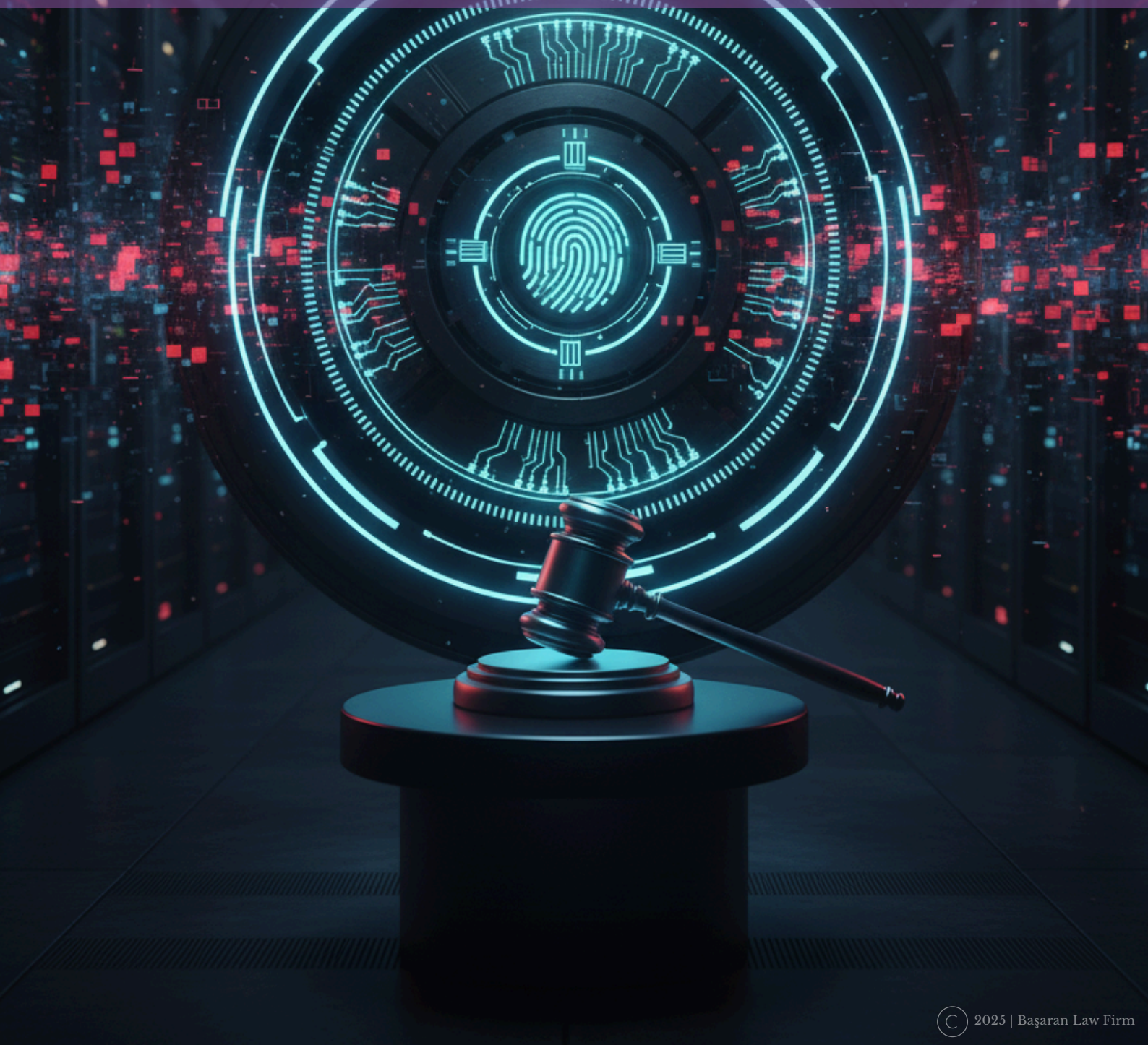
THE PULSE

BAŞARAN LAW FIRM

December 2025
Edition: 02

Regulatory Landscape in Data Protection Law



© 2025 | Başaran Law Firm

Less Bureaucracy, Stronger Structure: The EU's Digital Omnibus

On 19 November 2025, the European Commission publishes the Digital Omnibus proposal, aiming to simplify the EU's digital legislative framework while maintaining high standards of data protection. The proposal streamlines key instruments such as the GDPR, ePrivacy Directive, NIS2 and the Data Act, with the goal of reducing compliance costs without lowering the level of protection for personal data.

