# Personal Data Protection Bulletin

**2026**
Second Quarter

Sevgi Ünsal Özden
Gülnur Çakmak Ergene
Tuğçe Polat

# Current Developments from Türkiye

## Registration Period Extended for Data Controllers Required to Register with VERBİS Based on Their 2025 Annual Financial Balance Sheet Total

The Personal Data Protection Authority (Authority) announced that the registration period has been extended for data controllers that became subject to the obligation to register with the Data Controllers' Registry (VERBİS) based on their 2025 annual financial balance sheet total. Pursuant to the Personal Data Protection Law No. 6698 (KVKK) and the Regulation on the Data Controllers' Registry, data controllers are required to register with VERBİS within thirty days following the date on which the registration obligation arises. Accordingly, as the deadline for submitting 2025 corporate tax returns was 30 April 2026, the thirty-day registration period commenced as of that date.

Within this scope, the obligation to register with VERBİS applies to data controllers whose principal activity does not involve the processing of special categories of personal data and whose annual financial balance sheet total is TRY 100 million or more, as well as to data controllers whose principal activity involves the processing of special categories of personal data and whose annual financial balance sheet total is TRY 10 million or more.

With its Decision dated 13 May 2026 and numbered 2026/1026, the Personal Data Protection Board (Board) determined that, as the final week of the thirty-day registration period coincided with the Eid al-Adha holiday, the deadline for registration and notification was set as 5 June 2026. Accordingly, data controllers falling within the relevant scope were required to complete their VERBİS registration and notification procedures by that date.

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

## The Board Published a Principle Decision on the Processing of Biometric Data for Attendance Tracking

The Board's "Principle Decision on the Processing of Biometric Data for Attendance Tracking" was published in the Official Gazette dated 2 June 2026 and numbered 33268. Through the Principle Decision, the processing of employees' biometric data for attendance tracking purposes was assessed. The Board stated that, although employers are obliged to monitor employees' working hours, there is no explicit legal provision providing for such monitoring to be carried out through the processing of biometric data.

The Board also assessed that, due to the imbalance of power inherent in the employer–employee relationship, the explicit consent obtained from employees does not constitute a sufficient legal basis; and that, even where valid explicit consent has been obtained, the processing of biometric data for attendance tracking purposes would not be compatible with the principle of proportionality where less intrusive alternative methods are available. For this reason, the Board decided that attendance tracking should be carried out through alternative methods such as password-protected cards, PIN codes, RFID/NFC cards, or attendance sheets.

> You may access the Principle Decision in Turkish here and our announcement on this topic here.

## Public Announcement on the Use of Security Cameras in Apartment Buildings Published

The Authority published a public announcement on 8 June 2026 regarding the use of security camera systems in apartment buildings and residential complexes. The Authority stated that recording images through security cameras constitutes a personal data processing activity and that camera systems must be used in compliance with the KVKK and Condominium Law No. 634.

The announcement emphasized that cameras should be positioned in a manner that does not violate individuals' privacy, that facial recognition and audio recording features should not be used, that recordings should be retained only for the period necessary, that they should be protected against unauthorized access, and that the obligation to inform should be fulfilled.

> You may access the Authority's public announcement in Turkish here and our announcement on this topic here.

## Public Announcement on the Use of Security Cameras in Workplaces Published

The Authority published a public announcement on 8 June 2026 regarding the use of security camera systems in workplaces.

The announcement emphasized that security cameras may be used for legitimate purposes such as ensuring workplace security, occupational health and safety, and the prevention of crimes; however, cameras should not be used for the purpose of monitoring employees' attendance, performance, or general conduct. It was also stated that cameras should not be installed in private areas such as toilets, changing rooms, and rest areas; that audio recording should not be used unless its necessity has been demonstrated; that recordings should be retained only for the period necessary; and that the obligations regarding the obligation to inform and data security should be fulfilled.

> You may access the Authority's public announcement in Turkish here and our announcement on this topic here.

## Public Announcement on Live Broadcasts Conducted by Municipalities for Tourism Promotion Published

The Authority published a public announcement on 23 June 2026 regarding the live broadcasting over the internet of images obtained through cameras installed by municipalities in public areas such as streets, squares, parks, and beaches for tourism promotion purposes. The Authority stated that live broadcasts containing personal data, such as individuals' faces or vehicle licence plates, constitute a personal data processing activity even where the images are not recorded.

