapay zeka tarafından oluşturulan içeriklerin hukuki sorumluluğuna ilişkin tartışmaları yeniden gündeme taşıdı. ZAK’a göre AI Overviews ve benzeri yapay zeka destekli hizmetlerin oluşturduğu haber özetleri ve chatbot yanıtları, yalnızca üçüncü taraf içeriklerin gösterilmesi olarak değerlendirilemey, hizmet sağlayıcıların [kendi oluşturduğu içerikler](#) olarak kabul edilebilir. Açıklama, Münih’te görülen ve Google’ın AI Overviews tarafından oluşturulan hatalı bilgilerden sorumlu tutulabileceğine ilişkin mahkeme kararının ardından geldi.

Düzenleyici ayrıca, Google’ın yapay zeka özetlerini arama sonuçlarında öne çıkarmasının geleneksel haber bağlantılarının görünürlüğünü azaltabileceğini ve Perplexity gibi hizmetlerin kaynak ve bağlantıları seçerek haber içeriklerinin erişilebilirliğini etkilediğini belirtti. Bu nedenle söz konusu hizmetlerin, medya çoğulculuğunu korumaya yönelik kurallara tabi “[medya araçları](#)” olarak değerlendirilebileceği ifade edildi. Google ise karara itiraz edeceğini açıkladı. Gelişme, üretken yapay zeka tarafından oluşturulan içeriklerin yalnızca veri veya arama sonucu sunumu olarak değil, hizmet sağlayıcının hukuki sorumluluğunu doğurabil bir içerik faaliyeti olarak değerlendirilmesi bakımından önem taşımaktadır.

İlgili habere [buradan](#) ulaşabilirsiniz.

Birleşik Krallık NCSC’den siber saldırı sonrası müdahale ve kurtarma rehberi yayımlandı.

Birleşik Krallık Ulusal Siber Güvenlik Merkezi (NCSC), kuruluşların ciddi siber saldırılar sonrasında müdahale ve kurtarma süreçlerini yönetmelerine yönelik yeni bir rehber yayımladı.

Rehber; [olayın ilk saatlerinde müdahale ve koordinasyonun sağlanması, kritik iş süreçlerinin yeniden işler hale getirilmesi ve uzun vadede daha güvenli sistemlerin oluşturulması](#) olmak üzere üç aşamalı bir çerçeve sunmaktadır. Ayrıca kuruluşların yalnızca yazılı planlar hazırlamakla kalmayarak, yedeklerden sistemlerin yeniden kurulması ve sistemlerin devre dışı bırakılıp yeniden başlatılması gibi senaryoları düzenli olarak test etmeleri gerektiği vurgulanmaktadır.

İlgili rehber [buradan](#) ulaşabilirsiniz.



Dünyadaki Gelişmeler

Duyurular ve Haberler

Google, hukuk sektörüne özel yapay zeka çözümü Gemini Enterprise for Legal'ı duyurdu.

Google Cloud, 25 Ağustos 2026 tarihinde hukuk büroları ve şirket içi hukuk ekiplerinin kullanımına yönelik **Gemini Enterprise for Legal** adlı yapay zeka çözümünü duyurdu. Ürün, hukuki iş akışlarını desteklemek amacıyla hukuk teknolojileriyle entegrasyon sağlayan bağlantılar, hukuk alanına özgü yetenekler ve yapay zeka agent'ları sunmaktadır.

Çözüm kapsamında **sözleşme inceleme ve yönetimi, hukuki metin taslağı hazırlama, mevzuat takibi, hukuki atıfların doğrulanması, due diligence ve veri sahibi başvurularının (DSAR) yürütülmesi** gibi süreçlerin otomatikleştirilmesi hedeflenmektedir. Platformun Harvey, Legora, DocuSign, Thomson Reuters, iManage, RelativityOne ve NetDocuments gibi hukuk teknolojileriyle bağlantı kurabildiği belirtilmektedir.

Google ayrıca müşteri verileri, istemler ve yapay zeka çıktılarının kuruluşun özel bulut ortamında tutulduğunu, temel modellerin müşteri verileriyle eğitilmediğini ve mevcut erişim yetkilerinin korunduğunu belirtmektedir. Platformda risk yönetimi, denetim kayıtları ve yönetim özellikleri de sunulmaktadır.

İlgili duyuruya [buradan](#) ulaşabilirsiniz.

Almanya'da Meta'nın yapay zeka destekli akıllı gözlüklerine yönelik hukuki inceleme başlatıldı.

