Personal Data Protection Bulletin

2025
Fourth Quarter

Sevgi Ünsal Özden
Gülnur Çakmak Ergene
Fuat Sarı

www.erdem-erdem.av.tr

Developments from Türkiye

The VERBİS Q&A and the VERBİS Guide Updated

On 7 October 2025, the Personal Data Protection Authority (Authority) updated the documents titled "VERBİS Q&A" and the "VERBİS Guide", which were published to assist data controllers in fulfilling their registration and notification obligations under Article 16 of the Law on the Protection of Personal Data No. 6698 (KVKK) through the Data Controllers' Registry Information System (VERBİS).

> You may access in Turkish the Authority's announcement here, the updated VERBİS Guide here, and the VERBİS in Questions document here.

First Authorization Granted for Cross-Border Transfer of Personal Data with an Agreement Not Having the Status of an International Treaty

The Authority announced that permission was granted for the transfer of personal data by the Turkish Directorate General of Migration Management of the Ministry of Interior to the United Nations High Commissioner for Refugees, within the scope of an agreement executed between the parties that does not have the status of an international treaty.

> You may access the announcement published by the Authority in Turkish here.

Guidance on Generative AI and the Protection of Personal Data Published

On 24 November 2025, the Authority published the "Guidance on Generative AI and the Protection of Personal Data (In 15 Questions)" (Guidance). The Guidance assesses, within the framework of the KVKK, personal data processing activities arising during the development and use of generative AI systems across different sectors, based on a lifecycle approach and addresses the content generation processes, areas of use, legal risks, and the obligations of data controllers and data processors. In addition, the Guidance includes matters to be considered regarding the protection of personal data in the use of generative AI applications, particularly in respect of individuals and children.

> You may access the announcement published by the Authority here, and our announcement on this matter here.

Principle Decision Published on the Retention of Copies of Turkish Identity Cards by Hotels

The Personal Data Protection Board (Board)'s Principle Decision dated 06 November 2025 and numbered 2025/2120 (Principle Decision) requires a change in the current practices of establishments providing accommodation services, such as hotels. Accordingly, while the recording

of name, surname, and identity number is lawful under the Identity Notification Law No. 1774 and the relevant legislation, it is stated that the retention of copies of identity cards results in the processing of excessive personal data beyond the purposes of processing, that special categories of personal data were obtained in a manner exceeding the purpose due to older identity cards containing information on religion and blood type, and that such practice lacks a legal basis. In this context, it was decided that this practice must be discontinued and that previously collected and retained copies of identity cards must be destroyed.

You may access the announcement published by the Authority in Turkish here, and our announcement on this matter here.

Key Actions

- ✓ Data controllers providing accommodation services, such as hotels and guesthouses, should discontinue the collection and retention of copies of identity cards and should record only the name, surname and Turkish Identity Number during identity verification. Identity card copies previously collected in this manner should be identified and destroyed, and privacy notices, policies and procedures should be revised in line with the Principle Decision.

Biometric Authentication in Payment Services Framework Agreements Has Been Given a Legal Basis

With Law No. 7571, published in the Official Gazette dated 25 December 2025 and numbered 33118, the Law on Payment and Securities Settlement Systems, Payment Services, and Electronic Money Institutions No. 6493 was amended. Within the scope of this amendment, an explicit legal basis was introduced for the use of biometric authentication methods, such as fingerprint and facial recognition, as well as electronic identity verification tools, during the establishment of payment services framework agreements.

You may access Law No. 7571 here, and our announcement on this matter here.

Key Actions

- ✓ Data controller banks and all other actors falling within the scope of the relevant legislation should review their privacy notices, policies and procedures prepared in relation to data subjects and align them with the current legislation.

2026 Presidential Annual Program Includes the Objective of Aligning KVKK with GDPR

In the 2026 Presidential Annual Program, published in the Official Gazette dated 30 October 2025 and numbered 33062 (repeated), it was stated that the efforts carried out to align KVKK with European Union General Data Protection Regulation (GDPR) are aimed to be completed within 2026.

> You may access the 2026 Presidential Annual Program here.

Institutional Governance in the Field of AI Has Been Strengthened

With the Presidential Decrees published in the Official Gazette dated 25 December 2025 and numbered 33118, the institutional structuring in the field of AI within public administration was strengthened. In this context, Presidential Decree No. 191 renamed the General Directorate of National Technology operating under the Ministry of Industry and Technology as the General Directorate of National Technology and AI and expanded its remit to cover the development of policies and strategies relating to AI technologies, as well as legislative and infrastructure efforts.