The Authority assessed that municipalities' duties and powers relating to tourism and promotional activities do not, in themselves, constitute a legal basis for such practices and that live broadcasts accessible to an unlimited number of individuals are not proportionate. For this reason, it was stated that the existing live broadcasts that enable individuals to be identified should be discontinued immediately and that promotional activities should be carried out through alternative methods that do not involve the processing of personal data.

> You may access the public announcement published by the Authority in Turkish here and our announcement on this topic here.

## The Principle Decision on the Processing of Personal Data of Accident Victims Was Published

The Board's "Principle Decision on the Processing of Personal Data of Accident Victims" was published in the Official Gazette dated 1 July 2026 and numbered 33297. In the Principle Decision, the Board made assessments regarding contacting accident victims against their wishes and the unlawful processing of their personal data.

The Board stated that the personal data of accident victims may only be processed for the purpose of carrying out post-accident procedures and in accordance with the personal data processing conditions set out under the KVKK. It was emphasized that insurance loss adjusters may use such data only within the scope of their statutory duties and powers, and that the transfer of such data to unauthorized persons may give rise to administrative and criminal liability. It was also stated that data controllers should restrict access in accordance with the principle of least privilege and implement the necessary technical and administrative measures.

> You may access the Principle Decision in Turkish here, and our announcement on this topic here.

## The Authority Published the Guide on the Processing of Personal Data in Reality Show Programs

The Authority published the "Guide on the Processing of Personal Data in Live-Broadcast Reality Show Programs", prepared in cooperation with RTÜK, on 12 May 2026. The Guide explains how personal data processing activities carried out during the preparation, broadcasting, and post-broadcast stages of such programs should be assessed under the KVKK.

The Guide states that personal data processing activities falling within the scope of freedom of expression may be exempt from the KVKK; however, this exemption does not apply where the right to privacy or personality rights are violated, or where the processing constitutes a criminal offence. It was further stated that such assessment should be made on a case-by-case basis by considering the balance between public interest, timeliness, accuracy, and the essence of the content and the way it is presented.

The Guide also explains that, in outsourced productions, the broadcaster and the producer may jointly act as data controllers; that individuals participating in the program in person or by telephone should be duly informed; and that the obligations relating to personal data processing conditions, data security, transfer, retention, and destruction should be complied with.

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

## The HSK Designated Specialized Courts for Cases Concerning the Decisions of the KVKK and the Competition Authority

The Council of Judges and Prosecutors (HSK) published its Decision dated 20 April 2026 and numbered 890, which designates the specialized courts having jurisdiction over cases arising from the decisions of certain regulatory and supervisory authorities, in the Official Gazette dated 22 April 2026 and numbered 33232. Accordingly, as of 1 June 2026, actions brought against the decisions of the Board will be heard by the Ankara 12th, 14th and 15th Administrative Courts, while cases arising from the decisions of the Competition Authority will be heard by the Ankara 10th, 13th and 25th Administrative Courts.

Cases filed before this date and currently pending will be concluded before the existing courts, whereas new cases will be transferred to the designated specialized courts.

> You may access the HSK Decision in Turkish here.

## Amendments Aimed at the Protection of Children in the Digital Environment Published

With Law No. 7578 on the Amendment of the Social Services Law and Certain Other Laws (Amendment Law), published in the Official Gazette dated 1 May 2026, amendments were made to Law No. 5651 on the Regulation of Publications on the Internet and Combating Crimes Committed by Means of Such Publications. Accordingly, social network providers are required not to provide services to children under the age of 15 and to take the necessary measures, including age verification. In addition, obligations were introduced regarding the provision of differentiated services for children who have attained the age of 15, the provision of parental control tools, and the prevention of misleading advertisements.

The Amendment Law also defines the fundamental concepts relating to games and introduces obligations regarding age ratings and parental control tools for gaming platforms, as well as the appointment of a representative in Türkiye by foreign-based gaming platforms meeting certain conditions. The provisions introducing sanctions such as administrative fines, advertising bans, and the reduction of internet traffic bandwidth in the event of non-compliance will enter into force on 1 November 2026.

> You may access the Amendment Law in Turkish here.

