EGE
ÇAKIRCA

Attorneys at Law

HAZİRAN'26

KVKK BÜLTENİ



KURUM KARARLARI VE DUYURULAR

GLOBAL GELİŞMELER

YARGI KARARLARI

Ege Çakırca Avukatlık Bürosu tarafından Haziran – Temmuz 2026 tarihleri kişisel verilerin korunması hukuku kapsamındaki meydana gelen hukuki gelişmelere ilişkin olarak kaleme alınan işbu bülten, yalnızca genel bilgilendirme amacı taşımakta olup, herhangi bir şekilde hukuki görüş, mütalaa veya danışmanlık hizmeti teşkil etmemektedir. Bu içerikler, belirli bir somut olaya uygulanmak üzere hazırlanmadığından, avukat-müvekkil ilişkisinin kurulmasına da yol açmaz.

Metinlerde yer alan bilgi ve değerlendirmelerin güncelliği, doğruluğu veya belirli bir amaca uygunluğu konusunda açık ya da zımni herhangi bir taahhüt veya garanti verilmemektedir.

Bu içeriklere dayanılarak tesis edilecek her türlü işlem öncesinde, somut olayın özellikleri çerçevesinde yetkin bir hukuk uzmanından profesyonel destek alınması gerekmektedir. Aksi yönde yapılacak işlemlerden doğabilecek her türlü risk ve sorumluluk münhasıran ilgili kişiye aittir.

İşbu içeriklerin kullanımından, yorumlanmasından veya bunlara dayanılarak alınan kararlardan kaynaklanabilecek doğrudan ya da dolaylı hiçbir zarar ve ziyandan dolayı firmamız, ortakları, çalışanları ve avukatları herhangi bir sorumluluk kabul etmez.

— Kurum Kararları ve Duyuruları

1 İş Yerlerinde Güvenlik Kamerası Kullanımına İlişkin Duyuru

KARAR TARİHİ:29.04.2026

YAYIM TARİHİ: 02.06.2026

Kişisel Verileri Koruma Kurumu tarafından yayımlanan duyuruda, iş yerlerinde güvenlik kameralarının iş sağlığı ve güvenliği, iş yeri güvenliğinin sağlanması ve suçun önlenmesi gibi amaçlarla kullanılabileceği belirtilmiştir. Bununla birlikte kamera kayıtlarının, çalışanlar ve iş yerinde bulunan diğer kişiler bakımından kişisel veri işleme faaliyeti niteliğinde olduğu vurgulanmıştır.

Bu kapsamda işverenlerin kamera kullanımında 6698 sayılı Kişisel Verilerin Korunması Kanunu'nda yer alan işleme şartlarına ve genel ilkelere dikkat etmesi, özellikle kayıtların belirli, açık ve meşru amaçlarla; bu amaçlarla bağlantılı, sınırlı ve ölçülü şekilde işlenmesi ve yalnızca gerekli süre kadar saklanması önem taşımaktadır.

Duyuruda, kamera sistemlerinin çalışanların devam durumunun veya performansının izlenmesi gibi farklı amaçlarla kullanılmaması gerektiği vurgulanmış; elverişlilik, gereklilik ve orantılılık kriterleri çerçevesinde değerlendirilmesi gerektiği ifade edilmiştir.

Kurum, giriş-çıkış alanları, depo ve kasa gibi güvenlik riski bulunan yerlerde kamera kullanımının somut olaya göre mümkün olabileceğini; ancak tuvalet, soyunma odası, mescit ve dinlenme alanı gibi mahremiyet beklentisinin yüksek olduğu yerlere kamera yerleştirilmemesi gerektiğini belirtmiştir. Ses kaydı alınması özel hayata daha ağır bir müdahale niteliğindedir.

Sonuç olarak, iş yerlerinde kamera kullanımı tamamen yasaklanmış değildir; ancak kullanımın meşru bir amaca dayanması, ölçülü olması ve ilgili kişilerin mahremiyet beklentisini ihlal etmemesi gerekmektedir. Kurum, yükümlülüklere aykırı hareket edilmesi hâlinde veri sorumluları hakkında idari para cezası da dâhil olmak üzere işlem tesis edilebileceğini belirtmiştir.

Duyurunun tam metnine buradan ulaşabilirsiniz.

2 Apartman ve Sitelerde Güvenlik Kamerası Kullanımına İlişkin Duyuru

YAYIM TARİHİ:08.06.2026

Kişisel Verileri Koruma Kurumu tarafından yayımlanan duyuruda, apartman ve sitelerde genel güvenliğin sağlanması, ortak alanların korunması ve hırsızlık veya mala zarar verme gibi fiillerin önlenmesi amacıyla güvenlik kamerası kullanılabileceği belirtilmiştir. Bununla birlikte, kamera sistemleri aracılığıyla kişilerin görüntülerinin kaydedilmesinin 6698 sayılı Kişisel Verilerin Korunması Kanunu kapsamında kişisel veri işleme faaliyeti niteliğinde olduğu vurgulanmıştır.

Apartman ve site ortak alanlarında kamera kullanımı, somut olayın özelliklerine göre meşru menfaat veya hakkın korunması gibi hukuki sebeplere dayanabilir; ancak her durumda Kanun'daki genel ilkelere uygun olmalıdır.

Duyuruda özellikle ölçülülük ve veri minimizasyonu ilkelerine dikkat çekilmiştir. Kameraların, apartman sakinlerinin makul mahremiyet beklentisini ihlal etmeyecek şekilde konumlandırılması; bağımsız bölümlerin içini görebilecek alanlara, merdiven boşluklarına veya gereksiz şekilde geniş alanları kaydedecek noktalara yerleştirilmemesi gerektiği belirtilmiştir.

Kurum ayrıca, kamera sistemlerinin yalnızca güvenlik amacıyla sınırlı olması gerektiğini; yüz tanıma, ses kaydı veya özel hayata daha ağır müdahale teşkil edebilecek özelliklerden kaçınılması gerektiğini ifade etmiştir. Asansörler ortak alan niteliğinde olmakla birlikte, dar ve kapalı alanlar olması nedeniyle bu alanlara kamera yerleştirilmesi hâlinde bunun gerekçesinin açıkça ortaya konulması gerektiği vurgulanmıştır.

Sonuç olarak, apartman ve sitelerde güvenlik kamerası kullanımı yasak değildir; ancak kullanımın amaçla bağlantılı, sınırlı, ölçülü ve hukuka uygun olması gerekmektedir. Kurum, bu yükümlülüklere aykırı hareket edilmesi hâlinde idari para cezası da dâhil olmak üzere işlem tesis edilebileceğini belirtmiştir.

Duyurunun tam metnine buradan ulaşabilirsiniz.

3 Belediyelerin Turistik Tanıtım Amaçlı Canlı Yayınlarına İlişkin Kamuoyu Duyurusu

YAYIM TARİHİ:23.06.2026

Kişisel Verileri Koruma Kurumu tarafından yayımlanan duyuruda, bazı belediyeler tarafından turistik tanıtım amacıyla cadde, meydan, park ve sahil gibi alanlara yerleştirilen kameraların görüntülerinin belediye internet siteleri üzerinden canlı yayımlanmasına ilişkin çok sayıda ihbar ve şikâyetin Kuruma intikal ettiği belirtilmiştir.