Almanya merkezli dijital haklar kuruluşu HateAid, Meta ve Ray-Ban Meta akıllı gözlüklerinin Almanya'daki satışına ilişkin suç duyurusunda bulundu.

Şikayet, özellikle **kişilerin bilgisi dışında ses veya görüntü kaydı yapılmasını sağlayan iletişim cihazlarının satışını yasaklayan federal düzenlemelere** dayandırıldı. HateAid, kamerayla donatılmış ve günlük bir aksesuar görünümündeki akıllı gözlüklerin kişilerin farkında olmadan kaydedilmesi riskini artırdığını belirtti. Frankfurt'taki dijital suçlar birimi ZIT, şikayeti aldığını ve ön değerlendirme yapacağını açıkladı. Federal Ağ Ajansı (BNetzA) ise akıllı gözlük pazarını yakından izlediğini, ancak mevcut durumda resmi bir ihlal soruşturması yürütmediğini bildirdi.

Alman makamları, kayıt fonksiyonunun görünür bir uyarı ışığı gibi unsurlarla açıkça belli olması halinde cihazların satışının tek başına yasak olmadığını belirtmektedir. Gelişme, yapay zeka destekli giyilebilir teknolojilerde mahremiyet, gizli kayıt ve kişisel verilerin korunması konularının giderek daha fazla hukuki denetime konu olduğunu göstermektedir.

İlgili habere [buradan](#) ulaşabilirsiniz.



Dünyadaki Gelişmeler

Duyurular ve Haberler

Avrupa Komisyonu, ChatGPT'yi "Çok Büyük Çevrimiçi Arama Motoru" olarak belirledi.

Avrupa Komisyonu, 31 Ağustos 2026 tarihinde ChatGPT'yi Avrupa Birliği Dijital Hizmetler Yasası (DSA) kapsamında "Çok Büyük Çevrimiçi Arama Motoru" (Very Large Online Search Engine – VLOSE) olarak belirledi. ChatGPT'nin yanı sıra Reddit ve Roblox da aylık ortalama en az 45 milyon AB kullanıcısına ulaşmaları nedeniyle DSA kapsamında sırasıyla VLOP ve VLOSE statüsüne alındı. Kararın dikkat çeken yönlerinden biri, Avrupa Komisyonu'nun [ChatGPT'nin hukuki niteliğine ilişkin değerlendirmesi](#) oldu.

Komisyon, ChatGPT'nin kullanıcı istem ve sorularına yanıt vermesinin yanı sıra web üzerinde arama yapabilmesi nedeniyle hizmeti "hibrit bir hizmet" olarak değerlendirerek DSA kapsamında çevrimiçi arama motoru olarak kabul etti. Bu kapsamda ChatGPT, genel DSA yükümlülüklerinin yanı sıra VLOSE'lara uygulanan ilave yükümlülüklerle tabi olacaktır.

Yeni statüyle birlikte OpenAI'nin, hizmetten ve algoritmik sistemlerden kaynaklanan [sistemik riskleri belirlemesi, değerlendirmesi ve azaltması](#) gerektir. Bu riskler arasında hukuka aykırı içeriklerin yayılması, çocuklar üzerindeki olumsuz etkiler, kullanıcıların fiziksel ve ruhsal iyilik hali, temel haklar, seçim süreçleri ve kamu güvenliğiyle bağlantılı riskler yer almaktadır.

Bunun yanında ChatGPT'nin [bağımsız denetime ve iç uyum mekanizmalarına](#) tabi olması, belirli verileri Avrupa Komisyonu ve yetkili makamlarla paylaşması ve gerekli şartları sağlayan araştırmacıların belirli verilere erişimini mümkün kılması gerektir. Yeni yükümlülüklerle uyum için dört aylık süre öngörülürken, sürenin Ocak 2027'de sona ermesi beklenmektedir.

Belirlemeyle birlikte Avrupa Komisyonu, ChatGPT'nin işlevlerini ve gerektiğinde bunlarla bağlantılı sistemleri incelemek üzere doğrudan araştırma ve denetim yetkisine de sahip olacaktır. DSA kapsamındaki yükümlülüklerin ihlali halinde ise şirketlere dünya çapındaki yıllık cirolarının %6'sına kadar idari para cezası uygulanabilmektedir.

İlgili duyuruya [buradan](#) ulaşabilirsiniz.

Dünyadaki Gelişmeler



Duyurular ve Haberler

Avrupa Komisyonu, çocukların çevrimiçi güvenliğinin güçlendirilmesine yönelik EU KIDS Act teklifini yayımladı.

