

KİŞİSEL VERİLERİN KORUNMASI İLE İLGİLİ SEÇİLMİŞ GÜNCEL GELİŞMELER-62

* Kişisel Verileri Koruma Kurulunun 16.09.2026 tarih ve 2026/2035 sayılı “İşverenler Tarafından Çalışanlara Tahsis Edilen Kurumsal E-Posta Hesapları Başta Olmak Üzere, İşin Yürütülmesi Amacıyla Kullanılan İletişim Kanallarının Denetlenmesi Suretiyle Gerçekleştirilen Kişisel Veri İşleme Faaliyetlerinde Uyulması Gereken Usul ve Esaslar Hakkında İlke Kararı” 08.10.2026 tarih ve 33394 sayılı Resmî Gazete’de yayımlandı¹.

* Kurumumuz ile Türkiye Barolar Birliği iş birliğinde hazırlanan “Avukatların Mesleki Faaliyetlerinde Kişisel Verilerin Korunmasına İlişkin Uygulama Rehberi” yayımlandı².

* “İlgili Kişilerin Başvurularına Verilecek Cevabın Bildirim Usulüne İlişkin Kamuoyu Duyurusu” Kurumumuzun internet sitesinde yayımlandı³.

* Kurumumuz tarafından hazırlanan KVKK Bülten’in “Akıllı Cihazlar ve Dijital Mahremiyet” konulu 12’nci sayısı yayımlandı⁴. Bu sayıda;

- Veri Çağında Dijital Mahremiyetin Önemi
- Mahremiyet Tasarımla Başlar
- Nesnelerin İnterneti ve Kişisel Verilerin Korunması
- Akıllı Cihazlar Bizi Ne Kadar Tanıyor?
- Akıllı Cihaz Kullanıcısının 10 Altın Kuralı
- Mobil Uygulamalarda Mahremiyetin Korunmasında Bireylere Yönelik Tavsiyeler
- Akıllı Gözlük Kullanımında Kişisel Verilerin Korunması
- Çocuğunuz Akıllı Telefon Kullanmaya Hazır mı?
- Kişisel Verilerin Korunması ile İlgili Öne Çıkan Gelişmeler
- Bizden Haberler başlıkları yer almaktadır.

* Avrupa Veri Koruma Kurulu (EDPB), kamuoyu görüş sürecinin ardından Dijital Hizmetler Tüzüğü (DSA) ile AB Genel Veri Koruma Tüzüğü (GDPR) arasındaki etkileşime ilişkin rehberin nihai versiyonunu yayımladı⁵.

* Avrupa Veri Koruma Kurulu (EDPB), AB Genel Veri Koruma Tüzüğü (GDPR) kapsamındaki diğer düzeltici yetkilerle bağlantılı olarak idari para cezası uygulama yetkisinin kullanımına ilişkin rehberin kamuoyu görüşüne açıldığını duyurdu⁶. Bahse konu rehberde, veri koruma otoritelerinin idari para cezası uygulanıp uygulanmayacağına karar verirken izleyebilecekleri beş aşamalı yöntem ortaya konulmaktadır. Bu kapsamda ihlalin para cezasına konu olup olamayacağının belirlenmesi, hakkında inceleme yürütülen tarafa ilgili ihlal nedeniyle idari para cezası uygulanıp uygulanamayacağının tespit edilmesi, ihlalin kasıt veya ihmâl sonucu işlenip işlenmediğinin incelenmesi, ağırlaştırıcı ve hafifletici unsurların dikkate alınması ve idari para cezası uygulanmasının etkili, ölçülü ve caydırıcı olup olmayacağının değerlendirilmesi aşamalarına yer verilmektedir.

* Avrupa Komisyonu, çocukların çevrim içi güvenliğinin korunmasına yönelik olarak “EU KIDS Act” teklifini sundu⁷. Teklif kapsamında 13 yaşından küçüklerin sosyal medya hesabı açamaması, 13-14 yaş grubunun ebeveyn gözetiminde belirli şartlarla sınırlı şekilde hesap kullanabilmesi ve 15 yaşından itibaren bağımsız hesap açılabilmesi öngörülmektedir.