One of the most notable changes concerns the long-criticised dual regime between the GDPR and the ePrivacy Directive: rules on accessing personal data from terminal equipment are moved entirely under the GDPR, eliminating duplicate consent requirements. User preferences are to be expressed through automated, machine-readable browser or application settings, which service providers must respect, thereby reducing both "consent fatigue" and compliance burdens.

Targeted amendments to the GDPR further clarify the notion of personal data by emphasising reasonable identifiability, give controllers more flexibility in dealing with abusive access requests, limit data breach notifications to high-risk incidents while extending the deadline to 96 hours, and allow strictly controlled residual processing of special category data arising during AI training.

In parallel, personal data breach and cybersecurity incident notifications under various EU acts are consolidated into a single EU-level reporting platform operated by ENISA, based on a "report once, share many" model that is expected to generate substantial administrative savings while preserving the EU's high level of personal data protection.

The EU Launches a New Era for Data and Artificial Intelligence

On 19 November 2025, the European Commission released the Data Union Strategy – Unlocking Data for AI, setting out its roadmap to strengthen Europe's data economy and boost the development of trustworthy artificial intelligence.

The Strategy focuses on three main priorities: scaling up access to high-quality data for AI, simplifying the EU data regulatory framework, and reinforcing the EU's global position in international data flows.

The Commission plans to expand and interconnect European data spaces across key sectors such as health, energy, manufacturing, mobility and finance, enabling companies and researchers to access larger volumes of reliable data for innovation and AI training.

In parallel, the Strategy is closely aligned with the Digital Omnibus initiative and aims to reduce legal fragmentation and compliance costs through streamlined rules, standard contractual clauses and improved cloud governance.

A strong emphasis is also placed on digital sovereignty. While promoting fair and secure cross-border data flows with trusted partners, the Strategy seeks to shield EU data from undue access and misuse by third countries. Through targeted investments in data infrastructure and cloud technologies, the Commission aims to position the EU as a leading global hub for data-driven and AI-based innovation, while preserving high standards of data protection and cybersecurity.

Major GDPR Fine Imposed for Unsecured Cross-Border Data Transfers and Excessive Employee Data Processing

On 14 November 2025, the Croatian Personal Data Protection Agency imposed an administrative fine of EUR 4.5 million on a telecommunications operator for violations of the General Data Protection Regulation. The decision is based on

(i) the transfer of personal data to a group company in Serbia without a valid transfer mechanism,

(ii) the lack of transparent disclosure to data subjects regarding this transfer,

(iii) the unlawful and excessive processing of employees' identity card copies and criminal record certificates,

(iv) the failure to carry out prior security due diligence on a telemarketing service provider acting as a processor.

The Authority found that, after 27 December 2022, the controller continued to transfer data to the Serbian processor without renewing the standard contractual clauses, failed to conduct any Transfer Risk Assessment (TRA), and granted the processor unrestricted access to the SAP CRM database containing personal data of approximately 847,000 users.

The absence of clear information in the privacy notices regarding third-country transfers, the collection of excessive employee data despite the Data Protection Officer's warnings, and the lack of basic security controls over the processor were regarded as aggravating factors in determining the fine.

EDPS Strengthens Data Protection Approach for Artificial Intelligence

On 11 November 2025, the European Data Protection Supervisor (EDPS) published its Guidance on the Risk Management of Artificial Intelligence Systems, addressing the growing data protection risks linked to the use of AI by EU institutions. The Guidance sets out a structured risk management approach covering the design, procurement, deployment and monitoring of AI systems that process personal data.