Avrupa Komisyonu, çocukların sosyal medya ve diğer dijital hizmetlerde daha güvenli bir çevrimiçi deneyim yaşamasını amaçlayan EU KIDS Act teklifini yayımladı. Teklif, yaş sınırlarının yanı sıra yaş doğrulama, güvenli tasarım, öneri sistemleri ve çocukların mahremiyetinin korunmasına ilişkin kapsamlı düzenlemeler öngörmektedir. Teklife göre **13 yaşından küçük çocukların sosyal medya hesabı açması engellen**, 13-14 yaş grubundaki çocukların ise belirli riskli hizmetleri ebeveyn kontrolü altında kullanması öngörülmüştür. 15 yaşından itibaren bağımsız hesap açılabilir. Ayrıca sonsuz kaydırma, kesintisiz otomatik oynatma ve aşırı kullanımı teşvik eden bazı tasarım özelliklerinin sınırlandırılması planlanmaktadır. Veri koruması bakımından öne çıkan düzenlemelerden biri, platformlardan bağımsız ve sertifikalı yaş doğrulama çözümleri. Komisyon, platformların kullanıcıların kimliğini öğrenmeden yalnızca ilgili yaş eşliğinin karşılanıp karşılanmadığını doğrulayabilmesini sağlayacak “zero-knowledge proof” temelli çözümleri gündeme getirmektedir. Teklifin, çevrimiçi oyunlar, uygulama mağazaları ve çocukların erişebildiği yapay zeka chatbotları ve AI companion hizmetlerini de kapsamı öngörülmektedir.

İlgili açıklamaya [buradan](#) ulaşabilirsiniz.

EDPB, GDPR kapsamında idari para cezaları ve DSA-GDPR ilişkisine yönelik yeni rehberler yayımladı.

Avrupa Veri Koruma Kurulu (EDPB), 21 Eylül 2026 tarihinde GDPR kapsamında idari para cezalarının uygulanmasına ilişkin yeni rehberini ve Dijital Hizmetler Yasası (DSA) ile GDPR arasındaki etkileşime ilişkin rehberin nihai versiyonunu kabul etti.

Yeni idari para cezası rehberi, Avrupa’daki veri koruma otoritelerinin ceza uygulanıp uygulanmayacağına ilişkin değerlendirmelerini daha uyumlu hale getirmeyi amaçlamaktadır. Bu kapsamda otoritelerin, ihlalin cezalandırılabilir olup olmadığını, sorumluluğun veri sorumlusu veya veri işleyene ait olup olmadığını, ihlalin kasten veya ihmalle gerçekleştirilip gerçekleştirilmediğini, ağırlaştırıcı ve hafifletici unsurları ve cezanın **etkili, orantılı ve caydırıcı** olup olmayacağını beş aşamalı bir metodoloji çerçevesinde değerlendirmesi öngörülmektedir. Rehber ayrıca uyarı, kınama, emir ve işlemeye ilişkin kısıtlamalar gibi diğer düzeltici yetkilerin kapsamını açıklamakta ve 14 uygulama örneği sunmaktadır. Rehber için kamuoyu görüşü süreci 13 Kasım 2026’ya kadar devam edecektir. EDPB aynı toplantıda, DSA ile GDPR’ın birlikte uygulanmasına ilişkin rehberin kamuoyu görüşleri sonrasında nihai versiyonunu da kabul edilmiştir.

İlgili rehberlere [buradan](#) ulaşabilirsiniz.



Dünyadaki Gelişmeler

Güncel Kararlar

İspanya’da işverenin Teams üzerinden yanlışlıkla kaydedilen özel konuşmaları çalışana karşı kullanması hukuka aykırı bulundu.

İspanya Bask Bölgesi Yüksek Adalet Mahkemesi, **Microsoft Teams toplantısı sonrasında yanlışlıkla kaydedilen özel konuşmaların işveren tarafından çalışan aleyhine kullanılmasını** hukuka aykırı buldu. Olayda, toplantının sona ermesinin ardından Teams kaydının teknik bir hata nedeniyle devam ettiği ve çalışan ile eski CEO ve bir yönetim kurulu üyesi arasındaki özel konuşmaların katılımcıların bilgisi olmaksızın kaydedildiği tespit edilmiştir. Mahkeme, çalışanın kaydın devam ettiğinden haberdar olmadığını, kayda rıza göstermediğini ve teknik hataya kendisinin neden olmadığını belirterek **makul mahremiyet beklentisinin korunması gerektiğine** hükmetmiştir. Mahkeme ayrıca, ihlalin yalnızca kaydın yanlışlıkla oluşturulmasından değil, işverenin aylar sonra kayda erişerek içeriğini iş ilişkisi kapsamında çalışana karşı kullanmasından kaynaklandığını değerlendirmiştir. Bu nedenle kayıtların çalışan aleyhine delil olarak kullanılamayacağına karar veren Mahkeme, çalışanın iş sözleşmesini haklı nedenle sona erdirebileceğine hükmetmiştir. İşverene **328.491,62 Euro yasal tazminat ve 7.501 Euro manevi tazminat** ödeme yükümlülüğü getirilmiştir.