Under Presidential Decree No. 192, the scope of duties of the Cyber Security Presidency was expanded to include the digital government domain and AI applications in the public sector; within this framework, the General Directorate of Public Artificial Intelligence, the General Directorate of Digital Government, the General Directorate of Administrative Services, and the Strategy Development Department were established.

> You may access the full text of Presidential Decree No. 191 here, and the full text of Presidential Decree No. 192 here.

Amendments Introduced to the Regulation on Personal Health Data

With the amendment published in the Official Gazette dated 03 December 2025 and numbered 33096, significant changes were introduced regarding the processing of personal health data and access to such data. Within the scope of the amendment, the requirement for a specific authorization in the power of attorney for lawyers to access their clients' health data was abolished, and an explicit reference was made to Article 6/3 of KVKK, thereby limiting physicians' access authorities in accordance with this provision.

In addition, access to health data and security settings through the e-Nabız system was restructured; the retention period for health data of deceased persons was extended from 20 years to 30 years;

and access conditions in cases of custody, caregivers, and detention/imprisonment were clarified.

> You may access the amending regulation here, and our announcement for further details here.

New Regulation on Promotional and Informational Activities in Health Services Published

With the Regulation on Promotional and Informational Activities in Health Services (Regulation), which was published in the Official Gazette dated 12 November 2025 and numbered 33075 and entered into force on the same date, the procedures and principles governing promotional and informational activities carried out by healthcare professionals, private healthcare facilities, and intermediary organizations for international health tourism were regulated. The Regulation sets out the advertising ban on health services, the fundamental principles to be observed in promotional and informational activities, and obligations relating to patient privacy and the protection of personal data. In this context, obtaining the patient's explicit consent was made mandatory for the use of visual content relating to patients, and it was stipulated that promotional and informational activities must be conducted in compliance with KVKK and the provisions of the Regulation on Personal Health Data.

> You may access the Regulation on Promotional and Informational Activities in Health Services here.

Current Developments from the World

European Commission Launches New AI Act Implementation Tools

The European Commission (Commission) has launched the Artificial Intelligence (AI) Act Service Desk, the AI Act Single Information Platform (Platform), and a whistleblower tool to support the implementation of the European Union (EU) Artificial Intelligence Act (AI Act). The Platform provides a central access point for information on the AI Act, including guidance materials, FAQs, and digital tools such as a compliance checker, an AI Act explorer, and a dedicated channel for submitting questions to the Service Desk. In addition, the whistleblower tool provides a secure and confidential channel for individuals to report suspected breaches directly to the EU AI Office, with encrypted follow-up communication and the possibility to submit reports in all EU official languages.

EC's announcement on the AI Act Service Desk and the AI Act Single Information Platform is available here, and the announcement on the AI Act whistleblower tool is available here.

European Data Protection Supervisor Published Guidance for Risk Management of AI Systems

On 11 November 2025, the European Data Protection Supervisor (EDPS) published the "Guidance for Risk Management of Artificial Intelligence Systems" applicable to EU institutions, bodies, and agencies subject to the Regulation (EU) 2018/1725 (EUDPR). The Guidance outlines a risk-based framework for identifying and mitigating data protection risks associated with AI systems, particularly in relation to fairness, accuracy, data minimization, security, and data subject rights, and emphasizes the importance of accountability, governance structures, and lifecycle-wide risk management. It also notes that a Data Protection Impact Assessment (DPIA) should be carried out where AI use may pose high risks to individuals' rights and freedoms.

You may access the Guidance here.

Key Actions

- ✓ Organizations developing, procuring or using AI systems should identify and document data protection risks throughout the AI lifecycle, and conduct a DPIA where AI use may pose high risks to individuals' rights and freedoms. Controllers should also ensure clear governance and accountability for AI systems.

European Commission Published the Digital Omnibus Regulation Proposal

On 19 November 2025, the Commission published its Digital Omnibus Proposals, introducing targeted amendments to the GDPR, AI Act, Data Act, and related digital legislation with the aim of simplifying the EU digital regulatory framework. The proposal includes clarifications on the processing of personal data for AI training, adjustments to data breach notification obligations through a single-entry reporting mechanism, changes to cookie consent and terminal equipment rules, and harmonization of DPIA requirements at the EU level. It also proposes simplifications under the AI Act, including adjusted compliance timelines and reduced administrative burdens for SMEs and small mid-cap companies.

