KİŞİSEL VERİLERİN KORUNMASI İLE İLGİLİ SEÇİLMİŞ GÜNCEL GELİŞMELER-63

* 27.10.2026 tarih ve 33413 mükerrer sayılı Resmî Gazete'de yayımlanan "2027 Yılı Cumhurbaşkanlığı Yıllık Programı"nda, 6698 sayılı Kişisel Verilerin Korunması Kanunu'nun AB Genel Veri Koruma Tüzüğü (GDPR) başta olmak üzere AB müktesebatı ile uyumlaştırılmasına yönelik çalışmaların 2027 yılı içerisinde tamamlanacağı belirtildi[1].

* Ülkemizde Siber Güvenlik Başkanlığı tarafından hazırlanan "Sosyal Ağ Sağlayıcı Tarafından Çocuklara Özgü Ayrıştırılmış Hizmet Sunulmasına ve Yaş Doğrulamaya İlişkin Yönetmelik" 10.10.2026 tarih ve 33396 sayılı Resmî Gazete'de yayımlandı[2].

* Avrupa Veri Koruma Kurulu (EDPB), çocukların çevrim içi mahremiyet konusunda bilinçlendirilmesini desteklemek amacıyla ebeveynler, öğretmenler ve eğitimcilere yönelik olarak "Çocuklar için Mahremiyet" *(Privacy for Kids)* platformunu kullanıma sundu[3]. Bu kapsamda yapılan duyuruda; çevrim içi paylaşım, sosyal medya, akıllı telefonlar ve uygulamalar, evde ve okulda mahremiyet, siber zorbalık ve akıllı oyuncaklar gibi konularda projeler, bilgilendirme kampanyaları, oyunlar, infografikler, videolar ve testler dâhil olmak üzere çeşitli materyallere bahse konu platform üzerinden ulaşılabileceği belirtilmektedir.

* Fransa Veri Koruma Otoritesi (CNIL), çevrim içi ortamda erişilebilir verilerden hareketle kişilerin kurumsal e-posta adreslerinin yeniden oluşturulmasının hangi koşullarda hukuka uygun olabileceğine ilişkin bir içerik yayımladı[4].

* Avrupa Veri Koruma Denetçisi (EDPS), kişisel veri ihlallerinin bildirilmesine ilişkin sıkça sorulan soruları yayımladı[5]. Bu kapsamda bahse konu içerikte; risk değerlendirmesi, zorunlu bildirim formunun kullanımı, aşamalı bildirimler, riskleri azaltmaya yönelik tedbirler ve ihlalden etkilenen ilgili kişilerin bilgilendirilmesi gibi hususlara açıklık getirilmektedir. Ayrıca veri sorumluları ve veri işleyenler bakımından kişisel veri ihlallerinin bildirilmesi ve belgelendirilmesine yönelik açıklamalara yer verilmektedir.

* İspanya Veri Koruma Otoritesi (AEPD), "Mahremiyet, İnovasyon ve Teknoloji Dergisi"nin ikinci sayısının yayımlandığını duyurdu[6].

* Avrupa Veri Koruma Kurulu (EDPB), akıllı gözlüklerin kişisel verilerin korunması bakımından gündeme getirdiği hususlara ilişkin bir açıklama yayımladı[7]. Bahse konu açıklamada; akıllı gözlüklerin yaygınlaşmasının ve kullanım sıklığının artmasının iletişim, destek ve yenilik açısından fırsatlar sunduğu,

bununla birlikte kişisel verilerin korunması ve bireylerin hakları bakımından önemli soruları da gündeme getirdiği vurgulanmaktadır. Bu kapsamda ilgili açıklamada, akıllı gözlüklerin kullanım alanları ve bunlara özgü riskler ile veri sorumlusunun belirlenmesi, şeffaflığın sağlanması ve uygun hukuki sebebin tespiti gibi başlıklar çerçevesinde veri koruma mevzuatına uyuma ilişkin hususlar ele alınmaktadır.

* Avrupa Veri Koruma Kurulu (EDPB), akıllı gözlükler çağında video kaydı, gözetim ve delillerin yönetimine ilişkin olarak "Uzman Destek Havuzu" *(Support Pool of Experts)* programı kapsamında hazırlanan raporu yayımladı[8].

* Birleşik Krallık Veri Koruma Otoritesi (ICO), etken yapay zekânın *(Agentic AI)* ortaya çıkarabileceği veri koruma risklerine ilişkin değerlendirmelerine katkı sağlamak amacıyla bir görüş çağrısı başlatıldığını duyurdu[9]. Bu kapsamda, kuruluşların etken yapay zekâ ile ilgili veri koruma risklerini nasıl yönettiğine ilişkin olarak geliştiricilerden, bu sistemleri kullanıma alan kuruluşlardan ve diğer uzmanlardan görüş talep edildiği belirtilmektedir.

* Hamburg Veri Koruma ve Bilgi Edinme Özgürlüğü Komiseri (HmbBfDI), Hamburg şehir idaresinde kullanılan LLMoin adlı yapay zekâ sohbet robotu örneği üzerinden büyük dil modellerinin veri koruma mevzuatına uygun kullanımını ele alan bir vaka çalışması yayımladı[10].

* İspanya Veri Koruma Otoritesi (AEPD), yapay zekâ asistanları ve aracılarının *(agents)* kullanımında kişisel verilerin korunmasına ilişkin on maddelik bir doküman yayımladı[11].