İlgili karara ilişkin detaylara [buradan](#) ulaşabilirsiniz.

Birleşik Krallık Veri Koruma Otoritesi, izinsiz pazarlama SMS’leri nedeniyle şirkete 300 bin sterlin ceza verdi.

Birleşik Krallık Bilgi Komisyonu Ofisi (ICO), KRA Consultancy Ltd.’ye geçerli rıza olmaksızın 5,5 milyondan fazla doğrudan pazarlama SMS’i göndermesi ve gönderilerde şirket kimliğini gizlemesi nedeniyle **300.000 sterlin idari para cezası** uyguladı. ICO’nun incelemesinde, 24 Nisan 2022 ile 29 Mayıs 2025 tarihleri arasında borç yapılandırma ve borç silme hizmetlerini tanıtan 5.575.715 SMS’in şirket tarafından gönderildiği veya gönderilmesinin sağlandığı ve bu mesajlara ilişkin 60.000’den fazla spam şikayeti alındığı tespit edildi. Şirketin kredi başvurusu reddedilen kişilere ait **veri setleri ve diğer üçüncü taraf kaynaklardan elde edilen kişisel verileri kullandığı, ancak alıcıların pazarlama mesajlarını almaya geçerli şekilde rıza verdiğini gösteremediği** belirtildi. ICO ayrıca, bazı mesajlarda alıcıları baskı altına almak amacıyla “sahte icra memuru” mesajlarının kullanıldığını ve özellikle finansal açıdan kırılgan kişilerin hedeflendiğini tespit etti. Şirketin kimliğini gizlemek amacıyla farklı ticari isimler ve anonim internet siteleri kullanması da ihlalin ağırlığını artıran unsurlar arasında değerlendirildi.

İlgili karara ilişkin detaylara [buradan](#) ulaşabilirsiniz.



Dünyadaki Gelişmeler

Güncel Kararlar

Avrupa Komisyonu, Google'a Dijital Pazarlar Yasası ihlalleri nedeniyle 890 milyon Euro ceza verdi.

Avrupa Komisyonu, Google'ın **Dijital Pazarlar Yasası (DMA)** kapsamındaki yükümlülüklerini ihlal ettiğine karar vererek şirkete toplam 890 milyon Euro idari para cezası uygulanmasına hükmetti. Cezanın 460 milyon Euro'luk kısmı Google'ın arama sonuçlarında kendi hizmetlerini üçüncü taraf hizmetlere kıyasla avantajlı konumlandırması, 430 milyon Euro'luk kısmı ise Google Play'de uygulama geliştiricilerinin kullanıcıları alternatif ve daha uygun fiyatlı satın alma kanallarına yönlendirmesini kısıtlaması nedeniyle verildi. Komisyon, **Google Search'te alışveriş, otel, ulaşım ve spor hizmetleri gibi Google'a ait sonuçların daha görünür şekilde sunulduğunu ve üçüncü taraf hizmetlere eşit koşullar sağlanmadığını** tespit etti. Google Play bakımından ise geliştiricilerin kullanıcıları Google Play dışındaki teklif ve satın alma kanallarına yönlendirmelerinin hem teknik hem de sözleşmesel olarak kısıtlandığı değerlendirildi.

Komisyon, Google'a ihlalleri sona erdirmesi ve üçüncü taraf hizmetlere **adil ve ayrımcı olmayan koşullar sağlaması** yönünde talimat verdi. Şirketin kararlara 60 gün içinde uyum sağlaması gerekmektedir, aksi halde dünya çapındaki toplam cirosunun %5'ine kadar periyodik para cezası uygulanabilir.

İlgili karara ilişkin detaylara [buradan](#) ulaşabilirsiniz.

Belçika Veri Koruma Otoritesi, çalışanın özlük kayıtlarına erişim talebinin işveren tarafından reddedilemeyeceğine karar verdi.