The EDPS highlights that risks such as bias in training data, automated discrimination, inaccurate outputs, excessive data collection and weakening of data subjects' rights must be assessed at an early stage and continuously monitored throughout the lifecycle of AI systems. Particular emphasis is placed on the principles of fairness, accuracy, data minimisation, security and accountability.

The Guidance also underlines that interpretability and explainability are essential requirements for lawful AI use. According to the EDPS, reliance on "black-box" systems undermines transparency and makes it difficult for individuals to exercise their rights effectively. The document therefore signals a shift toward a more technology-aware and proactive data protection compliance model, in parallel with the forthcoming AI Act.

Guidelines on Generative Artificial Intelligence and the Protection of Personal Data Have Been Published

On 24 November 2025, the Turkish Personal Data Protection Authority published the Guidelines on Generative Artificial Intelligence and the Protection of Personal Data (in 15 Questions). The Guidelines are noteworthy for setting out the fundamental technical framework of generative AI by explaining its operating principles, content generation processes, model architecture and lifecycle. They also address the main areas of use of these technologies, as well as key risks such as hallucinations, bias, data security vulnerabilities, deepfakes and intellectual property infringements.

In addition, the Guidelines assess the obligations under Law No. 6698 within the context of generative AI, including the distinction between data controller and data processor, the conditions for processing personal data, core data protection principles, transparency and cross-border data transfers. They further provide guidance on how data subjects' rights should be exercised and how security measures should be implemented.

The document also includes practical recommendations for individuals in their daily use of generative AI, as well as specific guidance for parents with regard to child users. In an ecosystem where artificial intelligence technologies are developing at a rapid pace, the publication of such a framework for the protection of privacy constitutes an important step toward strengthening public trust and promoting the responsible use of AI.

Digital Economy Partnership Agreement Submitted for the Approval of the TBMM

The Organization of Turkic States (TDT) has taken a significant step that will strengthen digital trade and data security on a common ground.

The Digital Economy Partnership Agreement, signed in Bishkek on November 6, 2024, among TDT member countries, has entered the ratification process in Türkiye, and the relevant legislative proposal has been submitted to the Grand National Assembly of Türkiye (TBMM). While aiming to increase cooperation in the digital economy, the Agreement dedicates a specific article to the protection of personal data.

Article 19 of the Agreement imposes an obligation on the State Parties to establish a national legal framework regarding personal data protection or to maintain existing regulations. Furthermore, it envisages the determination of clear rules for cross-border data transfer, the public availability of information regarding the rights of individuals and the obligations of enterprises, and the enhancement of transparency in data protection practices.

This regulation bears importance as it facilitates secure data flow among TDT countries, establishes common standards in digital trade, and strengthens transparency regarding the protection of personal data. The Agreement is considered a strategic step towards the establishment of a common digital market in the Turkic world.

KVKK Approved Data Transfer Abroad Within the Scope of the Agreement Between the Presidency of Migration Management and UNHCR

The Personal Data Protection Authority shared an important decision regarding the transfer of personal data abroad with the public via an announcement published on November 10, 2025.

In the announcement, it was stated that an agreement not in the nature of an international treaty, signed between the Presidency of Migration Management of the Ministry of Interior and the United Nations High Commissioner for Refugees (UNHCR), was evaluated as the basis for data transfer.

The Board examined the agreement in question within the scope of Article 11 of the Regulation on Procedures and Principles Regarding the Transfer of Personal Data Abroad and concluded that the agreement contains the necessary safeguards and protection mechanisms for the transfer of personal data abroad. As a result of this evaluation, permission was officially granted on October 21, 2025, for the transfer of personal data abroad within the framework of the aforementioned agreement.

