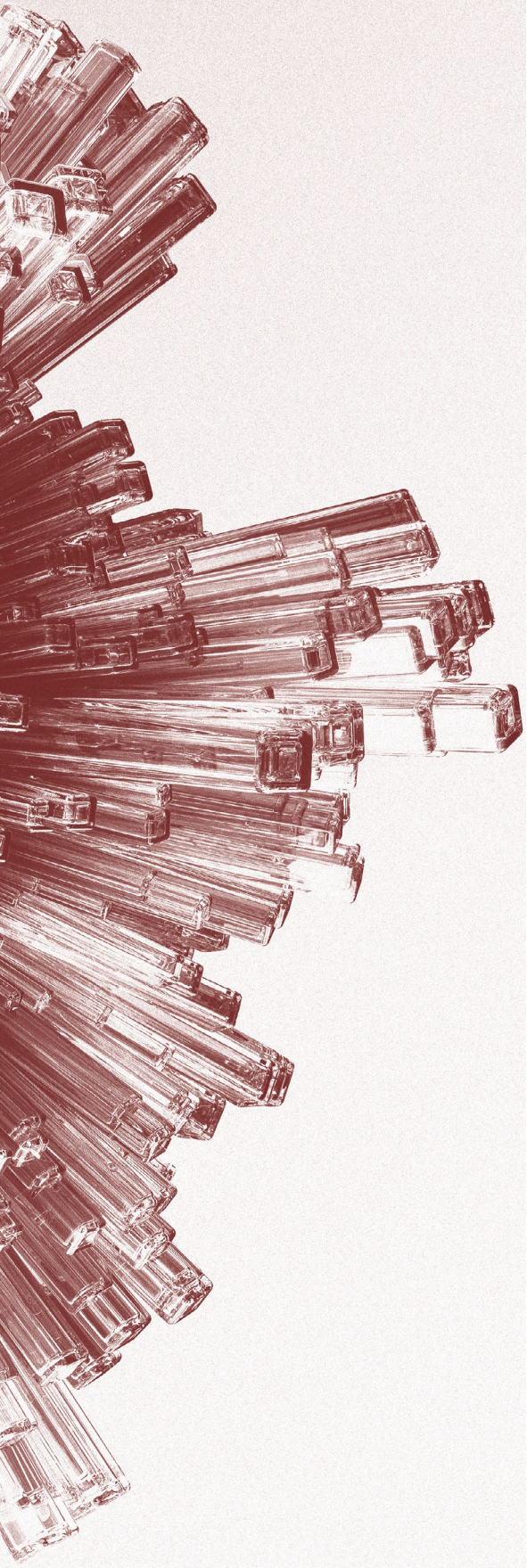


ERDEM & ERDEM

Personal Data Protection Bulletin

2025
Second Quarter

Sevgi Ünsal Özden
Gülnur Çakmak Ergene
İpek Ertem

Current Developments from Türkiye

The Personal Data Protection (the Authority) Published the Glossary of Personal Data Protection Terms

The "Glossary of Personal Data Protection Terms," published by the Authority, brings together definitions of one hundred selected terms related to personal data protection. These definitions were compiled from the Law on the Protection of Personal Data No. 6698 (KVKK), relevant legislation, and national studies, as well as from sources such as European Union regulations, the European Data Protection Board (EDPB), the European Data Protection Supervisor (EDPS), the International Association of Privacy Professionals (IAPP), and similar organizations. The glossary aims to provide easier access to key concepts associated with personal data protection by compiling them in a single resource.

> You can access the Glossary published by the Authority in Turkish here.

The Authority Published a Public Announcement on the Use of the Revenue Administration's E-Notification System for Serving Administrative Fines

The Authority has announced that the notification process for administrative fines will now be carried out via the E-Notification System of the Revenue Administration under the Ministry of Treasury and Finance. The new system will operate based on the infrastructure established under the Tax Procedure Law No. 213, and notifications will be deemed served on the fifth day following their delivery to the recipient's registered email address. Notifications to data controllers who are not tax liable will continue to be made in accordance with the previous procedure.

> You can access the Public Announcement published by the Authority in Turkish here and our related announcement here.

The Authority Published Recommendations on the Protection of Personal Data During Travel and Accommodation

The Authority has published an information note outlining recommendations for ensuring personal data security during travel and holiday periods.

The recommendations include being cautious of fake reservation notifications, avoiding the sharing of ticket or boarding pass images, reading privacy notices carefully, exercising discretion in social media posts, conducting sensitive transactions over secure connections, using strong passwords, and enabling remote access security measures on mobile devices.

> You can access the Recommendations published by the Authority in Turkish here.

The Personal Data Protection Board (the Board) Published a Principle Decision Requiring the Termination of Obtaining Explicit Consent via SMS

The Board published its Principle Decision dated June 10, 2025, and numbered 2025/1072 in the Official Gazette dated June 26, 2025, and numbered 32938.