Belçika Veri Koruma Otoritesi (APD/GBA), bir çalışanın **çalışma saatlerini gösteren hizmet formlarının kopyalarına erişim talebinin işveren tarafından yalnızca işyerinde inceleme imkanı sunularak karşılanamayacağına** karar verdi. Olayda çalışan, son beş yıla ait el yazılı hizmet formlarının kopyalarını talep etmiş, bu belgelerde çalışma saatleri, seyahatler, gerçekleştirilen hizmetler ve ziyaret edilen müşterilere ilişkin bilgiler yer almıştı. İşveren ise belgelerin farklı klasörlerde tarih bazında tutulduğunu ve kopyalanmalarının önemli bir iş yükü oluşturacağını belirterek çalışana kayıtları işyerinde incelemesini önermişti. Otorite, **GDPR m.15 kapsamında erişim hakkının, kişisel verilerin kopyasının sağlanmasını da içerdiğini** ve işverenin kendi arşivleme sisteminden kaynaklanan iş yükünün talebin "aşırı" kabul edilmesi için tek başına yeterli olmadığını değerlendirdi. Ayrıca çalışanların erişim taleplerinin gerekçesini açıklamak zorunda olmadığı vurgulandı. APD/GBA, GDPR'ın 12 ve 15. maddelerinin ihlal edildiğine hükmederek işverene kınama verilmesine ve talep edilen kayıtların bir ay içinde çalışana sunulmasına karar verdi.

İlgili karara ilişkin detaylara [buradan](#) ulaşabilirsiniz.



Dünyadaki Gelişmeler

Güncel Kararlar

Almanya'da iş başvurusu sırasında kişisel verilerin üçüncü kişiye aktarılması nedeniyle tazminata hükmedildi.

Almanya Federal Adalet Divanı (BGH), bir bankanın işe alım sürecinde **adayın kişisel verilerini yanlışlıkla üçüncü bir kişiye göndermesi** nedeniyle adayın manevi tazminat talep edebileceğine karar verdi. Olayda banka çalışanı, işe başvuran aday için hazırlanan ve adayın **adı ile ücret beklentisini** içeren mesajı yanlışlıkla başka bir kişiye göndermişti. Mahkeme, aktarımın GDPR m.6 kapsamında herhangi bir hukuki dayanağa dayanmadığını ve bu nedenle hukuka aykırı veri işleme teşkil ettiğini değerlendirdi. BGH, GDPR m.82 kapsamında manevi zararın oluşması için kişinin verileri üzerindeki kontrolünü kaybetmesinin yeterli olabileceğini belirtti. Somut olayda adayın, verilerinin alıcı tarafından kendi iş başvurularında kullanılabileceğine ilişkin endişesinin **kişisel veriler üzerindeki kontrol kaybı** oluşturduğu ve tazminat hakkı doğurduğu kabul edildi. Tazminat miktarının belirlenmesi için dosya alt mahkemeye gönderildi. Buna karşılık Mahkeme, aynı ihlalin tekrarlanma riski bulunmadığından ihtiyati tedbir talebinin karşılanamayacağına hükmetti.

İlgili karara ilişkin detaylara [buradan](#) ulaşabilirsiniz.

İspanya Veri Koruma Otoritesi, 23andMe'ye genetik ve sağlık verilerinin yetersiz korunması nedeniyle 2,4 milyon Euro ceza verdi.

İspanya Veri Koruma Otoritesi (AEPD), genomik ve biyoteknoloji şirketi **23andMe, Inc.** hakkında, hassas kişisel verilerin yeterli güvenlik önlemleriyle korunmaması ve veri ihlalinin 72 saatlik bildirim süresi içinde Kuruma bildirilmemesi nedeniyle toplam **2,4 milyon Euro idari para cezası** uygulanmasına karar verdi. Ekim 2023'te gerçekleşen kimlik bilgisi doldurma (credential stuffing) saldırısı sonucunda İspanya'da yaşayan 2.642 müşterinin kimlik, iletişim ve konum bilgilerinin yanı sıra genetik verileri, sağlık verileri ve etnik kökene ilişkin verileri ele geçirildi. AEPD, özellikle özel nitelikli kişisel verilerin işlenmesi nedeniyle güçlü güvenlik tedbirlerinin uygulanması gerektiğini belirtti. Şirketin çok faktörlü kimlik doğrulamayı zorunlu tutmaması, parola güvenliği ve hesap erişimine ilişkin ek kontroller uygulamaması yetersiz bulundu.