Kurum tarafından yapılan incelemelerde, söz konusu canlı yayınlarda gerçek kişilerin yüzlerinin göründüğü ve araç plakalarının okunabildiği tespit edilmiştir. Bu kapsamda, görüntüler kaydedilmese dahi internet üzerinden herkesin erişimine açık şekilde yayımlanmasının, kişisel verileri erişilebilir kılması nedeniyle kişisel veri işleme faaliyeti niteliğinde olduğu vurgulanmıştır.

Duyuruda, belediyelerin turizm ve tanıtım faaliyetleri yürütme yetkisi bulunmakla birlikte, bu yetkinin kişilerin kimliklerinin tespit edilebildiği canlı kamera yayınlarını doğrudan hukuka uygun hâle getirmediği ifade edilmiştir. Ayrıca söz konusu yayınların, yetkili kamu makamlarınca yürütülen kamusal alan güvenliği izleme faaliyetleri kapsamında değerlendirilemeyeceği belirtilmiştir.

Kurum, meydan, yürüyüş yolu, oturma alanı ve kumsal gibi kişilerin sosyalleştiği alanların canlı yayımlanmasının özel hayata saygı hakkına müdahale oluşturabileceğine dikkat çekmiştir. Görüntülerin internet üzerinden sınırsız sayıda kişi tarafından erişilebilir olması ise kötüye kullanım ve telafisi güç zarar riski doğurmaktadır.

> Sonuç olarak Kurum, belediyelerin turizm ve tanıtım amacıyla gerçek kişilerin kimliklerinin tespit edilmesine yol açan ve geçerli bir hukuki sebebe dayanmayan mevcut canlı yayın faaliyetlerini ivedilikle durdurmaları gerektiğini belirtmiştir. Aynı amaca, kişilerin tanımlanmasına imkân vermeyen görüntüleme yöntemleri veya kişisel veri içermeyen görsel materyaller gibi daha az müdahaleci alternatiflerle ulaşılması gerektiği vurgulanmıştır.

Duyurunun tam metnine buradan ulaşabilirsiniz.

4 Kaza Mağdurlarının Kişisel Verilerinin İşlenmesine İlişkin İlke Kararı

KARAR TARİHİ:20.05.2026
YAYIM TARİHİ:01.07.2026

Kişisel Verileri Koruma Kurulu kararına konu süreçte, kaza mağdurlarının rızaları dışında arandığı, kendilerine vekâlet vermeleri hâlinde tazminat alacaklarının takip edilebileceğinin söylendiği ve bazı durumlarda mağdurlar adına talimat alınmaksızın işlem yapıldığı yönünde çok sayıda ihbar ve şikâyet Kuruma iletilmiştir.

Kararda, Avukatlık Kanunu, Sigortacılık Kanunu ve ilgili meslek kuralları çerçevesinde; hasar danışmanlık şirketleri veya benzeri adlarla faaliyet gösteren kişi ve kuruluşların, hukuka aykırı şekilde tazminat alacaklarını takip etmelerinin idari ve cezai sorumluluk doğurabileceği belirtilmiştir.

> Kurulun kişisel verilerin korunması hukuku bakımından temel vurgusu, kaza mağdurlarına ait kişisel verilerin yalnızca hukuka uygun, belirli ve sınırlı amaçlarla işlenebileceğidir. Kaza sonrası adli ve idari süreçlerin yürütülmesi, tedavi, hasar tespiti, araç onarımı ve sigortacılık işlemleri kapsamında veri işlenmesi mümkün olmakla birlikte; bu verilerin amacı dışında kullanılması, yetkisiz kişilerle paylaşılması veya hukuka aykırı şekilde elde edilmesi KVKK kapsamında ihlal teşkil edebilecektir.

Kararda sigorta eksperlerinin kişisel veri işleme faaliyetleri de ayrıca ele alınmıştır. Eksperlerin, hasar tespiti, raporlama ve tazminat süreçleriyle sınırlı olmak üzere kişisel veri işleyebileceği; ancak görevleri kapsamında edindikleri verileri yetkisiz üçüncü kişilerle paylaşmaları hâlinde KVKK'ya aykırılığın gündeme gelebileceği belirtilmiştir.

> Sonuç olarak Kurul, sigortacılık, hasar yönetimi, ekspertiz, sağlık hizmetleri ve avukatlık faaliyetleri bakımından kaza mağdurlarına ait kişisel verilerin işlenmesinde veri minimizasyonu, amaçla sınırlılık, erişim kontrolü, yetki yönetimi ve veri güvenliği yükümlülüklerine dikkat edilmesi gerektiğini ortaya koymuştur. Yükümlülüklere aykırı hareket eden veri sorumluları hakkında KVKK kapsamında idari yaptırım uygulanabileceği gibi, somut olayın niteliğine göre Cumhuriyet savcılıklarına suç duyurusunda bulunulması da gündeme gelebilecektir.

Kararın tam metnine buradan ulaşabilirsiniz.

5 Biyometrik Verilerle Mesai Takibi Hakkında İlke Kararı

KARAR TARİHİ:29.04.2026
YAYIM TARİHİ:01.07.2026



Kurul, parmak izi, yüz tanıma, iris ve retina taraması gibi biyometrik verilerin özel nitelikli kişisel veri olduğunu; mesai takibinin biyometrik veriyle yapılmasını açıkça öngören bir kanuni düzenleme bulunmadığını belirtmiştir.

Kararda, işçi-işveren ilişkisindeki güç dengesizliği nedeniyle açık rızanın geçerliliğinin tartışmalı olabileceği; ayrıca kart, PIN, RFID/NFC kimlik kartı veya imza çizelgesi gibi daha az müdahaleci alternatiflerin bulunduğu vurgulanmıştır.

Bu nedenle Kurul, mesai takibi amacıyla biyometrik veri işlenmesinin ölçülülük ilkesine uygun olmayabileceğini ifade etmiş; işverenlerin mevcut uygulamalarını hukuki sebep, veri minimizasyonu ve veri güvenliği ilkeleri çerçevesinde yeniden değerlendirmesi gerektiğine işaret etmiştir.

Kararın tam metnine buradan ulaşabilirsiniz.

6 Rekabet Kurumu'ndan Meta Hakkında Soruşturma ve Geçici Tedbir Kararı

Kurul, üçüncü taraf üretken yapay zekâ sohbet robotları ve asistanlarının WhatsApp üzerinden hizmet sunmasının engellenmesini hâkim durumun kötüye kullanılması bakımından ciddi bir bulgu olarak değerlendirmiş; nihai karar verilinceye kadar telafisi güç zararların önlenmesi amacıyla Meta hakkında geçici tedbir uygulanmasına hükmetmiştir. Bu kapsamda Meta'nın, üçüncü taraf yapay zekâ sağlayıcılarının WhatsApp üzerinden hizmet sunmasını fiilî veya ekonomik olarak zorlaştırmayacak koşulları tesis etmesi gerektiği belirtilmiştir. Karar, dijital platformların kendi yapay zekâ hizmetlerini platformlarına entegre ederken rakip sağlayıcıların pazara erişimini sınırlayıp sınırlamadığının rekabet hukuku bakımından giderek daha yakından incelendiğini göstermektedir.