* Avrupa Veri Koruma Denetçisi (EDPS), TechDispatch serisi kapsamında “güvenli çok taraflı hesaplama” (*secure multi-party computation*) yöntemini ele alan bir doküman yayımladı⁸.

* Avrupa Birliği Siber Güvenlik Ajansı (ENISA), 1 Ocak 2025 - 31 Aralık 2025 tarihleri arasında gözlemlenen olayların analiz edildiği “Tehdit Görünümü 2026” raporunu yayımladı⁹.

* ABD Siber Güvenlik ve Altyapı Güvenliği Ajansı (CISA), iç tehditlerin azaltılmasına ilişkin rehberin güncellenmiş versiyonunu yayımladı¹⁰. İlk olarak 2020 yılında yayımlanan rehberin, kuruluşların iç tehditleri daha iyi anlamalarına ve bu tehditlerin azaltılmasına yönelik programlarını oluşturmalarına veya geliştirmelerine yardımcı olmayı amaçladığı belirtilmektedir. Rehberin güncellenmiş versiyonunda ise güncel vaka çalışmalarına ve istatistiksel bilgilere, hibrit ve uzaktan çalışma düzenlerinin yaygınlaşması ile yapay zekâ kullanımı gibi güncel iş yeri eğilimlerinin iç tehditler bakımından gündeme getirdiği hususlara ilişkin yeni değerlendirmelere ve kuruluşların hazırlık kapasitesini güçlendirmeye yardımcı olabilecek güncel CISA kaynaklarına yer verildiği ifade edilmektedir.

* Avrupa Parlamentosu Araştırma Servisi (EPRS), Avrupa bulut ve yapay zekâ ekosisteminin güçlendirilmesine ilişkin bir bilgi notu yayımladı¹¹.

* UNESCO, yapay zekâ ve algoritmalar çağında eğitimin geleceğine ilişkin olarak büyük ölçüde kaçınıldığı veya ele alınmadığı belirtilen temel meseleleri gündeme getiren bir derleme yayımladı¹². 26 değerlendirme yazısından oluşan derlemede; karar alma yetkisi, otonomi ve gözetimin kimde olacağı; gençlerin ilişkisel, duygusal ve bilişsel gelişiminin nasıl şekilleneceği; pedagoji ve değerlendirme süreçleri bakımından neyin anlamlı ve uygun olacağı; nasıl düşüneceğimiz, sorgulayacağımız ve kendimizi ifade edeceğimiz; kamusal amaçlara hizmet eden ve kamuya karşı hesap verebilir ortak bir değer olarak eğitimin nasıl yönetileceği ve yapay zekânın eğitimin geleceğine dair düşünme biçimimizi nasıl etkileyebileceği gibi sorular ele alınmaktadır.

* Avrupa Komisyonu, eğitimde üretken yapay zekâ kullanımının ele alındığı bir rapor yayımladı¹³. Bahse konu raporda; üretken yapay zekâ kullanımının genel olarak eğitim sistemi üzerindeki etkileri ile öğrenciler, öğretmenler ve ebeveynler bakımından ortaya çıkarabileceği etkiler değerlendirilmektedir.

* İrlanda Veri Koruma Otoritesi (DPC), 2021-2025 yılları arasında yapay zekâ ürün ve hizmetlerine ilişkin gözetim faaliyetlerinden elde edilen bulguları içeren bir rapor yayımladı¹⁴. Raporda yer alan bulgular arasında; üretken yapay zekânın son yıllardaki hızlı gelişiminin de etkisiyle yapay zekâyâ ilişkin temaslarda önemli bir artış yaşandığı, inovasyon ile veri korumanın birbirini dışlayan kavramlar olmadığı, büyük dil modelleri ve öneri sistemleri gibi farklı yapay zekâ uygulamalarına ilişkin çok sayıda temas kapsamında hukuki sebep, şeffaflık, veri minimizasyonu ve çocukların korunması alanlarında veri koruma mevzuatına uyum bakımından önemli iyileştirmeler sağlandığı, yapay zekânın eğitimi bakımından meşru menfaat hukuki sebebinin uygulanması ve şeffaflığın sağlanmasının Otorite'nin temel odak alanları arasında yer aldığı ve bireylerin haklarına yönelik risklerin yeterli düzeyde azaltılamadığı durumlarda Otorite'nin acilen müdahale etmeye hazır olduğu gibi hususlar bulunmaktadır.