## Significant Amendments Made to the Regulation on Commercial Advertising and Unfair Commercial Practices

With the Regulation Amending the Regulation on Commercial Advertising and Unfair Commercial Practices, published in the Official Gazette dated 1 July 2026 and numbered 33297, significant amendments were made to commercial advertisements, particularly digital advertising.

Under the Regulation, which entered into force on 1 August 2026, it has become mandatory to clearly disclose the use of artificial intelligence or the inclusion of digital characters indistinguishable from humans where they are likely to significantly affect consumers' economic behavior. Advertisements creating the impression that AI-generated digital replicas of real persons have experienced, used, or recommended a good or service contrary to the truth have also been prohibited.

In targeted advertising, consumers must be informed, in an easily accessible manner, of the criteria according to which an advertisement is displayed and how those criteria may be changed. In addition, targeted advertising directed at children through profiling based on personal data has been prohibited. Amendments were also made to the Regulation concerning environmental claims, social media influencers, discounted sales, and consumer reviews.

> You may access the Regulation in Turkish here, and our announcement on this topic here.

## Amendments Made to the Regulation of Personal Health Data

With the amendment published in the Official Gazette dated 4 July 2026 and numbered 33300, the procedures regarding the correction of personal health data and the reassessment of previous diagnoses based on an individual's current health condition were regulated.

Under the new amendment, previous diagnoses may be reassessed based on an individual's current health condition. Where it is determined that the current health condition does not confirm the previous diagnosis, without prejudice to the special provisions set out under the relevant legislation, the current medical board report will be taken as the basis in all processes, particularly recruitment processes.

In addition, it was provided that these procedures will be reflected in the records of healthcare service providers. Updates to the databases of other institutions and organizations will be assessed within the framework of their own legislation.

> You may access the Regulation in Turkish here, and our announcement on this topic here.

## Significant Amendments Made to Subscription Procedures in the Electronic Communications Sector

With the Regulation Amending the Regulation on the Identity Verification Process of Applicants in the Electronic Communications Sector, published in the Official Gazette dated 11 June 2026 and numbered 33277 and entered into force on 25 June 2026, significant amendments were made to identity verification procedures for electronic communications subscriptions.

Under the Regulation, identity verification methods were revised, and alternative methods, including verification through the e-Devlet Kapısı, visual, password-based or fingerprint verification using electronic identity documents, transaction-specific video verification for in-person applications, and verification through the Directorate General of Migration Management, were introduced.

With respect to foreign applicants, it was if applicants who do not hold an identity document with electronic identity verification capability will be verified through the Directorate General of Migration Management, while holders of certain foreign mission identity cards will be verified through the e-Devlet Kapısı via the Ministry of Foreign Affairs.

> You may access the Regulation in Turkish here.

## New Regulation on Cybersecurity in Nuclear Facilities Entered into Force

The Regulation on Cybersecurity in Nuclear Facilities, prepared by the Nuclear Regulatory Authority, was published in the Official Gazette dated 5 May 2026 and entered into force. The Regulation sets out the procedures and principles regarding the planning, implementation, and management of cybersecurity in nuclear facilities, and introduces obligations for organizations to prepare cybersecurity plans, manage critical digital assets based on risk, ensure supply chain security, and establish cyber incident response processes.

The Regulation also requires cyber incidents affecting or are likely to affect security, safety, or nuclear security to be reported immediately to the Nuclear Regulatory Authority and the Cybersecurity Directorate. It further provides that, within five business days following the detection of the incident, a report containing the causes, effects, and measures taken in relation to the incident must be submitted to the Authority. The Regulation also requires organizations authorized or having applied for authorization before its entry into force to prepare and submit compliance action plans to the Authority within six months.

> You may access the Regulation in Turkish here.

## The Board Approved the First Binding Corporate Rules Application

In its announcement published on 21 May 2026, the Authority stated that the Binding Corporate Rules application submitted by Sosyo-Plus Bilgi Bilişim Teknolojileri Danışmanlık Hizmetleri A.Ş. had been assessed under Article 9/4(b) of the KVKK and approved by the Board on 20 May 2026.

The decision is significant as it marks the first approval of Binding Corporate Rules by the Board in Türkiye. Binding Corporate Rules constitute one of the appropriate safeguards available for cross-border transfers of personal data between companies belonging to the same group of undertakings.

> You may access the Authority's announcement in Turkish here.