Kararın tam metnine buradan ulaşabilirsiniz.

— YARGI KARARLARI

1 Alenileştirilmiş Kişisel Verilerin İşlenmesine İlişkin KVKK İdari Para Cezası Hakkında AYM İhlal Kararı

KARAR TARİHİ: 27.01.2026
YAYIM TARİHİ: 16.06.2026
2020/32193

Başvuruya konu olayda, sigortacılık alanında faaliyet gösteren başvurucu şirket; ilgili kişinin ad, soyad ve telefon numarası bilgilerini kamuya açık bir internet sitesinden elde ettiğini ve bu verilerin ilgili kişi tarafından alenileştirildiğini ileri sürmüştür. Buna karşılık Kişisel Verileri Koruma Kurulu, söz konusu verilerin alenileştirme amacı dışında ticari randevu/teklif amacıyla kullanıldığını değerlendirerek başvurucu hakkında 6698 sayılı Kanun'un 12'nci ve 18'inci maddeleri kapsamında idari para cezası uygulanmasına karar vermiştir.

AYM, 6698 sayılı Kanun'un 5'inci maddesinin ikinci fıkrasının (d) bendinde ilgili kişinin kendisi tarafından alenileştirilmiş kişisel verilerin açık rıza aranmaksızın işlenebileceğinin düzenlendiğini; ancak Kanun'da "alenileştirme amacı", "alenileştirme amacıyla sınırlı kullanım" veya "amaç dışı kullanım" şeklinde açık bir yaptırım ölçütü bulunmadığını belirtmiştir. Mahkeme, kanunda açıkça düzenlenmeyen bir yükümlülüğün idari yorum yoluyla genişletilerek yaptırıma esas alınmasının öngörülebilirlik ve hukuki güvenlik ilkeleriyle bağdaşmadığını değerlendirmiştir.

Bu kapsamda AYM, başvurucu şirket hakkında uygulanan idari para cezasının Anayasa'nın 38'inci maddesinde güvence altına alınan suçta ve cezada kanunilik ilkesini ihlal ettiğine karar vermiştir. Karar, alenileştirilmiş kişisel verilerin her durumda sınırsız biçimde ticari amaçlarla kullanılabileceği anlamına gelmemekle birlikte; KVKK kapsamında idari yaptırım uygulanabilmesi için yaptırıma esas yükümlülüğün kanun düzeyinde açık, belirli ve öngörülebilir şekilde düzenlenmesi gerektiğini ortaya koymaktadır.

Kararın tam metnine buradan ulaşabilirsiniz.

2 KVKK Kapsamında Verilen İdari Para Cezalarında Kanunilik İlkesine İlişkin AYM Kararı

KARAR TARİHİ: 27.01.2026
YAYIM TARİHİ: 16.06.2026
2020/3219

Başvuruya konu olayda, ilgili kişi sigortacılık faaliyetleri kapsamında randevu talebiyle aranması üzerine, kişisel verilerinin açık rızası olmaksızın temin edilerek işlendiği iddiasıyla Kişisel Verileri Koruma Kurumuna başvurmuştur. Başvurucu şirket ise ilgili kişinin ad, soyad ve telefon numarası bilgilerinin bir internet sitesinden elde edildiğini, söz konusu verilerin ilgili kişi tarafından alenileştirildiğini ve bu nedenle KVKK m.5/2(d) kapsamında açık rıza aranmaksızın işlenebileceğini ileri sürmüştür.

Kişisel Verileri Koruma Kurulu, ilgili verilerin internet sitesinde yer alması ihtimalinde dahi, bu verilerin şirket tarafından alenileştirilme amacıyla uyumlu şekilde kullanılmadığı kanaatine varmıştır. Bu doğrultuda Kurul, kişisel verilerin hukuka aykırı işlenmesini önlemeye yönelik gerekli teknik ve idari tedbirlerin alınmadığı gerekçesiyle idari para cezası uygulanmasına karar vermiştir.

> Anayasa Mahkemesi ise değerlendirmesinde, ad, soyad ve telefon numarası bilgilerinin kişisel veri niteliğinde olduğunu ve kişisel verilerin kural olarak ilgili kişinin açık rızası olmaksızın işlenemeyeceğini belirtmiştir. Bununla birlikte Mahkeme, KVKK'da "alenileştirme amacı" kavramına, alenileştirilen kişisel verilerin bu amaca aykırı kullanılmasına veya bu aykırılığın ayrıca yaptırıma bağlanmasına ilişkin açık bir düzenleme bulunmadığını tespit etmiştir.

Bu kapsamda Anayasa Mahkemesi, kanunda açıkça düzenlenmeyen "alenileştirme amacı" kavramına dayanılarak idari para cezası uygulanmasının başvurucu bakımından öngörülebilir olmadığı sonucuna varmıştır. Mahkeme ayrıca, başvurucunun veri sorumlusu sıfatının hangi gerekçelerle kabul edildiği ve verilerin ilk yayımlandığı internet sitesinin sorumluluğunun bulunup bulunmadığı hususlarının da yeterli açıklıkta ortaya konulmadığını değerlendirmiştir.

> Sonuç olarak Anayasa Mahkemesi, idari para cezaları bakımından da uygulama alanı bulan suçta ve

cezada kanunilik ilkesinin ihlal edildiğine karar vermiştir. Karar, KVKK kapsamında idari yaptırım tesis edilirken yalnızca veri işleme faaliyetinin hukuka uygunluğunun değil, yaptırıma esas alınan fiilin kanuni dayanağının açık, belirli ve öngörülebilir olup olmadığının da ayrıca değerlendirilmesi gerektiğini göstermesi bakımından önem taşımaktadır.

Kararın tam metnine buradan ulaşabilirsiniz.

3 İstanbul 14. Asliye Ticaret Mahkemesi'nden Yabancı Mahkeme Kararlarının Tenfizi ve Yargılamada Yapay Zeka Kullanımına İlişkin Dikkat Çekici Karar

KARAR TARİHİ: 30.04.2026
E. 2025/976, K. 2026/413

Karara konu uyuşmazlık, Hollanda'da açılması planlanan bir göz kliniğine ilişkin danışmanlık sözleşmesinden kaynaklanmıştır. Hollanda mahkemelerince davacı lehine verilen kararın Türkiye'de icra kabiliyeti kazanması amacıyla tanıma ve tenfiz davası açılmıştır.

Mahkeme, 5718 sayılı Milletlerarası Özel Hukuk ve Usul Hukuku Hakkında Kanun kapsamında tenfiz şartlarını değerlendirmiştir. Bu kapsamda yabancı mahkeme kararının kesinleşmesi, gerekli belgelerin sunulması, görevli mahkeme, yabancılık teminatı, mütekabiliyet ve kamu düzenine aykırılık iddiaları ayrı ayrı incelenmiştir.

Kararda, tarafların tacir olması ve uyuşmazlığın ticari alacaktan kaynaklanması nedeniyle Asliye Ticaret Mahkemesi'nin görevli olduğu kabul edilmiştir. Ayrıca Türkiye ve Hollanda'nın taraf olduğu 1954 tarihli Hukuk Usulüne Dair Lahey Sözleşmesi uyarınca, Hollanda'da mukim davacı şirketin yabancılık teminatından muaf olduğu sonucuna varılmıştır.