This decision draws attention as it constitutes a concrete example regarding the scope of application of the provision regulating the permission for personal data transfer through "agreements not in the nature of an international treaty," regulated under Article 9, paragraph 4, subparagraph (a) of the Law.

Basaran Law Firm
Istanbul · Türkiye

For further details about our practice areas or to discuss how we may assist you
Please reach us at:

E-mail: info@basaranlawfirm.com
www.linkedin.com/company/basaran-law-firm
www.basaranlawfirm.com

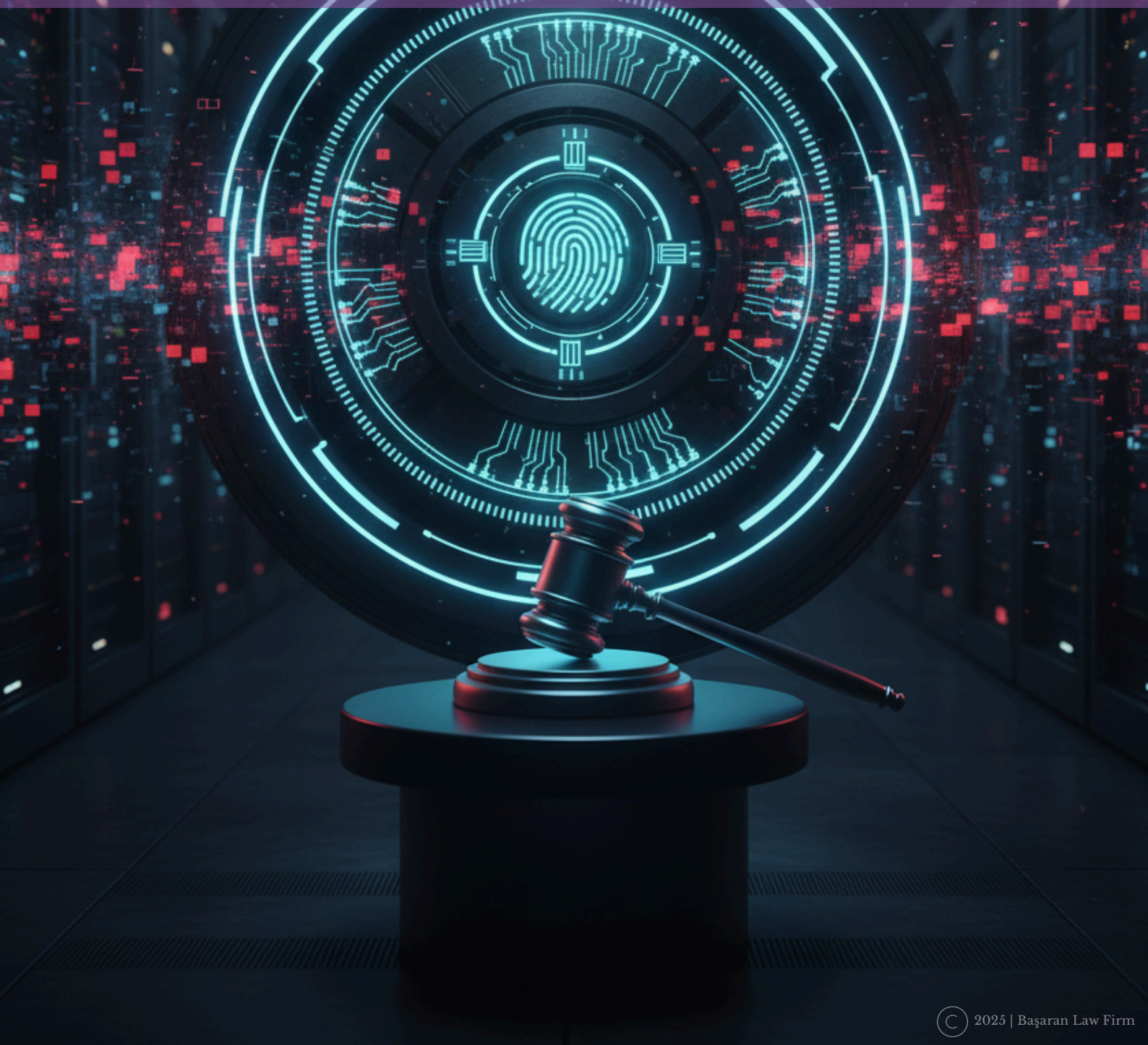
*This newsletter is prepared solely for informational purposes and does not constitute any legal advice for a specific case or client.