AEPD ayrıca, ihlalden **5 Ekim 2023'te haberdar olunmasına rağmen** Kuruma bildirimin 17 Ekim'de yapılmasını **GDPR m.33'e aykırı değerlendirdi**. Buna göre cezanın 2 milyon Euro'luk kısmı GDPR m.5(1)(f), 400 bin Euro'luk kısmı ise m.33 ihlali nedeniyle uygulandı.

İlgili karara ilişkin detaylara [buradan](#) ulaşabilirsiniz.



Dünyadaki Gelişmeler

Güncel Kararlar

İtalya Veri Koruma Otoritesi, Lusha Systems'e hukuka aykırı kişisel veri işleme nedeniyle 2 milyon Euro ceza verdi.

İtalya Veri Koruma Otoritesi (Garante), B2B iletişim verileri sağlayan **Lusha Systems Inc.** hakkında, kişilerin mesleki iletişim bilgilerinin geçerli bir hukuki dayanak olmaksızın toplanması, birleştirilmesi ve üçüncü taraflara sunulması nedeniyle **2 milyon Euro idari para cezası** uygulanmasına karar verdi. Otorite, şirketin farklı kaynaklardan topladığı isim, e-posta adresi, telefon numarası ve mesleki bilgiler ile bunlara ek olarak CRM kayıtları, e-posta içerikleri, takvim bilgileri ve tarama verilerini birleştirerek sürekli güncellediğini tespit etti. Bu kapsamlı veri işlemenin, **meşru menfaat hukuki sebebine dayanmak için gerekli ve orantılı olmadığı** değerlendirildi. Ayrıca şirketin meşru menfaat değerlendirmesinin yeterli bir dengeleme analizi içermediği ve ilgili kişilere sunulan aydınlatmaların kolay erişilebilir, anlaşılır ve yeterince şeffaf olmadığı belirtildi. Garante ayrıca kamu görevlilerinin verilerinin sistemden çıkarılmasına yönelik filtrelerin yetersiz olduğunu ve **tasarımdan itibaren veri koruma yükümlülüğünün yerine getirilmediğini** tespit etti. Buna ek olarak, İtalya'daki ilgili kişilere ait hukuki dayanak olmaksızın işlenen verilerin işlenmesinin durdurulmasına ve silinmesine karar verildi.

İlgili karara ilişkin detaylara [buradan](#) ulaşabilirsiniz.

Macaristan Veri Koruma Otoritesi, e-ticaret şirketine aydınlatma yükümlülüklerini yerine getirmemesi nedeniyle 15 milyon HUF ceza verdi.

Macaristan Veri Koruma Otoritesi (NAIH), bir e-ticaret şirketinin müşterilerinin kişisel verilerinin işlenmesine ilişkin yeterli ve anlaşılır bilgilendirme yapmaması nedeniyle **15 milyon HUF (yaklaşık 41.500 Euro) idari para cezası uygulanmasına** karar verdi. NAIH, Ocak 2020-Kasım 2025 dönemini inceleyerek şirketin farklı tarihlerde yürürlükte bulunan birden fazla aydınlatma metni ve farklı belgeler aracılığıyla kişisel veri işleme faaliyetlerine ilişkin bilgi sunduğunu tespit etti. Belgelerde yer alan bilgilerin birbiriyile **çelişkili, eksik ve dağınık olması nedeniyle şeffaflık ilkesinin ihlal edildiği** değerlendirildi. Otorite ayrıca, her bir veri işleme faaliyeti bakımından işleme amaçları ve hukuki sebeplerin, kişisel verilerin aktarılacağı alıcıların ve saklama sürelerinin yeterince açık şekilde belirtilmediğini tespit etti. Bunun yanı sıra, internet sitesinde kişisel verilerin Amerika Birleşik Devletleri'ne aktarılıp aktarılmadığı konusunda da çelişkili bilgilere yer verildiği belirtildi. NAIH, GDPR'ın 5(1)(a), 12(1), 13(1) ve 13(2). maddelerinin ihlal edildiğine karar vererek idari para cezasının yanı sıra şirketin internet sitesindeki ilgili veri koruma düzenlemelerini GDPR'a uygun hale getirmesine hükmetti.

İlgili karara ilişkin detaylara [buradan](#) ulaşabilirsiniz.



Dünyadaki Gelişmeler

Güncel Kararlar

Hollanda Veri Koruma Otoritesi, Uber'e otomatik karar alma süreçleri nedeniyle 824,99 milyon Euro ceza verdi.