Mahkeme, Türkiye ile Hollanda arasında tanıma ve tenfize ilişkin ikili bir anlaşma bulunmamasına rağmen, mütekabiliyet şartının yalnızca ahdî mütekabiliyetle sınırlı olmadığını belirtmiştir. Hollanda hukukundaki düzenlemeler ve güncel yargı kararları dikkate alınarak kanunî ve fiilî mütekabiliyetin mevcut olduğu kabul edilmiştir. Kamu düzeni itirazı bakımından ise yabancı mahkeme kararında yer alan cezai şartın, tarafların tacir sıfatı ve sözleşme serbestisi çerçevesinde Türk kamu düzenine açıkça aykırılık teşkil etmediği değerlendirilmiştir.

Kararın dikkat çeken bir diğer yönü, mahkemenin karar hazırlık sürecinde yabancı hukuk kaynaklarının teyidi ve çeviri desteği amacıyla yapay zekâ teknolojisinden teknik bir araç olarak yararlanıldığını açıkça belirtmesidir. Sonuç olarak Mahkeme, Hollanda mahkemesi kararının belirli hükümlerinin tenfizine, bazı hükümlerinin ise tanınmasına karar vermiştir. Karar, hem Türkiye-Hollanda arasındaki mütekabiliyet şartının yorumu hem de yargılamada yapay zekânın yardımcı teknik araç olarak kullanımı bakımından önem taşımaktadır.

Kararın tam metnine buradan ulaşabilirsiniz.

4 Anayasa Mahkemesi'nden E-Ticaret Aracı Hizmet Sağlayıcılarına İlişkin İptal Kararı

KARAR TARİHİ: 12.02.2026

Kararda, aracı hizmet sağlayıcıların ayıplı maldan kaynaklanan tüketici taleplerinden tamamen sorumsuz tutulmasının ve tüketici sözleşmeleri bakımından genel bir sorumsuzluk rejimi öngörülmesinin tüketicinin korunması ilkesiyle bağdaşmadığı değerlendirilmiştir. İptal hükümleri 02.03.2027 tarihinde yürürlüğe girecektir.

Karar, e-ticaret platformlarının her durumda satıcı veya sağlayıcı gibi sorumlu tutulacağı anlamına gelmemekle birlikte, platformların mutlak ve kategorik bir sorumsuzluk rejiminden yararlanamayacağını ortaya koymaktadır. Bu kapsamda platformun işlem üzerindeki rolü, mal veya hizmete ilişkin bilgi ve kontrol düzeyi, tüketici nezdinde yarattığı güven ile ödeme, teslimat, iade ve şikâyet süreçlerindeki etkisi sorumluluk değerlendirmesinde dikkate alınacaktır.

Kararın tam metnine buradan ulaşabilirsiniz.

5 AYM'den Dijital Deliller ve Kişisel Verilerin Korunmasına İlişkin Önemli Karar

KARAR TARİHİ: 12.02.2026



Anayasa Mahkemesi, 12.02.2026 tarihli kararıyla CMK'nın bilgisayarlarda, bilgisayar programlarında ve kütüklerinde arama, kopyalama ve elkoymaya ilişkin 134'üncü maddesini Anayasa'ya aykırı bularak iptal etmiştir.

Kararda, dijital materyallerde yer alan verilerin çok geniş kapsamlı kişisel veri içerebileceği; bu nedenle arama, kopyalama ve elkoyma işlemlerinin özel hayatın gizliliği ve kişisel verilerin korunması hakkına müdahale niteliğinde olduğu vurgulanmıştır. Mahkeme, dijital delil elde etme süreçlerinde yalnızca delile erişimin

değil; erişilen verilerin kapsamı, saklama süresi, imhası, ilgisiz verilerin ayrıştırılması ve veri güvenliğinin de açık kanuni güvencelere bağlanması gerektiğini belirtmiştir. Bu yaklaşım, KVKK'da yer alan amaçla sınırlılık, ölçülülük, veri minimizasyonu ve gerekli süre kadar muhafaza ilkeleriyle de paralellik göstermektedir.

Karar doğrudan KVKK kapsamında verilmiş bir Kurul kararı niteliğinde olmasa da, ceza yargılamasında dijital verilere müdahale edilirken kanunilik, ölçülülük ve etkili güvencelerin önemini ortaya koymaktadır. Bu yönüyle karar, dijital delillerin elde edilmesi ve kişisel verilerin korunması bakımından önemli bir içtihat niteliği taşımaktadır.

Kararın tam metnine buradan ulaşabilirsiniz.

— GLOBAL GELİŞMELER

1 Türkiye Yapay Zekâ Eylem Planını Açıkladı



Türkiye'nin yapay zekâ alanındaki yol haritasını ortaya koyan "Türkiye Yapay Zekâ Eylem Planı", Cumhurbaşkanı Recep Tayyip Erdoğan'ın katılımıyla İstanbul'da düzenlenen Türkiye Yapay Zekâ Zirvesi'nde açıklanmıştır. Eylem Planı; "fark et, istifade et, üret ve yönet" olmak üzere dört temel eksen üzerine inşa edilmiştir.

Eylem Planı kapsamında; Ulusal Yapay Zekâ Okuryazarlığı Programı'nın başlatılması, 81 ilde yapay zekâ okuryazarlığı atölyeleri kurulması ve iki yıl içinde 5 milyon vatandaşa eğitim verilmesi hedeflenmektedir. Ayrıca 10 bin ileri düzey yapay zekâ uzmanı ile 100 bin yapay zekâ uygulama profesyonelinin yetiştirilmesi; sağlık, tarım, savunma ve elektronik ticaret başta olmak üzere en az 2 bin kamu veri setinin Ulusal Veri Kütüphanesi üzerinden erişime açılması öngörülmektedir.

Plan, veri merkezi altyapısı ve yerli yapay zekâ teknolojileri bakımından da önemli hedefler içermektedir. Bu kapsamda; 2030 yılına kadar Türkiye'nin veri merkezi kurulu gücünün en az 1 gigavata çıkarılması, veri merkezi, bulut ve yapay zekâ altyapılarında en az 10 milyar dolarlık özel sektör ağırlıklı kaynağın harekete geçirilmesi ve Türkçe büyük dil modeli çalışmalarının desteklenmesi planlanmaktadır. Eylem Planı'nda ayrıca; kullanıcı haklarını koruyan, yatırımcılara öngörülebilirlik sağlayan ve orantılı risk yaklaşımına dayanan bir düzenleyici çerçeve oluşturulacağı ifade edilmiştir.

Duyurunun tam metnine buradan ulaşabilirsiniz.

2 İspanya, AB Yapay Zeka Tüzüğü'nün Uygulanmasına İlişkin Kanun Tasarısını Kabul Etti

İspanya Bakanlar Kurulu, AB Yapay Zekâ Tüzüğü'nü ("AI Act", Reg. (AB) 2024/1689) ulusal düzeyde uygulamaya geçiren "Yapay Zekânın İyi Kullanımı ve Yönetişimine İlişkin Organik Kanun Tasarısı"nı kabul ederek parlamentoya sevk etmiştir. Tasarı, AI Act ile paralel şekilde; yapay zekâ sistemlerinin risk temelli sınıflandırılması, yaptırım rejimi, insan denetimi, algoritmik şeffaflık, çocukların korunması ve veri mahremiyeti gibi temel güvenceleri ulusal hukuk düzeyinde somutlaştırmayı amaçlamaktadır.