THE PULSE

BAŞARAN LAW FIRM

Aralık 2025
Sayı: 02

Veri Koruma Alanındaki Hukuki Düzenlemeler



© 2025 | Başaran Law Firm

Daha Az Bürokrasi, Daha Güçlü Bir Yapı: AB'nin Dijital Omnibus Paketi

19 Kasım 2025 tarihinde Avrupa Komisyonu, AB'nin dijital mevzuat yapısını sadeleştirmeyi ve bunu yaparken yüksek veri koruma standartlarını muhafaza etmeyi amaçlayan Dijital Omnibus Teklifini yayımladı. Teklif; GDPR, ePrivacy Direktifi, NIS2 ve Veri Yasası (Data Act) gibi temel düzenlemeleri sadeleştirerek, kişisel verilerin korunmasından ödün vermeksizin uyum maliyetlerini azaltmayı hedeflemektedir.

Teklifte yer alan en dikkat çekici değişikliklerden biri, uzun süredir eleştirilen GDPR ile ePrivacy Direktifi arasındaki ikili yapıya ilişkindir. Kişisel verilere erişime ilişkin kurallar tamamen GDPR kapsamına alınıyor ve böylece mükerrer rıza yükümlülükleri ortadan kaldırılıyor. Kullanıcı tercihleri, hizmet sağlayıcıların uymakla yükümlü olduğu otomatik ve makine tarafından okunabilir tarayıcı veya uygulama ayarları yoluyla ifade edilecek. Bu düzenlemenin hem kullanıcılar açısından "rıza yoğunluğunu", hem de işletmeler açısından uyum yükünü önemli ölçüde azaltması beklenmektedir.

GDPR'a yönelik hedefli değişiklikler de teklif kapsamında yer almaktadır. Buna göre; kişisel veri kavramı içinde "makul şekilde tanımlanabilirlik" vurgusu netleştirilmekte, veri sorumlularına kötüye kullanım niteliği taşıyan erişim talepleriyle mücadelede daha fazla esneklik tanınmakta ve veri ihlali bildirim yükümlülüğü yalnızca yüksek riskli olaylarla sınırlandırılmaktadır. Ayrıca bildirim süresi 96 saate çıkarıldı. Bunun yanında, yapay zekâ eğitim sürecinde kaçınılmaz olarak ortaya çıkabilecek özel nitelikli kişisel verilerin sınırlı ve sıkı denetime tabi artık işlenmesine de kontrollü şekilde izin verilmektedir.

Paralel olarak, farklı AB mevzuatları kapsamında öngörülen kişisel veri ihlali ve siber güvenlik olayı bildirimleri, ENISA tarafından işletilecek tek bir AB düzeyinde bildirim platformu altında birleştirilmektedir. "Bir kez bildir, birçok kez paylaş" modeli esas alınarak oluşturulan bu yapı sayesinde, AB'nin yüksek kişisel veri koruma seviyesinden taviz verilmeden önemli ölçüde idari tasarruf sağlanması amaçlanmaktadır.

AB, Veri ve Yapay Zekâda Yeni Bir Döneme Giriyor

Avrupa Komisyonu, aynı tarihte "Data Union Strategy – Yapay Zekâ İçin Verinin Önünün Açılması" başlıklı strateji belgesini de yayımlamış; Avrupa'nın veri ekonomisini güçlendirmeyi ve güvenilir yapay zekâ geliştirilmesini hızlandırmayı amaçlayan yol haritasını kamuoyu ile paylaşmıştır.