> You may access the Digital Omnibus Regulation Proposal here and the Proposal amending the AI Act here .

European Banking Authority Published an Information Note on the Implications of the AI Act for the Banking and Payments Sector

In its information note titled "AI Act: implications for the EU banking and payments sector," published on 21 November 2025, the European Banking Authority (EBA) examined the potential implications of the AI Act for the banking and payments sector. The paper confirms that AI systems for creditworthiness and credit scoring of natural persons qualify as high-risk AI systems and notes that the AI Act is complementary to existing EU banking and payment legislation, with no immediate need to amend current EBA Guidelines.

> You can access the relevant paper here.

UK Parliament Introduced a Bill Proposing Comprehensive Regulations on Cyber Security and Resilience

The Cyber Security and Resilience (Network and Information Systems) Bill was introduced to the United Kingdom (UK) Parliament on 12 November 2025. The Bill proposes significant reforms to the Network and Information Systems Regulations 2018 (NIS) by expanding its scope to additional sectors and service providers, introducing stricter and time-bound incident notification obligations, and strengthening enforcement and penalty regimes. The Bill is expected to enter into force in 2026 through a phased implementation supported by secondary legislation.

> You may access the Cyber Security and Resilience Bill here.

Belgian Data Protection Authority Fines Data Broker Infobel for Unlawful Resale of Personal Data

On 27 November 2025, the Belgian Data Protection Authority imposed a EUR 40,000 administrative fine on the data broker Infobel for reselling personal data for direct marketing purposes without valid consent, in breach of the GDPR. The Authority found that the personal data, originally obtained from a telecommunications operator, was resold without data subjects being properly informed and without obtaining specific and unambiguous consent for resale. The decision also ordered the deletion of personal data lacking a valid legal basis and required Infobel to inform its corporate customers of the decision and the unlawfulness of the consent relied upon.

> You may access the decision here.

The Commission Publishes First Draft Code of Practice on Transparency of AI-Generated Content

On 17 December 2025, the Commission published the first draft Code of Practice on the transparency of AI-generated content under the AI Act. The draft is intended to support compliance with the AI Act's transparency obligations and sets out rules on the labeling and detectability of AI-generated or manipulated content, including specific transparency rules for deepfake content. Following further expert and stakeholder consultations, a second draft is expected in March 2026, with the final version, which is expected to serve as a voluntary compliance tool for providers and deployers of generative AI systems.

> You may access the draft Code of Practice here.

Australian Data Protection Authority Publishes Guidance on the Use of Generative AI in the Workplace

On 4 December 2025, the Office of the Australian Information Commissioner (OAIC) published guidance on the use of generative AI tools in the workplace, such as ChatGPT and similar platforms. OAIC reiterated that organizations subject to the Privacy Act should avoid entering personal and sensitive information into public GPAI tools, as such may be difficult or impossible to control or delete once disclosed. The guidance emphasizes that misuse of GPAI can result in unauthorized disclosures, inaccurate outputs, flawed decision-making and regulatory exposure. OAIC underlines the need for strong privacy governance, including DPIA, clear internal policies, staff training, and technical controls, when GPAI tools are used in business operations.

> You may access the guidance here.

Key Actions

- ✓ Organizations using GPAI tools in the workplace should, where possible, prohibit the input of personal and sensitive data into publicly available AI tools and assess whether a DPIA is required for AI-enabled processes. Internal policies, staff training, and technical controls should be implemented to manage risks related to unauthorized disclosure, inaccurate outputs and regulatory exposure.

Australia Bans Social Media Use for Children Under 16

Australia has introduced legislation establishing a minimum age of 16 for access to age-restricted social media platforms, making it the first country to adopt a nationwide framework of this kind. Under the new rules, social media platforms are required to take reasonable steps to prevent users under 16 from holding accounts, while no penalties apply to children, parents, or carers. Platforms that fail to comply may face civil penalties of up to AUD 49.5 million. The regime relies on flexible age-assurance measures, guided by the eSafety Commissioner, rather than mandating specific age-verification technologies.

> You may access the related announcement here.

The Commission Imposes First Fine Under the Digital Services Act on X

On 5 December 2025, the Commission adopted its first non-compliance decision under the Digital Services Act (DSA), imposing a EUR 120 million fine on X. The Commission found that X breached its transparency obligations by presenting paid "blue checkmark" accounts as verified without meaningful identity checks, misleading users about the authenticity of accounts and content. The decision also identified deficiencies in X's advertising repository, including limited accessibility and the absence of key information such as the content of ads and the identity of the paying entity, which restricted public and civil society scrutiny. In addition, X was found to have imposed unjustified restrictions on researchers' access to publicly available platform data.