> Tasarı, bazı yönleriyle AI Act'in mevcut metninden daha ileri bir yaklaşım benimsemektedir. Söz konusu yaklaşımlar üzerinde 7 Mayıs 2026 tarihinde AB düzeyinde siyasi mutabakata varılmış olmakla birlikte, düzenleme henüz resmî olarak AI Act metnine işlenmemiştir. Bu yönüyle İspanya, öncülüğünü yaptığı yaklaşımı ulusal tasarısına yansıtmıştır.

Tasarı ayrıca merkezi idare bakımından AI Act'in ötesine geçen bazı ek yükümlülükler öngörmektedir. AI Act, kamu kurumları için yüksek riskli sistemler bakımından temel hak etki değerlendirmesi yükümlülüğü getirirken; İspanya tasarısı, kamu kurumlarında mevzuata uyumu koordine edecek ve kamu projeleri ile ihalelerde danışmanlık yapacak "yapay zekâ sorumlusu" rolünü ve idari süreçlerde kullanılan tüm yapay zekâ sistemlerini kapsayan daha geniş bir envanter yükümlülüğünü öngörmektedir.

La Moncloa duyurusunun tam metnine buradan ulaşabilirsiniz.

3 Avrupa Parlamentosu, AI Act Uyum Takvimini Değiştiren Düzenlemeyi Kabul Etti

Avrupa Parlamentosu, 16.06.2026 tarihinde AB Yapay Zekâ Tüzüğü'nde ("AI Act") değişiklik öngören dijital omnibus düzenlemesini 423 lehte, 57 aleyhte ve 174 çekimser oyla kabul etmiştir. Düzenleme; bazı yüksek riskli yapay zekâ sistemlerine ilişkin yükümlülüklerin uygulama tarihlerini ertelemekte, yapay zekâ ile üretilen içeriklerin etiketlenmesine ilişkin takvimi netleştirmekte ve rıza dışı mahrem veya cinsel içerik üreten yapay zekâ sistemlerine açık bir yasak getirmektedir. Düzenlemenin yürürlüğe girmesi için AB Konseyi tarafından da resmen kabul edilmesi gerekmektedir.

Yeni takvime göre, yapay zekâ ile üretilen içeriklerin makine tarafından okunabilir şekilde etiketlenmesine ilişkin yükümlülükler; 2 Ağustos 2026'dan önce piyasaya sürülen sistemler bakımından 02.12.2026 tarihinde uygulanmaya başlayacaktır. Aynı tarihten itibaren, çocuk cinsel istismarı materyali üreten veya kimliği belirlenebilir kişileri rızaları dışında

mahrem ya da cinsel içeriklerde gösteren görüntü, video veya ses üreten yapay zekâ sistemleri de yasak kapsamına alınacaktır.

Yüksek riskli yapay zekâ sistemlerine ilişkin yükümlülüklerin uygulama tarihi ise; bağımsız yüksek riskli sistemler bakımından 02.12.2027'ye, AB sektörel ürün güvenliği mevzuatı kapsamındaki ürünlere güvenlik bileşeni olarak entegre edilen yapay zekâ sistemleri bakımından ise 02.08.2028'e ertelenmiştir.

Düzenleme ayrıca; makine ürünlerine ilişkin çakışan yükümlülüklerin azaltılması, "güvenlik bileşeni" kavramının netleştirilmesi, önyargı tespiti ve düzeltimi için gerekli güvenceler altında kişisel veri işlenebilmesi, KOBİ kolaylıklarının küçük ve orta ölçekli şirketlere genişletilmesi ve bazı genel amaçlı yapay zekâ sistemleri bakımından AB Yapay Zekâ Ofisi'nin uygulama rolünün sadeleştirilmesi gibi değişiklikleri de içermektedir.

Avrupa Parlamentosu duyurusunun tam metnine buradan ulaşabilirsiniz.

4 Almanya'da Bundesnetzagentur, Avrupa Veri Yasası'nın Yetkili Uygulama Otoritesi Oldu

Almanya'da Veri Yasası Uygulama ve Yürütme Kanunu'nun ("DADG") yürürlüğe girmesiyle birlikte Bundesnetzagentur, 30.05.2026 tarihi itibarıyla Avrupa Veri Yasası'nın ("Data Act") Almanya'daki uygulanmasından sorumlu yetkili otorite hâline gelmiştir. Kurum, Data Act'e ilişkin tüm sorular bakımından tek temas noktası olarak görev yapacak; piyasa aktörlerini destekleyecek ve yeni kurallara uyumu denetleyecektir.

Bundesnetzagentur'un yeni görevleri arasında; veri koruma konularında Federal Veri Koruma ve Bilgi Özgürlüğü Komiseri ile, ayrıca Avrupa Komisyonu ve Avrupa Veri İnovasyon Kurulu ile ulusal ve sınır ötesi iş birliği yürütmek yer almaktadır. Kurum ayrıca; Almanya'daki uyuşmazlık çözüm mercilerini sertifikalandıracak, veri ekonomisindeki teknolojik ve ekonomik gelişmeleri izleyecek, veri birlikte çalışabilirliğini artırmaya yönelik standardizasyon çalışmalarına katkı sunacak ve bulut sağlayıcıları arasında geçişi kolaylaştırmaya ilişkin kurallara uyumu denetleyecektir.

Avrupa Veri Yasası; bağlantılı araçlar, akıllı ev cihazları ve endüstriyel makineler gibi ürünlerden elde edilen verilere erişim ile bu verilerin kullanımı bakımından tüketicilere ve işletmelere daha fazla kontrol sağlamayı amaçlamaktadır. Düzenleme; otomotiv, makine, tarım ve sağlık başta olmak üzere birçok sektörü kapsamakta, ayrıca istisnai ihtiyaç hâllerinde kamu kurumlarına veri sağlanmasına ve bulut sağlayıcıları arasında geçişin kolaylaştırılmasına ilişkin hükümler içermektedir.

Bundesnetzagentur duyurusunun tam metnine buradan ulaşabilirsiniz.

5 Avrupa Komisyonu'ndan Yapay Zekâ ile Üretilen İçeriklerin Etiketlenmesine İlişkin Uygulama Kuralları

Avrupa Komisyonu, 10.06.2026 tarihinde yapay zekâ ile üretilen içeriklerin işaretlenmesi ve etiketlenmesine ilişkin nihai Uygulama Kurallarını yayımlamıştır. Gönüllü nitelikteki Kurallar; üretken yapay zekâ sistemi sağlayıcılarının ve kullanıcılarının, AB Yapay Zekâ Tüzüğü'nün ("AI Act") 02.08.2026 tarihinde uygulanmaya başlayacak şeffaflık yükümlülüklerine uyum sağlamalarına yönelik pratik adımlar içermektedir.