In the decision, the Board assessed that the use of SMS verification codes sent during service processes such as payment, registration, or membership to obtain explicit consent or commercial communication approval without providing adequate information to data subjects constitutes a violation. The Board emphasized that the obligation to inform must be fully fulfilled, and that explicit consent must be obtained freely and separately for each processing activity. It was also underlined that presenting explicit consent as a prerequisite for receiving a service does not constitute valid consent.

You can access the text of the Principle Decision in Turkish here and our related announcement here.

Key Actions

- ✔ In transactions where a verification code is sent, data subjects must be informed in a clear, comprehensible, and layered manner both prior to the transaction and within the SMS content.
- ✔ Obtaining membership approval, commercial communication consent, and personal data processing consent through a single action should be avoided; separate explicit consent mechanisms must be provided for each.
- ✔ Commercial electronic communication consent must not be presented as a prerequisite for receiving the service; it should be clearly stated that individuals who do not give explicit consent can still benefit from the service.
- ✔ Personnel involved in these processes should receive regular training, and practices should be periodically reviewed to ensure compliance with applicable legislation.

Current Developments from the World

EDPB Published the Final Version of Guidelines 02/2024 on Article 48 of the General Data Protection Regulation (GDPR)

EDPB published Guidelines 02/2024 on Article 48 of the GDPR on 4 June 2025, following the public consultation process.

The Guidelines explain the legal framework to be followed under the GDPR in cases where third country authorities request personal data directly from data controllers or data processors. The EDPB emphasizes that such requests can only be valid if there is a valid international agreement between the EU and the third-country and that in such cases, both the legal bases under Article 6 of the GDPR and the transfer provisions under Chapter V of the GDPR must be complied with.

> You can see the Guidelines here.

The Court of Justice of the European Union Published the 2024 Edition of the "Selection of Key Decisions"

The Court of Justice of the European Union published the new edition of the "Selection of Key Decisions," which contains summaries of the important judgments delivered in 2024.

The selection includes sample decisions on matters related to the protection of personal data, such as the processing of electronic communications data, biometric and genetic data, the scope of the GDPR, the definition of data controller, and legal remedies available in cases of violations.

> You can access the 2024 edition of the "Selection of Key Decisions" published by the CJEU here.

The European Commission Published a Question-and-Answer Document on Artificial Intelligence Literacy

The European Commission published a question-and-answer document on artificial intelligence literacy under Article 4 of the EU Artificial Intelligence Act.

The document outlines the obligations of artificial intelligence system providers, as well as individuals and organizations using such systems in non-personal and professional contexts, to ensure an adequate level of artificial intelligence literacy for their employees and representatives.

> You can access the question-and-answer document published by the European Commission here.

The National Security Agency (NSA) of the United States of America (USA) Published the Document Titled "Data Security in AI: Best Practices for Securing Data Used in the Training and Operation of AI Systems," Prepared Jointly with the Cybersecurity Agencies of Australia, New Zealand, and the United Kingdom

The document presents best practices for securing data used during the development, testing, and operation of artificial intelligence systems, in alignment with the NIST Artificial Intelligence Risk Management Framework. Recommendations include the use of digital signatures to ensure data integrity, tracking data provenance, preferring trusted infrastructures, and conducting continuous risk assessments throughout the lifecycle.

> You can access the document published by NSA here.

The United Kingdom Adopted a Series of New Regulations Reshaping Data Protection Rules

The United Kingdom adopted a series of new regulations reshaping data protection rules. Within the scope of the regulations, a new reform package introducing significant changes to the United Kingdom General Data Protection Regulation (UK GDPR), the Data Protection Act 2018, and the Privacy and Electronic Communications Regulations (PECR) was adopted. These changes, which will gradually enter into force as of June 2025, bring both flexibility and new obligations to data processing practices.

The changes under the reform include clarifying how personal information can be used for research purposes, removing certain restrictions on automated decision-making, specifying how certain cookies can be used without user consent, allowing, in some cases, charities to carry out email marketing without obtaining consent, requiring organizations to establish a procedure to handle data protection complaints, and introducing a new legal basis termed *"recognized legitimate interests."*

With the reform, the powers of the Information Commissioner's Office's authority have also been expanded, allowing for stronger oversight and the imposition of higher fines.

> You can access more detailed information about the reforms here.

The United Kingdom National Cyber Security Centre (NCSC) Published the "Cyber Security Culture Principles," Outlining the Cultural Foundation Needed for Organizations to Develop Effective Cyber Security Practices

The "Cyber Security Culture Principles" published by the NCSC recommend viewing cybersecurity as an integral part of organizational goals, creating an environment that encourages secure behavior among employees, ensuring that leaders take responsibility in this area, and implementing clear security rules that everyone can understand.

NCSC also highlights the importance of collaboration among cybersecurity professionals, culture experts, and leaders in building a sustainable security culture. It underscores that not only technical measures, but also behavior and communication patterns shape culture. The United Kingdom strives to establish a secure digital society through this approach.

> You can access the Cyber Security Culture Principles published by the NCSC here.