Strateji üç ana önceliğe odaklanmaktadır: yapay zekâ için yüksek kaliteli verilere erişimin ölçeklendirilmesi, AB veri mevzuatı çerçevesinin sadeleştirilmesi ve uluslararası veri akışlarında AB'nin küresel konumunun güçlendirilmesi.

Komisyon; sağlık, enerji, imalat, mobilite ve finans gibi kilit sektörlerde Avrupa veri alanlarının genişletilmesini ve birbirine entegre edilmesini planlamaktadır. Bu sayede şirketlerin ve araştırmacıların, yenilikçilik ve yapay zekâ eğitimi için daha büyük hacimlerde güvenilir verilere erişmesi mümkün olacaktır.

Strateji, aynı zamanda Dijital Omnibus girişimiyle yakın uyum içinde olup; sadeleştirilmiş kurallar, standart sözleşme maddeleri ve geliştirilmiş bulut yönetişimi yoluyla hukuki parçalanmışlığın ve uyum maliyetlerinin azaltılmasını hedeflemektedir.

Güvenilir ortaklarla adil ve güvenli sınır ötesi veri akışları teşvik edilirken, AB verilerinin üçüncü ülkeler tarafından haksız erişim ve kötüye kullanıma karşı korunması amaçlanmaktadır. Veri altyapısı ve bulut teknolojilerine yönelik hedefli yatırımlar yoluyla Komisyon, yüksek veri koruma ve siber güvenlik standartları korunmak kaydıyla, AB'yi veri ve yapay zekâ temelli inovasyonun küresel merkezlerinden biri hâline getirmeyi hedeflemektedir.

Güvencesiz Sınır Ötesi Veri Aktarımları Nedeniyle Yüksek GDPR Cezası

14 Kasım 2025 tarihinde Hırvatistan Kişisel Verileri Koruma Otoritesi, Genel Veri Koruma Tüzüğü (GDPR) ihlalleri nedeniyle bir telekomünikasyon işletmecisine 4,5 milyon Avro tutarında idari para cezası uygulamıştır.

Karar aşağıdaki ihlallere dayanmaktadır:

(i) Kişisel verilerin, geçerli bir aktarım mekanizması bulunmaksızın, grup şirketlerinden birine Sırbistan'a aktarılması,

(ii) Bu aktarıma ilişkin olarak ilgili kişilere şeffaf bilgilendirme yapılmaması,

(iii) Çalışanlara ait kimlik kartı kopyaları ve adli sicil kayıtlarının hukuka aykırı ve ölçüsüz şekilde işlenmesi.

(iv) Veri işleyen sıfatıyla faaliyet gösteren bir tele-pazarlama hizmet sağlayıcısı hakkında önceden herhangi bir güvenlik incelemesi (due diligence) yapılmaması.

Otorite, 27 Aralık 2022 tarihinden sonra veri sorumlusunun, standart sözleşme maddelerini yenilemeden Sırbistan'daki veri işleyiciye veri aktarmaya devam ettiğini, herhangi bir Aktarım Risk Değerlendirmesi (Transfer Risk Assessment – TRA) gerçekleştirmediğini ve yaklaşık 847.000 kullanıcıya ait kişisel verileri içeren SAP CRM veritabanına veri işleyiciye sınırsız erişim yetkisi tanıdığını tespit etmiştir.

Üçüncü ülkelere yapılan veri aktarımlarına ilişkin gizlilik bildirimlerinde açık ve yeterli bilgilendirme bulunmaması, Veri Koruma Görevlisinin uyarılarına rağmen çalışanlara ait aşırı veri toplanması ve veri işleyici üzerinde temel güvenlik kontrollerinin dahi uygulanmamış olması, idari para cezasının belirlenmesinde ağırlaştırıcı unsurlar olarak değerlendirilmiştir.