> You may access the press release here.

Italian Data Protection Authority Fines Curtarolo Municipality for Unlawful Use of CCTV Footage in Disciplinary Proceedings

On 23 October 2025, the Italian Data Protection Authority imposed a EUR 15,000 administrative fine on the Curtarolo Municipality for unlawfully using urban security CCTV footage in an employment-related disciplinary investigation. The authority found that video recordings collected for public security purposes were repurposed to monitor an employee's conduct, violating the purpose limitation, lawfulness, and transparency principles under the GDPR. The decision also identified failures to provide adequate privacy notices, to carry out a DPIA for large-scale public surveillance, and to comply with safeguards applicable to employee monitoring under Article 88 GDPR and national labor law.

You may access the decision in Italian here.

Key Actions

- ✓ Employers should avoid using CCTV footage collected for security purposes for employee monitoring or disciplinary investigations. Where video surveillance is in place, organizations should assess DPIA requirements, ensure appropriate privacy notices, and comply with employee monitoring safeguards under GDPR and labor law.

Email Newsletters May Constitute Direct Marketing under the ePrivacy Directive

In its judgment of 13 November 2025 (Case C-654/23, Inteligo Media), the Court of Justice of the EU (CJEU) held that the sending of a daily email newsletter may constitute direct marketing under Article 13 of the ePrivacy Directive, even where the content is informational, if it is designed to promote access to paid content or subscriptions. The CJEU further clarified that email addresses collected during registration for a free online account may be regarded as having been obtained "in the context of the sale of a service" within the meaning of Article 13(2), where the free service forms part of a broader commercial offering aimed at promoting paid services and involves indirect remuneration. In such circumstances, and provided that users are clearly informed and given an easy and free opt-out at the time of collection and in each message, the controller may rely on the ePrivacy soft opt-in regime, without the need to identify a separate legal basis under Article 6 GDPR, pursuant to Article 95 GDPR.

You may access the decision here.

Key Actions

- ✔ Organizations sending newsletters, announcements or promotional emails should assess whether such communications qualify as direct marketing and review at which stage email addresses are collected. Where activities fall within the scope of EU law, organizations subject to the ePrivacy Directive should evaluate whether the soft opt-in regime under Article 13(2) applies.

The CJEU Rules That Online Marketplaces May Qualify as (Joint) Data Controllers Under the GDPR

In X v Russmedia (C-492/23), the CJEU held that operators of online marketplaces may qualify as (joint) data controllers where they actively shape the dissemination of user-generated content for their own commercial purposes.

The Court clarified that, where advertisements contain sensitive data under Article 9 GDPR, platforms cannot rely solely on a notice-and-takedown approach. They must implement pre-publication safeguards to identify such ads and verify whether the advertiser is the data subject. If not, publication must be refused unless the advertiser demonstrates the data subject's explicit consent or another Article 9(2) exception.

The Court further confirmed that the hosting liability exemption under the e-Commerce Directive does not limit GDPR responsibility where the platform's role is active rather than purely technical or passive.

You may access the decision here.

Key Actions

- ✔ Platforms operating online marketplaces or similar services should assess whether their involvement in the dissemination of user-generated content triggers (joint) controller status and ensure that their content management and moderation practices appropriately reflect data protection principles, particularly where advertisements may contain special categories of personal data, without relying solely on notice-and-takedown or hosting safe-harbor arguments where their involvement goes beyond a purely technical or passive role.

Key Contacts

Sevgi Ünsal Özden
Managing Associate and Mediator

sevgiunsal@erdem-erdem.com

Disclaimer

İSTANBUL

Ferko Signature
Büyükdere Caddesi, No. 175 Kat. 3
34394, Esentepe - Şişli, İstanbul

+90 212 291 73 83
+90 212 291 73 82

istanbul@erdem-erdem.av.tr

İZMİR

1476 Sokak, No. 2, D. 27, Aksoy
Plaza Alsancak, İzmir

+90 232 464 66 76
+90 232 466 01 21

izmir@erdem-erdem.com

AMSTERDAM

Office 4.31, Strawinskylaan 457,
1077 XX Amsterdam

+31 (0)20 747 1113

amsterdam@erdem-erdem.nl

www.erdem-erdem.av.tr