* OECD, yapay zekâ bağlamında kullanıcı kontrolünün ve bireylerin mahremiyetinin korunmasının güçlendirilmesine ilişkin bir politika notu yayımladı[12]. Bahse konu dokümanın temel mesajları arasında;

- Yapay zekâ modellerinin geliştirilmesinde büyük miktarda ve yüksek kaliteli veriye ihtiyaç duyulduğu, bu verilerin kişisel verileri de içerebildiği ve yapay zekânın yaşam döngüsü boyunca yüksek kaliteli verilere erişimin kolaylaştırılması ile mahremiyetin ve kullanıcıların kişisel verileri üzerindeki kontrolünün sağlanmasının birlikte gözetilmesi gerektiği,

- Yapay zekânın eğitiminde kullanılan verilerin önemli bir bölümünün üretken yapay zekâ sistemleri ile kullanıcı etkileşimlerinden ve internette kamuya açık verilerin web kazıma yoluyla toplanmasından elde edildiği, statik eğitim veri kümelerinin yanı sıra yapay zekâ sistemlerinde harici bilgilere gerçek zamanlı olarak erişilmesini ve bu bilgilerin kullanılmasını sağlayan "erişim destekli üretim" *(retrieval-augmented generation-RAG)* gibi dinamik yaklaşımların da giderek daha fazla kullanıldığı,

- Veri koruma otoritelerinin rehberlerinde, yapay zekâ sohbet botlarının girdilerde yer alan kişisel verilerin nasıl işlendiği ve bunların modellerin eğitimi veya iyileştirilmesinde kullanılıp kullanılmayacağı konusunda kullanıcıların bilgilendirilmesi gerektiğinin vurgulandığı, bu doğrultuda geliştiricilerin şeffaflığı artırdığı ve küresel "opt-out" mekanizmaları sunduğu,

- Kişisel verilerin model ağırlıklarına gömülü hale gelebilmesi veya eğitim sırasında "ezberlenebilmesi" nedeniyle erişim, düzeltme ve silme haklarının kullanılmasında zorluklar ortaya çıkabildiği,

- Yapay zekâ sistemlerinin etken (agentic) ve çoklu yapay zekâ aracısı sistemlerine *(multi-agent systems)* dönüşmesinin geleneksel veri koruma ilkelerinin uygulanmasını zorlaştırabileceği, bununla birlikte yapay zekâ aracılarının karmaşık veri etkileşimlerinde kullanıcıların mahremiyetlerini yönetmelerine de katkı sağlayabileceği,

- Yapay zekânın eğitilmesi amacıyla web kazıma yoluyla elde edilen verilerin yönetişiminin düzenleyici rehberler, sektör standartları ve teknik güvencelerin birlikte uygulanmasıyla gelişmekte olduğu

gibi hususlar yer almaktadır.

* Avrupa Parlamentosu, yapay zekâda toplumsal cinsiyet yanlılığı ve teknoloji destekli cinsiyete dayalı şiddete ilişkin bir çalışma yayımladı[13]. Bahse konu çalışmada; bu sorunların farklı alanlardaki görünümleri ve kadınlar üzerindeki etkileri ile bunların önlenmesine ve ortaya çıkan mağduriyetlerin giderilmesine yönelik hukuki, yönetişimsel ve teknik yaklaşımların etkililiği değerlendirilmektedir.

* Yapay zekâ sistemlerine yönelik siber güvenlik tehditlerinin ve güvenlik ihlallerinin ele alınmasına ilişkin olarak "ISO/IEC 27090:2026" standardı yayımlandı[14].

İLGİLİ LİNKLER

1 https://www.resmigazete.gov.tr/eskiler/2026/10/20261027M1-1.pdf, 27.10.2026.

2 https://www.resmigazete.gov.tr/eskiler/2026/10/20261010-15.pdf, 10.10.2026.

3 https://www.edpb.europa.eu/news/edpb-helps-kids-stay-safe-online_en, 04.11.2026.

4 https://www.cnil.fr/fr/reconstitution-adresses-professionnelles-quel-cadre, 16.10.2026.

5 https://www.edps.europa.eu/data-protection/our-role-supervisor/personal-data-breach/faq-about-data-breach-notification_en, 28.10.2026.

6 https://revista.aepd.es/revistaprivacidad/issue/view/2, 08.10.2026.

7 https://www.edpb.europa.eu/news/edpb-publishes-statement-on-the-data-protection-challenges-of-smart-glasses_en, 13.10.2026.

8 https://www.edpb.europa.eu/news/edpb-publishes-statement-on-the-data-protection-challenges-of-smart-glasses_en, 13.10.2026.

9 https://ico.org.uk/about-the-ico/ico-and-stakeholder-consultations/2026/10/agentic-ai-call-for-evidence/, 08.10.2026.

10 https://datenschutz-hamburg.de/news/ki-systeme-datenschutzkonform-einsetzen-hmbbfdi-veroeffentlicht-fallstudie-zu-llmoin, 05.11.2026.

11 https://www.aepd.es/prensa-y-comunicacion/notas-de-prensa/la-aepd-publica-un-decalogo-para-delegar-tareas-en-asistentes, 27.10.2026.

12 https://www.oecd.org/en/publications/enhancing-user-control-and-privacy-protections-in-the-context-of-ai_e0bd9a46-en.html, 15.10.2026.

13 https://www.europarl.europa.eu/thinktank/en/document/IUST_STU(2026)791844, 04.11.2026.

14 https://www.iso.org/standard/27090, Ekim 2026.