EDPS, Yapay Zekâ İçin Veri Koruma Yaklaşımını Güçlendirdi

11 Kasım 2025 tarihinde Avrupa Veri Koruma Denetçisi (EDPS), AB kurumları tarafından yapay zekâ kullanımına bağlı olarak ortaya çıkan veri koruma risklerini ele alan Yapay Zekâ Sistemlerinde Risk Yönetimine İlişkin Rehberini yayımlamıştır. Rehber, kişisel veri işleyen yapay zekâ sistemlerinin tasarımı, tedariki, devreye alınması ve izlenmesi aşamalarını kapsayan yapılandırılmış bir risk yönetimi yaklaşımı ortaya koymaktadır.

EDPS; eğitim verilerindeki önyargı (bias), otomatik ayrımcılık, hatalı çıktılar, aşırı veri toplama ve ilgili kişi haklarının zayıflaması gibi risklerin erken aşamada değerlendirilmesi ve yapay zekâ sistemlerinin tüm yaşam döngüsü boyunca sürekli olarak izlenmesi gerektiğini vurgulamaktadır.

Bu soruşturma, Komisyon'un yeni yetkilerini kullanmak için beklemediğini ve uyumu aktif şekilde izlediğini kanıtlıyor. Olası sonuçlar ciddi; bir şirketin toplam küresel cirosunun %10'una kadar para cezası uygulanabilir ve tekrar eden ihlallerde bu oran %20'ye çıkabilir. Bu durum, DMA'nın dijital ekonomide oyun alanını eşitlemek için güçlü bir araç olarak tasarlandığını ve özellikle medya gibi kritik sektörlerin korunmasına odaklandığını gösteriyor.

Özellikle adil işlem, doğruluk, veri minimizasyonu, güvenlik ve hesap verebilirlik ilkelerine özel önem atfedilmektedir.

Rehber ayrıca, yorumlanabilirlik ve açıklanabilirliğin (interpretability & explainability) hukuka uygun yapay zekâ kullanımı açısından temel gereklilikler olduğunu açıkça ortaya koymaktadır. EDPS'ye göre, "kara kutu" niteliğindeki sistemlere dayanılması şeffaflığı zedelemekte ve bireylerin haklarını etkin şekilde kullanmasını zorlaştırmaktadır. Bu yönüyle belge, yaklaşmakta olan Yapay Zekâ Tüzüğü (AI Act) ile paralel biçimde, daha teknoloji farkındalığı yüksek ve proaktif bir veri koruma uyum modeline geçişin sinyalini vermektedir.

Üretken Yapay Zekâ ve Kişisel Verilerin Korunması Rehberi yayınlandı

Kişisel Verileri Koruma Kurumu 24 Kasım 2025 tarihinde Üretken Yapay Zekâ ve Kişisel Verilerin Korunması Rehberi'ni (15 Soruda) yayınladı. Bu rehber üretken yapay zekânın çalışma prensiplerini, içerik üretim süreçlerini, model yapısını ve yaşam döngüsünü açıklayarak temel teknik çerçeveyi ortaya koyması ile ilgi çekiyor. Rehberde ayrıca bu teknolojilerin kullanım alanları ile halüsinasyon, ön yargı, veri güvenliği, deep fake ve fikri mülkiyet ihlalleri gibi riskler ele alınıyor.

Bunun yanında Rehber; veri sorumlusu–veri işleyen ayrımı, kişisel veri işleme şartları, temel ilkeler, şeffaflık ve yurt dışına aktarım gibi 6698 sayılı Kanun kapsamındaki yükümlülükleri değerlendiriyor; ilgili kişilerin haklarının nasıl kullandırılacağı ve güvenlik tedbirlerinin nasıl uygulanacağına ilişkin açıklamalar sunuyor. Ayrıca bireylerin günlük kullanımda dikkat etmesi gereken hususlar ile çocuk kullanıcılar bakımından ebeveynlere yönelik önerilere de yer vermekte.