* Avrupa Parlamentosu Araştırma Servisi (EPRS), yapay zekâ ve suç ilişkisini ele alan bir bilgi notu yayımladı¹⁵. Bahse konu dokümanda; yapay zekâ destekli ve yapay zekâ ile güçlendirilmiş saldırılar (sosyal mühendislik, oltalama ve dolandırıcılık, deepfake, yapay zekâ ile oluşturulan kötü amaçlı yazılımlar vb.), yapay zekâ modellerindeki zafiyetlerden kaynaklanan kötü amaçlı eylemler (modelin bütünlüğüne yönelik saldırılar, algoritmik alım satım/piyasa manipülasyonu, mahremiyete yönelik saldırılar vb.), kolluk faaliyetlerinde yapay zekâ kullanımı ve konuya ilişkin hukuki çerçeve gibi hususlar ele alınmaktadır.

* Birleşik Krallık Ulusal Siber Güvenlik Merkezi (NCSC), gölge yapay zekânın ortaya çıkarabileceği siber güvenlik risklerinin yönetilmesine ilişkin bir içerik yayımladı¹⁶. Bahse konu içerikte “gölge yapay zekâ”, kuruluşun onaylı sistem ve süreçleri kapsamında yer almayan yapay zekâ teknolojilerinin kullanımı şeklinde tanımlanmakta olup yakın tarihli araştırmaların gölge yapay zekâ kullanımının yaygın olduğunu gösterdiği ve bir çalışmada, çalışanların neredeyse dörtte üçünün (%71) işverenleri tarafından onaylanmamış yapay zekâ araçlarını kullandığını belirttiği ifade edilmektedir.

Diğer taraftan gölge yapay zekânın, kuruluşların tespit etmekte ve dolayısıyla yönetmekte zorlanabileceği riskler ortaya çıkarabileceği ve bu durumun çeşitli güvenlik sorunlarına yol açabileceği vurgulanmakta olup bu kapsamda gölge yapay zekânın ortaya çıkarabileceği siber güvenlik riskleri arasında; hassas bilgilerin açığa çıkması, kuruluşların veriler üzerindeki görünürlüğünün ve kontrolünün azalması ve saldırganlar açısından yeni fırsatların ortaya çıkması sayılmaktadır.

Söz konusu risklerin azaltılması amacıyla ise çalışanların onaylanmamış yapay zekâ araçlarına yönelme nedenlerinin anlaşılması, açık iletişimi teşvik eden pozitif bir siber güvenlik kültürünün benimsenmesi ve yapay zekâ sistemlerinin iş ortamlarına güvenli şekilde entegre edilmesi yönünde tavsiyelerde bulunmaktadır.

* OECD, kuruluşlarda etken yapay zekâ (*Agentic AI*) sistemlerinin geliştirilmesi, kullanıma alınması ve yönetişimine ilişkin erken dönem bulgularını ele alan bir doküman yayımladı¹⁷. Çeşitli bölge ve sektörlerden 25 kuruluşla yapılan görüşmelerden yararlanılan çalışmanın temel bulguları arasında;