The Irish Data Protection Commission (DPC) Imposed a 530 Million Euros Fine on TikTok for the Transfer of Personal Data to China

DPC concluded, following its investigation into TikTok regarding the transfer of user personal data to China, that TikTok had infringed the GDPR.

In the decision dated 2 May 2025, it was stated that the remote access-based transfer of data belonging to European Economic Area (EEA) users to China violated Article 46/1 of the GDPR, as an equivalent level of data protection to that in the EU was not guaranteed during such access. It was also determined that TikTok's privacy policy did not clearly specify the countries to which data was transferred and did not transparently explain the activities related to the transfer. For these reasons, DPC found that TikTok had also infringed the transparency obligation under Article 13/1-f of the GDPR, ultimately imposing a 530 million Euros fine on TikTok and requiring the company to bring its data transfer practices into compliance within 6 months.

> You can access the summary of the decision issued by the DPC here.

EDPB and EDPS Published a Joint Letter Supporting the Proposal on Simplification of Record-Keeping Obligations under the GDPR

The EDPB and EDPS published a joint letter regarding the draft legislation prepared by the European Commission, which proposes to simplify record-keeping obligations under Article 30/5 of the GDPR. The proposal aims to reduce the administrative burdens on data controllers and data processors without compromising data protection standards.

Within the scope of the proposed amendments, it is envisaged that the exemption

from record-keeping obligations will be extended to small mid-cap companies with fewer than 500 employees and to certain non-profit organizations, in addition to businesses with fewer than 250 employees; that the scope of the exemption will be redefined based on the concept of “high risk”; and that certain exceptions will be removed. In addition, an exemption from the record-keeping obligation is also planned for the processing of special categories of data carried out within the context of employment and social security law.

> You can access the joint letter published by the EDPB and EDPS here.

Global Cross-Border Privacy Rules and Privacy Recognition for Processors Certifications Published

The Global Cross-Border Privacy Rules Forum (Global CBPR Forum) launched the Global Cross-Border Privacy Rules Certification (Global CBPR) and the Privacy Recognition for Processors Certification (PRP) systems on June 2, 2025. Developed based on the existing Asia-Pacific Economic Cooperation (APEC) CBPR framework, these mechanisms enable data controllers and data processors to be voluntarily certified under internationally recognized privacy standards. Certified organizations undergo an independent audit to demonstrate their compliance with internationally recognized privacy and data protection standards.

The Global CBPR system automatically recognizes existing certifications under the APEC CBPR framework.

> You can access the certifications published by the Global CBPR Forum here.

The Higher Regional Court of Cologne (OLG Köln) Ruled that the Use of Personal Data for Artificial Intelligence Training Does Not Violate the Digital Markets Act (DMA)

In April 2025, Meta Platforms Ireland announced that it would begin using publicly available profile data of users for artificial intelligence training as of 27 May 2025, while allowing users to object to such processing. Following this announcement, the Consumer Association in North Rhine-Westphalia (Verbraucherzentrale NRW) filed for interim relief against Meta before the Higher Regional Court of Cologne.

In its decision dated 23 May 2025, OLG Köln ruled that Meta's use of publicly available content from Facebook and Instagram users in Europe for the training of artificial intelligence models does not violate Article 5/2-b of the DMA.

Based on the court's preliminary assessment, the processing activity carried out without user consent was deemed to rely on legitimate interest under the GDPR, and Meta's use of data for artificial intelligence development was considered lawful. For these reasons, the request for interim relief was rejected.

> You can access the decision published by OLG Köln here.

Brazil Launched a Pilot Project for the Commercialization of Personal Data

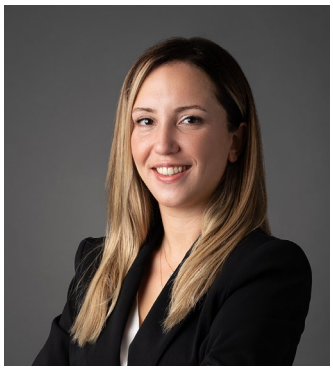
Brazil launched a pilot project for a digital wallet called "dWallet," which enables citizens to claim ownership of their digital data and generate income from it. The project is the first public-private partnership model implemented between government agencies and the private sector and is one of the first comprehensive initiatives in the world based on revenue sharing tied to personal data ownership. The project is carried out by Dataprev, the state-owned company providing IT services for Brazil's social security programs, in partnership with DrumWave, a U.S.-based company specializing in data valuation.

Users will be able to transfer data generated through their daily digital activities into a data savings account, and payments from companies that bid for these data will be deposited directly into the dWallet and transferred to users' bank accounts. Through this system, users will be able to generate financial gains beyond merely consenting to data sharing.

The legal basis of the project is a draft bill currently under discussion in the Brazilian Congress, which defines personal data as a type of property with economic value. If adopted, the bill will require companies to pay users in exchange for data collection, allowing citizens to treat their digital assets as economic resources.

> You can access the announcement published regarding the pilot project here.

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