Yapay zekâ teknolojilerinin hızla geliştiği bir ekosistemde, mahremiyetin korunmasına yönelik böylesi bir çerçevenin yayımlanması; toplumsal güvenin güçlendirilmesi ve sorumlu yapay zekâ kullanımının teşvik edilmesi açısından önemli bir adım niteliğinde.

Dijital Ekonomi Ortaklık Anlaşması TBMM'nin Onayına Sunuldu

Türk Devletleri Teşkilatı (TDT), dijital ticaret ve veri güvenliğini ortak bir zeminde güçlendirecek önemli bir adım attı. TDT üyesi ülkeler arasında 6 Kasım 2024'te Bişkek'te imzalanan Dijital Ekonomi Ortaklık Anlaşması, Türkiye'de onay sürecine girdi ve Anlaşmanın uygun bulunmasına dair 27/11/2025 tarihli Kanun teklifi yayımlandı.

Anlaşma, dijital ekonomide iş birliğini artırmayı hedeflerken özellikle kişisel verilerin korunmasına özel bir madde ayırıyor. Anlaşmanın 19. maddesi, taraf devletlere kişisel veri korumasına ilişkin ulusal bir yasal çerçeve oluşturma veya mevcut düzenlemeleri sürdürme yükümlülüğü getiriyor.

Ayrıca sınır ötesi veri aktarımı için açık kurallar belirlenmesi, bireylerin haklarına ve işletmelerin yükümlülüklerine ilişkin bilgilerin kamuya açık şekilde sunulması ve veri koruma uygulamalarında şeffaflığın artırılması öngörülüyor. Bu düzenleme, TDT ülkeleri arasında güvenli veri akışını kolaylaştırması, dijital ticarette ortak standartlar oluşturması ve kişisel verilerin korunması konusunda şeffaflığı güçlendirmesi nedeniyle önem taşıyor. Anlaşma, Türk dünyasında ortak bir dijital pazarın kurulmasına yönelik stratejik bir adım olarak değerlendiriliyor.

Bir İlk: Anlaşma Kapsamında Yurt Dışına Veri Aktarımına Onay Verildi

Kişisel Verileri Koruma Kurumu, 10 Kasım 2025 tarihinde yayımladığı duyuru ile, kişisel verilerin yurt dışına aktarılmasına ilişkin önemli bir kararını kamuoyu ile paylaştı. Duyuruda, İçişleri Bakanlığı Göç İdaresi Başkanlığı ile Birleşmiş Milletler Mülteciler Yüksek Komiserliği (BMMYK) arasında imzalanan uluslararası sözleşme niteliğinde olmayan bir anlaşmanın, veri aktarımına dayanak olarak değerlendirildiği belirtildi.

Kurul, söz konusu anlaşmayı Kişisel Verilerin Yurt Dışına Aktarılmasına İlişkin Usul ve Esaslar Hakkında Yönetmelik'in 11. maddesi kapsamında inceleyerek anlaşmanın kişisel verilerin yurt dışına aktarımında gerekli güvence ve koruma mekanizmalarını içerdiği sonucuna ulaştı. Bu değerlendirme sonucunda, kişisel verilerin anılan anlaşma çerçevesinde yurt dışına aktarımına resmî olarak izin verildi.

Bu karar, Kanun'daki "uluslararası sözleşme niteliğinde olmayan anlaşmalar" yoluyla kişisel veri aktarımına izin verilebilmesine ilişkin hükmün uygulama alanına dair somut bir örnek oluşturması bakımından dikkat çekiyor.

Basaran Law Firm
İstanbul · Türkiye

Hizmet alanlarımız hakkında daha fazla bilgi almak veya size nasıl yardımcı olabileceğimizi görüşmek için lütfen bizimle iletişime geçin:

E-posta: info@basaranlawfirm.com
www.linkedin.com/company/basaran-law-firm
www.basaranlawfirm.com

Bu bülten yalnızca bilgilendirme amacıyla hazırlanmıştır; herhangi bir somut olay veya müvekkile yönelik hukuki görüş niteliği taşımaz.