- Etken yapay zekâ sistemlerinin deneysel uygulamaların ötesine geçerek kurumsal iş akışlarına dahil olmaya başladığı ve kullanım alanları arasında tedarik zinciri ve endüstriyel optimizasyon, siber güvenlik, yazılım geliştirme, altyapı planlaması ve bilimsel araştırma gibi alanların bulunduğu,
- Bu sistemlerin kullanıma alınma olgunluk düzeyinin teknik hazırlık, kuruluşların öncelikleri ve risk toleransındaki farklılıklara göre kuruluşlar arasında değişkenlik gösterdiği,
- Etken yapay zekâ çözümlerinin operasyonel verimliliğin artırılması, maliyetlerin azaltılması, iş gücü kısıtlarının ele alınması ve yeni değer ortaya çıkarılması gibi amaçlarla kullanıldığı,
- Yönetişim ve teknik tedbirlerin henüz erken aşamada olduğu, bununla birlikte kuruluşların mevcut yönetim çerçevelerini uyarladığı, otonomi düzeyinin kademeli olarak artırılması, yüksek riskli eylemler için insan kontrol noktaları oluşturulması ve alan uzmanlarıyla birlikte tasarım yapılması gibi tedbirlere başvurulduğu; ancak değerlendirme ve güvence, siber güvenlik, hesap verebilirlik ve çok aracı yapılar da izlenebilirlik gibi konularda zorlukların devam ettiği

gibi hususlar bulunmaktadır. Diğer taraftan bulguların sınırlı coğrafi ve sektörel kapsama dayandığı göz önünde bulundurularak örnekleyici nitelikte değerlendirilmesi gerektiği vurgulanmaktadır.

İLGİLİ LİNKLER

- 1 <https://www.resmigazete.gov.tr/eskiler/2026/10/20261008-6.pdf>, 08.10.2026.
- 2 <https://www.kvkk.gov.tr/Icerik/8990/avukatlarin-mesleki-faaliyetlerinde-kisisel-verilerin-korunmasina-iliskin-uygulama-rehberi-yayimlandi>, 22.09.2026.
- 3 <https://www.kvkk.gov.tr/Icerik/9024/ilgili-kisilerin-basvurularina-verilecek-cevabin-bildirim-usulune-iliskin-kamuoyu-duyurusu>, 01.10.2026.
- 4 <https://www.kvkk.gov.tr/SharedFolderServer/CMSFiles/MTZhYmJhODgyMmVkZDA.pdf>, 29.09.2026.
- 5 https://www.edpb.europa.eu/news/edpb-harmonises-fining-methodology-and-adopts-final-dsa-gdpr-guidelines_en, 21.09.2026.
- 6 https://www.edpb.europa.eu/news/edpb-harmonises-fining-methodology-and-adopts-final-dsa-gdpr-guidelines_en, 21.09.2026.
- 7 <https://digital-strategy.ec.europa.eu/en/news/eu-kids-act-restrict-social-media-platforms-access-children-eu>, 17.09.2026.
- 8 https://www.edps.europa.eu/data-protection/our-work/publications/techdispatch/2026-09-17-techdispatch-12026-secure-multi-party-computation_en, 17.09.2026.
- 9 <https://www.enisa.europa.eu/publications/enisa-threat-landscape-2026>, 22.09.2026.
- 10 <https://www.cisa.gov/resources-tools/resources/insider-threat-mitigation-guide>, Eylül 2026.
- 11 [https://www.europarl.europa.eu/thinktank/en/document/EPRS_BRI\(2026\)788157](https://www.europarl.europa.eu/thinktank/en/document/EPRS_BRI(2026)788157), 25.09.2026.
- 12 <https://www.unesco.org/en/articles/algorithm-room-seeing-and-confronting-implications-ai-future-education>, 08.09.2026.
- 13 <https://op.europa.eu/en/publication-detail/-/publication/e1317635-b62b-11f1-81de-01aa75ed71a1/language-en>, 22.09.2026.
- 14 <https://dataprotection.ie/en/dpc-guidance/publications/dpc-AI-insights-report>, 24.09.2026.
- 15 [https://www.europarl.europa.eu/thinktank/en/document/EPRS_BRI\(2026\)791525](https://www.europarl.europa.eu/thinktank/en/document/EPRS_BRI(2026)791525), 30.09.2026.
- 16 <https://www.ncsc.gov.uk/blogs/the-hidden-risks-of-shadow-ai>, 07.09.2026.
- 17 <https://oecd.ai/en/ai-publications/agent-ai-in-organisations>, 24.09.2026.