Hollanda Veri Koruma Otoritesi (AP), Uber'in sürücüler hakkında insan müdahalesi olmaksızın otomatik kararlar alması ve sürücülerini bu süreçler hakkında yeterince bilgilendirmemesi nedeniyle **824,99 milyon Euro idari para cezası** uygulanmasına karar verdi. AP'nin incelemesine göre Uber, 2018-2022 yılları arasında sürücülerin davranışlarını ve müşteri değerlendirmelerini yazılım aracılığıyla takip etti. Dolandırıcılık şüphesi veya düşük müşteri puanları tespit edildiğinde bazı sürücü hesapları otomatik olarak geçici süreyle devre dışı bırakılırken, düşük puanların devam ettiği durumlarda hesaplar kalıcı olarak kapatılabilir. Bu süreçlerde yeterli insan müdahalesinin bulunmadığı ve kararların sürücülerin gelir elde etme imkanlarını doğrudan etkilediği belirtildi. AP ayrıca, **sürücülerin otomatik karar alma mekanizmaları hakkında yeterince bilgilendirilmediğini** tespit etti. Soruşturma, 171 Fransız sürücünün şikayeti üzerine Fransız Veri Koruma Otoritesi (CNIL) aracılığıyla başlatıldı ve Uber'in Avrupa merkezinin Hollanda'da bulunması nedeniyle Hollanda'daki tek durak mekanizması kapsamında yürütüldü. Uber karara itiraz ettiğini belirtirken, AP ihlallerin sona erdirildiğini açıkladı.

İlgili karara ilişkin detaylara [buradan](#) ulaşabilirsiniz.

İspanya Veri Koruma Otoritesi, yetkisiz SIM kart değişimi nedeniyle telekomünikasyon şirketine 200 bin Euro ceza verdi.

İspanya Veri Koruma Otoritesi (AEPD), bir telekomünikasyon şirketinin, müşteri adına yetkisiz bir üçüncü kişiye mükerrer SIM kart düzenlemesi nedeniyle GDPR'ın 6. maddesinde düzenlenen hukuka uygunluk ilkesini ihlal ettiğine karar vererek **200 bin Euro idari para cezası** uyguladı. Olayda, üçüncü bir kişi müşteriye ait telefon hattı için mükerrer SIM kart talebinde bulunarak müşterinin kimlik belgesinin kopyasını sundu. Şirket çalışanı, kimlik belgesini yalnızca görsel olarak kontrol ederek talepte bulunan kişiyi müşteri olarak kabul etti ve yeni SIM kartı düzenledi. Ancak daha sonra yapılan incelemede doğum yeri ve tarihi, adres ve ebeveyn isimleri gibi bilgilerin gerçek müşteri bilgileriyle uyuşmadığı tespit edildi. AEPD, **mükerrer SIM kart düzenlenmesinin kişisel veri işleme faaliyeti olduğunu ve yetkisiz kişinin talebinin mevcut sözleşme ilişkisi kapsamında hukuki dayanak oluşturamayacağını** belirtti. Şirketin kimlik doğrulama prosedürleri bulunmasına rağmen bunların etkin şekilde uygulanmamasını gerekli özen yükümlülüğünün ihlali olarak değerlendirdi. Otorite ayrıca, olayın üçüncü kişinin dolandırıcılık faaliyetinden kaynaklanmasının şirketin sorumluluğunu ortadan kaldırmayacağına hükmetti.

İlgili karara ilişkin detaylara [buradan](#) ulaşabilirsiniz.



Dünyadaki Gelişmeler

Güncel Kararlar

İrlanda Veri Koruma Komisyonu, sağlık kayıtlarının güvenli şekilde saklanmaması nedeniyle HSE'ye 645 bin Euro ceza verdi.