AI Act kapsamında; deepfake içerikler ile kamu yararını ilgilendiren konularda yayımlanan, yapay zekâ tarafından üretilmiş veya yapay zekâ ile manipüle edilmiş metinlerin açıkça etiketlenmesi, ayrıca kullanıcıların chatbot gibi etkileşimli yapay zekâ sistemleriyle iletişim kurdukları konusunda bilgilendirilmesi öngörülmektedir. Bu yükümlülükler; aldatılma, manipülasyon ve dezenformasyon risklerinin azaltılması bakımından önem taşımaktadır.

Avrupa Komisyonu duyurusunun tam metnine buradan ulaşabilirsiniz.

6 Avrupa Komisyonu'ndan Temu'ya DSA kapsamında 200 Milyon Euro Para Cezası

Avrupa Komisyonu, 28.05.2026 tarihinde Temu'ya, Dijital Hizmetler Yasası ("DSA") kapsamındaki risk değerlendirme yükümlülüklerini ihlal ettiği gerekçesiyle 200 milyon Euro idari para cezası verdiğini açıklamıştır. Komisyon, Temu'nun platformunda yasa dışı ürünlerin sunulmasından kaynaklanan sistemik riskleri yeterince tespit etmediğini, analiz etmediğini ve değerlendirmediğini belirtmiştir.

Komisyona göre Temu'nun 2024 yılı risk değerlendirmesi, platformun kendi hizmetine özgü somut veriler yerine genel e-ticaret sektörü risklerine dayanmış; AB'deki tüketicilerin yasa dışı ürünlerle karşılaşma ihtimalini olduğundan

düşük tahmin etmiş ve tavsiye sistemleri ile influencer destekli ürün tanıtımlarının bu riskleri nasıl artırabileceğini yeterince değerlendirmemiştir. Soruşturma kapsamında yapılan testlerde ise bazı şarj cihazları ve bebek oyuncaklarının temel güvenlik gerekliliklerini karşılamadığı tespit edilmiştir.

Temu'nun, DSA'nın 75'inci maddesi uyarınca 28.08.2026 tarihine kadar ihlalin giderilmesine yönelik bir eylem planı sunması gerekmektedir. Uyumsuzluğun devam etmesi hâlinde şirket hakkında dönemsel para cezaları uygulanabilecektir. Karar; çevrim içi pazaryerleri bakımından ürün güvenliği, tüketicinin korunması, algoritmik tavsiye sistemleri ve platform yönetişimi alanlarında düzenleyici denetimin güçlendiğini göstermektedir.

Avrupa Komisyonu duyurusunun tam metnine buradan ulaşabilirsiniz.

7 Avrupa Parlamentosu Araştırma Servisi'nden Sosyal Medya için Asgari Yaş Tartışmasına İlişkin Brifing

Avrupa Parlamentosu Araştırma Servisi ("EPRS"), Haziran 2026 tarihli brifinginde çocukların sosyal medya kullanımına ilişkin asgari yaş sınırı tartışmalarını değerlendirmiştir. Brifingde UNICEF verilerine göre yaklaşık 40 ülkede sosyal medyaya erişim için yaşa dayalı sınırlamaların tartışıldığı, önerildiği veya uygulanmaya başlandığı belirtilmiştir. Ancak Avustralya örneğinde görüldüğü üzere, sosyal medya hesaplarının kapatılmasına rağmen birçok çocuğun platformlara erişmeye devam etmesi, bu tür yasakların tek başına etkili olmayabileceğini göstermektedir.

EPRS, sosyal medya için asgari yaş tartışmasının merkezinde yaş doğrulama ve yaş tahmini teknolojilerinin bulunduğunu vurgulamaktadır. Bu teknolojiler çocukların korunması bakımından önemli görülmekle birlikte; mahremiyet, yanlış dışlama, ayrımcılık, biyometrik veri işleme ve kolayca aşılabilme gibi riskler barındırmaktadır. Bu nedenle AB düzeyinde, parçalı ulusal düzenlemeler yerine gizliliği koruyan, ölçülü, güvenilir ve ayrımcı olmayan ortak bir yaş doğrulama çerçevesinin geliştirilmesi tartışılmaktadır.

Brifingde ayrıca, mevcut AB hukukunun sosyal medya için tek tip bir asgari yaş öngörmediği; ancak GDPR, Dijital Hizmetler Yasası ("DSA"), Avrupa Dijital Kimlik Çerçevesi ve Görsel-İşitsel Medya Hizmetleri Direktifi'nin çocukların çevrim içi korunması bakımından önemli rol oynadığı ifade edilmiştir. 6698 sayılı Kişisel Verilerin Korunması Kanunu bakımından ise yaş doğrulama sistemlerinde çocuklara ait kişisel verilerin işlenmesi; amaçla sınırlılık, veri minimizasyonu, ölçülülük, aydınlatma ve veri güvenliği ilkeleri çerçevesinde dikkatle değerlendirilmelidir.

EPRS brifinginin tam metnine buradan ulaşabilirsiniz.

8 Birleşik Krallık Veri Koruma Otoritesi'nden ("ICO") Sağlık Sektöründe Hasta Verilerine Yetkisiz Erişim Uyarısı

ICO, 22.06.2026 tarihinde yayımladığı "Curiosity is not an excuse: protecting patient data in healthcare" başlıklı yazısında, sağlık sektöründe hasta kayıtlarına yetkisiz erişim riskine dikkat çekmiştir. ICO; sağlık çalışanlarının görevleri gereği hasta kayıtlarına erişebilmesinin, her durumda bu kayıtları inceleyebilecekleri anlamına gelmediğini, erişimin mutlaka meşru, görevle bağlantılı ve gerekli olması gerektiğini vurgulamıştır.

ICO'ya göre; özellikle kamuoyunda geniş yankı uyandıran olaylar, ciddi suçlar veya toplumsal hassasiyet yaratan vakalar sonrasında, sağlık çalışanlarının merak saikiyle ilgili kişilerin sağlık kayıtlarına erişme riski artabilmektedir. Ancak bu tür erişimler açıkça hukuka aykırı olup; disiplin yaptırımları, mesleki akreditasyonun kaybı ve bazı durumlarda cezai süreçler dâhil olmak üzere ciddi sonuçlar doğurabilir.

Bu değerlendirme, 6698 sayılı Kişisel Verilerin Korunması Kanunu ("KVKK") bakımından da önem taşımaktadır. Sağlık verileri, KVKK m.6 kapsamında özel nitelikli kişisel veri niteliğindedir. Bu nedenle sağlık verilerinin işlenmesi ve bu verilere erişim; ancak kanunda öngörülen işleme şartlarının varlığı hâlinde ve belirli bir görev, yetki ve amaçla sınırlı olarak mümkündür. Teknik olarak erişim yetkisinin bulunması, hukuken erişim hakkının bulunduğu anlamına gelmemektedir.

KVKK m.12 uyarınca veri sorumluları; kişisel verilerin hukuka ve çalışanlarına somut örneklerle desteklenen veri koruma eğitimleri vermesi önem taşımaktadır.

ICO ayrıca, kamuoyunun dikkatini çeken olaylar sonrasında hasta mahremiyeti ve veri koruma yükümlülüklerinin üst yönetim tarafından personele derhâl hatırlatılmasının etkili bir önleyici tedbir olabileceğini belirtmiştir. Bu yaklaşım, sağlık kuruluşlarında veri güvenliği kültürünün yalnızca teknik kontrollerle değil,

güçlü bir kurumsal farkındalık ve hesap verebilirlik anlayışıyla da desteklenmesi gerektiğini göstermektedir.