İrlanda Veri Koruma Komisyonu (DPC), Health Service Executive (HSE) tarafından kâğıt ortamındaki sağlık kayıtlarının uygun olmayan dış depolama tesislerinde saklanması nedeniyle toplam **645 bin Euro idari para cezası** uygulanmasına karar verdi. Soruşturma, 2023 yılında St. Loman's ve St. Conal's hastanelerinde saklanan kâğıt sağlık kayıtlarına yetkisiz kişilerin erişmesi üzerine başlatıldı. DPC'nin ülke genelinde gerçekleştirdiği 12 saha incelemesinde kayıtların küf, su ve hayvan dışkısı nedeniyle zarar gördüğü, bazı belgelerin kullanılamaz hale geldiği ve kişisel verilerin terk edilmiş binalar, kullanılmayan odalar ve uygun olmayan depolama alanlarında tutulduğu tespit edildi. DPC, **HSE'nin GDPR m.5(1)(f) ve m.32 kapsamında kişisel verilerin bütünlüğünü ve gizliliğini sağlayacak uygun güvenlik tedbirlerini uygulamadığına, ayrıca saklama süresiyle sınırlama ilkesini ihlal ettiğine** karar verdi. Kurumun bazı veri ihlallerini 72 saat içinde bildirmemesi ve ilgili kişilere ihlaller hakkında bildirimde bulunmaması da GDPR m.33 ve m.34 kapsamında ihlal olarak değerlendirildi. HSE'ye ayrıca tüm depolama tesislerinin denetlenmesi, gerekli olmayan kayıtların güvenli şekilde imha edilmesi ve kayıt yönetimi ile takip sistemlerinin güçlendirilmesi yönünde düzeltici emirler verildi.

İlgili karara ilişkin detaylara [buradan](#) ulaşabilirsiniz.

Fransa Veri Koruma Otoritesi, hasta verilerinin güvenliğinin sağlanmaması nedeniyle hastaneye 500 bin Euro ceza verdi.

Fransa Veri Koruma Otoritesi (CNIL), Hôpital Privé de la Loire hakkında, **elektronik hasta kayıt sisteminde yeterli güvenlik tedbirlerinin uygulanmaması ve veri ihlali sonrasında ilgili kişilerin tamamına bildirim yapılmaması nedeniyle 500 bin Euro idari para cezası** uygulanmasına karar verdi. Haziran 2025'te bir saldırgan, hastaneye bağlı bir hekimin kimlik bilgilerini ele geçirerek elektronik hasta kayıt sistemine erişti ve yaklaşık 524.867 hasta kaydını elde etti. Kayıtlarda kimlik ve iletişim bilgileri, sosyal güvenlik numaraları, bazı durumlarda kimlik belgeleri ve sağlık verileri bulunmuştu. CNIL incelemesinde, dış kullanıcıların sisteme yalnızca kullanıcı adı ve parola ile, VPN veya çok faktörlü kimlik doğrulama olmaksızın erişebildiği, sağlık çalışanlarının görevleriyle ilgisi olmayan hastaların kayıtlarına erişebildiği ve erişim loglarının yeterince etkin şekilde izlenmediği tespit edildi. CNIL ayrıca ihlal sonrasında dış sağlık çalışanlarına ortak bir parola atanmasını ve yazılım sağlayıcısının sisteme sürekli erişimini de güvenlik açısından yetersiz buldu. Bunun yanında, verileri ihlal edilen 202.246 güvenilir kişinin doğrudan bilgilendirilmemesi GDPR m.34'e aykırı değerlendirildi. Hastaneye ayrıca erişim kontrolleri ve log izleme süreçlerini güçlendirmesi yönünde düzeltici emirler verildi.

İlgili karara ilişkin detaylara [buradan](#) ulaşabilirsiniz.



www.dlattorneysatlaw.com

İstanbul’da bulunan DL Avukatlık Bürosu (“DL”), müvekkillerine genellikle kurumsal çözümler üzerinde odaklanmış kapsamlı hukuki hizmet sunmaktadır. DL Türkiye’nin önde gelen hukuk bürolarından biri olarak, ticari ve vergisel çözümler sunarak piyasadaki deneyimi ile müvekkillerine çözüm odaklı ve kişiye özel hukuki hizmet vermektedir.

Büromuzda hizmet veren avukatlar, Şirketler Hukuku – Birleşme & Devralmalar, Regüle Sektörler, Rekabet Hukuku, Kişisel Verilerin Korunması, Ticaret Hukuku, İş Hukuku, Tasfiye ve Kurumsal Yeniden Yapılandırma, Taşınmazlar, Davalar ve Vergi Uyuşmazlıkları dahil ve fakat bunlarla sınırlı olmamak üzere birçok alanında uzmanlaşmışlardır. DL Avukatlık Bürosu şirketler hukuku alanında karmaşık Birleşme & Devralma işlemlerinde hukuki danışmanlık hizmeti sunmak başta olmak üzere ortak girişim, yeniden yapılandırma ve genel şirketler hukuku konularına ilişkin hukuki görüş ve destek vermektedir. DL Avukatlık Bürosu gerek yerli gerekse yabancı şirket ve şirket gruplarına hizmet vermektedir.