Sonuç olarak ICO'nun açıklaması, sağlık verilerine erişimde temel ölçütün "erişebiliyor olmak" değil, "görev gereği ve hukuken erişmesi gerekiyor olmak" olduğunu ortaya koymaktadır. KVKK bakımından da, sağlık verilerinin özel nitelikli kişisel veri niteliği dikkate alındığında, sağlık kuruluşlarının hasta kayıtlarına erişim süreçlerini asgari yetki, amaçla sınırlılık ve düzenli denetim ilkeleri çerçevesinde yönetmesi gerekmektedir.

ICO'nun konuya ilişkin yazısının tam metnine buradan ulaşabilirsiniz.

9 CNIL'den Bulut Bilişim Hizmetlerinde GDPR Kapsamındaki Rol ve Sorumluluklara İlişkin Rehber

Fransa Veri Koruma Otoritesi ("CNIL"), 28.05.2026 tarihinde bulut bilişim hizmetlerinde tarafların GDPR kapsamındaki rollerinin belirlenmesine ilişkin bir rehber yayımlamıştır. Rehberde, bulut bilişim ekosisteminde veri sorumlusu, ortak veri sorumlusu ve veri işleyen sıfatlarının doğru belirlenmesinin; sözleşmesel yükümlülükler, veri güvenliği tedbirleri ve ilgili kişi haklarının kullanımı bakımından önem taşıdığı vurgulanmıştır.

CNIL'e göre bulut hizmetlerinde rol tespiti, IaaS, PaaS ve SaaS modellerindeki farklı kontrol seviyeleri, müşterinin hizmeti yapılandırma imkânı ve hizmet sağlayıcının süreçler üzerindeki fiilî etkisi dikkate alınarak her somut olay özelinde yapılmalıdır. Genel olarak bulut hizmetini kendi amaçları doğrultusunda kullanan müşteri veri sorumlusu, verileri müşterinin talimatları doğrultusunda işleyen bulut hizmet sağlayıcısı ise veri işleyen olarak kabul edilmektedir. Ancak sağlayıcının hizmet iyileştirme, izleme araçları veya çerezler gibi yollarla kendi amaçları doğrultusunda veri işlemesi hâlinde veri sorumlusu ya da ortak veri sorumlusu olarak nitelendirilmesi mümkündür.

Rehber, 6698 sayılı Kişisel Verilerin Korunması Kanunu bakımından da bulut hizmeti alan taraflar ile hizmet sağlayıcıları arasındaki rol ve sorumluluk dağılımının sözleşmesel ve operasyonel düzeyde açıkça belirlenmesi gerektiğini göstermektedir. Bu kapsamda veri işleme amaçları, talimat ilişkisi, güvenlik tedbirleri, alt işleyen kullanımı, saklama ve imha süreçleri, erişim yetkileri ve ilgili kişi başvurularının yönetimi gibi hususların netleştirilmesi önem taşımaktadır.

CNIL rehberinin tam metnine buradan ulaşabilirsiniz.

10 BM İnsan Hakları Ofisi'nden Çocukların Çevrim İçi Güvenliğine İlişkin 10 Rehber İlke

Birleşmiş Milletler İnsan Hakları Yüksek Komiserliği Ofisi ("OHCHR"), çocukların çevrim içi güvenliğinin sağlanmasına ilişkin "Getting Children's Safety Online Right" başlıklı rehber ilkeleri yayımlamıştır.

Rehberde, çocukların çevrim içi güvenliğinin yalnızca erişim yasakları veya genel sosyal medya sınırlamalarıyla sağlanamayacağı belirtilmektedir. Bunun yerine; platformların tasarımdan itibaren güvenli hâle getirilmesi, bağımlılık yaratıcı tasarım özelliklerinin ele alınması, çocuklara yönelik çevrim içi pazarlamanın sıkı şekilde düzenlenmesi ve çocukların ticari amaçlarla mikro hedeflemeye tabi tutulmasının engellenmesi önerilmektedir. Ayrıca şirketlerin çocuk hakları etki değerlendirmesi yapması ve platformların çocuklar üzerindeki etkilerine ilişkin şeffaf raporlama yükümlülüklerine tabi tutulması gerektiği ifade edilmiştir.

OHCHR, yaş doğrulama sistemlerinin kullanılması hâlinde mahremiyet ve veri koruma bakımından güçlü güvencelerin getirilmesi gerektiğine dikkat çekmektedir. Bu kapsamda; veri toplama ve saklama süreçlerinin sınırlandırılması, yaş doğrulama hizmeti sağlayan taraflara ilişkin şeffaflığın sağlanması, ayrımcılık risklerinin değerlendirilmesi ve resmî belgeye sahip olmayan çocuklar bakımından da erişilebilir çözümler geliştirilmesi önerilmektedir. Yaş temelli sınırlamaların ise genel nitelikte değil, açıkça tespit edilmiş belirli zararlara yönelik olması gerektiği belirtilmiştir.

İlgili yazıya buradan ulaşabilirsiniz.

11 Almanya'da Google AI Overviews Hakkında Sorumluluk Kararı

KARAR TARİHİ: 27.01.2026

Almanya'da Münih Bölge Mahkemesi, Google'ın AI Overviews özelliği tarafından üretilen hatalı ifadelerden sorumlu tutulabileceğine ilişkin dikkat çekici bir karar vermiştir. Kararda, Google'ın arama sonuçlarında yapay zekâ tarafından üretilen yanıltıcı veya gerçeğe aykırı ifadelerin yayılmasını önlemekle yükümlü olduğu değerlendirilmiştir.

Uyuşmazlık, Google'ın yapay zekâ destekli özetlerinin bazı yayıncı şirketleri herhangi bir dayanak olmaksızın şüpheli ticari uygulamalar ve dolandırıcılık iddialarıyla ilişkilendirmesinden kaynaklanmıştır. Mahkeme, geleneksel

arama motorlarından farklı olarak AI Overviews'un üçüncü kişi içeriklerini yalnızca listelemediğini, mevcut kaynaklardan hareketle yeni ve bağımsız ifadeler ürettiğini belirtmiştir.

Karar; yapay zekâ sistemlerini tasarlayan, eğiten, işleten ve yöneten şirketlerin, bu sistemlerin ürettiği hatalı içeriklerin yol açabileceği zararlardan sorumlu tutulabileceğini göstermesi bakımından önem taşımaktadır. Bu yaklaşım, üretken yapay zekâ sistemlerinde yalnızca "çıktılar hatalı olabilir" uyarısının sorumluluğu ortadan kaldırmaya yeterli olmayabileceğine işaret etmektedir.

WIRED haberinin tam metnine buradan ulaşabilirsiniz.

12 Avusturya Veri Koruma Otoritesi'nden Zorunlu Cinsiyet Bazlı Hitap Seçimini İlişkin Karar

KARAR TARİHİ: 24.11.2025

2025-0.950.759

Başvuruya konu olayda ilgili kişi, çevrim içi mağazada hesap oluştururken cinsiyet bazlı hitap seçimi yapmak zorunda kalmış ve sonrasında veri sorumlusundan, kendisine yönelik cinsiyet bazlı hitap kullanımına son verilmesini talep etmiştir. Veri sorumlusu başlangıçta teknik değişikliğin mümkün olmadığını belirtmiş; ancak süreç devam ederken sistemini güncelleyerek cinsiyet nötr kayıt imkânı sağlamıştır. DSB, düzeltme ve silme talepleri bakımından ihlalin giderildiğini kabul etmekle birlikte, geçmişteki veri işleme faaliyetinin GDPR'ın 5'inci maddesindeki ilkelere uygun olup olmadığını ayrıca incelemiştir.

DSB, Avrupa Birliği Adalet Divanı'nın C-394/23 sayılı "Mousse" kararına da atıf yaparak, cinsiyet bazlı hitap verisinin sözleşmenin ifası için zorunlu olmadığını ve kişiselleştirilmiş ticari iletişim amacıyla işlenmesinin veri minimizasyonu ilkesiyle bağdaşmadığını değerlendirmiştir. Bu kapsamda; siparişin alınması, teslimat, ödeme veya ticari iletişim gibi amaçlar bakımından cinsiyet bazlı hitap verisinin işlenmesinin gerekli olmadığı, daha az müdahaleci ve eşit derecede etkili alternatiflerin bulunduğu sonucuna varılmıştır.

Kararda, veri sorumlusunun GDPR m. 6/1-b kapsamında sözleşmenin ifası veya m. 6/1-f kapsamında meşru menfaat hukuki sebebine dayanamayacağı belirtilmiştir. DSB'ye göre, müşterilere kişisel hitapta bulunma yönünde ekonomik bir menfaat kural olarak meşru kabul edilebilse de somut olayda zorunlu cinsiyet bazlı hitap verisinin işlenmesi gerekli değildir. Bu nedenle veri işleme faaliyeti, GDPR m. 5/1-b'de düzenlenen amaçla sınırlılık ve m. 5/1-c'de düzenlenen veri minimizasyonu ilkelerine aykırı bulunmuştur.

Kararın tam metnine buradan ulaşabilirsiniz.

13 Adalet Bakanlığı Yargıda Yapay Zeka Destekli Yeni Dönemi Duyurdu

Adalet Bakanlığı, UYAP AI Karar Destek Sistemi ile yargı süreçlerinde hız, verimlilik ve etkinliğin artırılmasını hedefleyen yapay zekâ destekli yeni dönemi duyurmuştur. Sistemin; içtihat ve emsal karar taraması, dava dosyalarının özetlenmesi, gerekçeli karar taslakları, delil analizleri ve bilirkişi raporlarının değerlendirilmesi gibi alanlarda hâkim ve savcılara destek sunması amaçlanmaktadır. Duyuruda, sistemin karar verici değil yalnızca karar destek aracı olduğu; nihai kararın hâkim ve savcılar tarafından verileceği, süreçlerin insan kontrolünde, şeffaf ve denetlenebilir şekilde yürütüleceği vurgulanmıştır.

Duyurunun tam metnine buradan ulaşabilirsiniz.

14 Dünya Ekonomik Forumu'ndan Yapay Zekanın Benimsenmesinde İnsan Faktörüne İlişkin Değerlendirme

Dünya Ekonomik Forumu, iş yerlerinde yapay zekâ kullanımının başarısının yalnızca teknolojik altyapıya değil, çalışanların güven düzeyine, psikolojik hazırlığına ve kurum kültürüne de bağlı olduğunu vurgulamıştır. Yazıda, çalışanların yapay zekâya farklı düzeylerde yaklaştığı; iş kaybı, gözetim, beceri kaybı ve teknolojiye güvensizlik gibi endişelerin dönüşüm sürecini etkileyebileceği belirtilmiştir. Bu nedenle kurumların yapay zekâ benimsemesini yalnızca teknik eğitimlerle değil, çalışanların kaygı ve beklentilerini dikkate alan insan odaklı stratejilerle yönetmesi gerektiği ifade edilmiştir.

WEF yazısının tam metnine buradan ulaşabilirsiniz.

15 Avrupa Komisyonu'ndan Yapay Zekânın Toplumsal Etkilerine İlişkin Bağımsız Uzman Raporu

Avrupa Komisyonu Araştırma ve Yenilik Genel Müdürlüğü tarafından görevlendirilen bağımsız uzmanlarca hazırlanan raporda, yapay zekânın sağlık, iklim dayanıklılığı, üretkenlik ve sürdürülebilirlik gibi alanlarda önemli fırsatlar

sunduğu; ancak bu fırsatların eşitlik, şeffaflık, hesap verebilirlik ve insan onuru gibi değerlerle uyumlu bir yönetişim modeli içinde değerlendirilebileceği vurgulanmıştır. Raporda ayrıca şeffaflık eksikliği, dezenformasyon, kaynak eşitsizlikleri, kişisel verilerin korunması, iş yerinde yapay zekâ temelli gözetim ve fikrî mülkiyet gibi konulara dikkat çekilmiş; yapay zekâ sistemlerinin geliştirilmesi ve kullanılması süreçlerinde insan denetimi, mahremiyet, hesap verebilirlik ve toplumsal etki değerlendirmesinin birlikte ele alınması gerektiği belirtilmiştir

Raporun tam metnine buradan ulaşabilirsiniz

16 Avrupa Veri Koruma Denetçisi'nden ("EDPS") Gölge Yapay Zekâ Kullanımına İlişkin Veri İhlali Uyarısı

DPS, çalışanların kurum onayı olmaksızın üretken yapay zekâ sohbet botları, kodlama asistanları veya otomatik toplantı kayıt araçları kullanmasını "gölge yapay zekâ" olarak tanımlamakta ve bu kullanımın veri koruma ile bilgi güvenliği açısından önemli riskler doğurabileceğini belirtmektedir. Onaylanmamış araçlara girilen verilerin nerede saklandığı, kimler tarafından erişildiği veya model eğitiminde kullanılıp kullanılmadığı belirsiz hâle gelebilmektedir.

KVKK bakımından bu tür kullanımlar; amaçla sınırlılık, veri minimizasyonu, işleme şartları ve veri güvenliği ilkeleri çerçevesinde dikkatle değerlendirilmelidir. Veri sorumlularının yalnızca genel uyarılarla yetinmeyip, hangi yapay zekâ araçlarının kullanılabileceğini ve hangi verilerin bu araçlara girilemeyeceğini açıkça belirlemesi önem taşımaktadır.

EDPS; yapay zekâ kullanım politikaları, veri sınıflandırma kuralları, erişim kontrolleri, çalışan farkındalığı ve güvenli alternatif araçların sunulmasını temel tedbirler arasında göstermektedir.

EDPS'in konuya ilişkin blog yazısının tam metnine buradan ulaşabilirsiniz.

İLETİŞİM

EGE ÇAKIRCA AVUKATLIK BÜROSU

Esentepe Mahallesi Harman 1 Sokak Harmancı Giz Plaza No: 5 Kat: 5 – İstanbul 34394

info@eclawtr.com

+90 212 352 3318

eclawtr.com

EGE • ÇAKIRCA







Kurucu Ortak
Özlem EGE POLAT

Avukat
Ceren AYDEMİR

Yasal Stajyer
Ezgi OPRUKÇU