## The Constitutional Court Issued a Significant Decision on the Principle of Legality in Administrative Fines Imposed under the KVKK

The Constitutional Court's decision dated 27 January 2026 and numbered 2020/32193 was published in the Official Gazette dated 16 June 2026 and numbered 33282. In the decision, the Board Decision imposing an administrative fine on the grounds that publicly disclosed personal data had been used for purposes contrary to the purpose of disclosure was assessed in light of the principle of legality of crimes and penalties.

The Court held that neither the criterion of "use in accordance with the purpose of disclosure" nor the sanction applicable in the event of non-compliance with that criterion was expressly regulated under the KVKK. It therefore concluded that imposing an administrative fine based on a criterion not clearly set out in law violated the principle of legality of offences and penalties safeguarded under Article 38 of the Constitution.

> You may access the decision here, and our announcement provides detailed information on this topic here.

## AWS Local Zone in Istanbul Becomes Generally Available

On 20 May 2026, Amazon Web Services (AWS) announced the general availability of its AWS Local Zone in Istanbul. The AWS Local Zone enables certain cloud computing, networking and storage services to be provided in Türkiye, allowing customers to run low-latency applications and to store and process data relating to supported workloads within Türkiye. In addition, Amazon S3 and Amazon EBS Local Snapshots services have been made available in an AWS Local Zone in the Europe, Middle East and Africa (EMEA) region for the first time.

The Istanbul Local Zone supports use cases requiring low latency and data residency, including those in the financial services, gaming, retail and human resources sectors, while operating in integration with the Europe (Frankfurt) Region.

> You may access the announcement here.

# Current Developments in the World

## The European Data Protection Board Published a Standard Template and an Explanatory Document on Data Protection Impact Assessments (DPIAs)

The European Data Protection Board (EDPB) adopted, on 10 March 2026, a Template and an Explainer on the use of the Template for Data Protection Impact Assessments (DPIA) to be carried out under the General Data Protection Regulation (GDPR). The documents were published on 14 April 2026 and opened for public consultation until 9 June 2026.

The Template covers the main stages of the DPIA process, including the description of the processing activity, legal bases, the assessment of necessity and proportionality, risk analysis, and technical and administrative measures to mitigate risks. The Explainer explains how the Template should be completed and the key points to be considered during the process.

> You may access the DPIA Template published by the EDPB here and the Explainer here.

## The Spanish Data Protection Authority Issued a Decision on the Installation of Monitoring Applications on Employees' Personal Mobile Phones

The Spanish Data Protection Authority (AEPD) issued a decision concerning a transport company that used four monitoring applications on company-issued, or employees' personal mobile phones used for work purposes. During the investigation, it was determined that the applications continuously monitored employees' activities and that two of the applications had access to location data, physical condition data, photographs, and videos.

The AEPD assessed that the company encouraged employees to use their personal mobile phones and, therefore, that the consent provided by the employees was not based on free will. It further found that the data processed by the applications exceeded what was necessary for the performance of work. Accordingly, a total administrative fine of EUR 200,000 was imposed on the company for violating the principle of data minimization, the lawful processing condition, and the obligation to inform.

> You may access the full text of the decision in Spanish here.

## The AEPD Imposed an Administrative Fine on a University for Using Facial Recognition Technology in Online Examinations

The AEPD issued a decision concerning a university that used facial recognition technology to verify students' identities in online examinations and conducted monitoring through video and audio recordings during the examination. The AEPD found that the explicit consent for the processing of biometric data had not been given freely and that the Data Protection Impact Assessment (DPIA) had been carried out after the processing activity had commenced.

The AEPD imposed a total administrative fine of EUR 200,000 on the university for the unlawful processing of biometric data and the breach of the DPIA obligation.

> You may access the decision in Spanish here.

## The European Commission Published the Final Code of Practice on the Transparency of AI-Generated Content

On 10 June 2026, the European Commission published the Code of Practice on Transparency of AI-Generated Content (Code of Practice) to support the implementation of the transparency obligations under Article 50 of the EU Artificial Intelligence Act (AI Act). The Code of Practice includes measures for the labelling and detection of AI-generated or manipulated content, as well as the labelling of deep-fakes and certain texts relating to matters of public interest.

Together with the final text, the European Union also published a common set of icons that may be used for the labelling of AI-generated content. The European Commission and the AI Office considered the Code of Practice to be an appropriate voluntary tool supporting compliance with Article 50 of the AI Act.

The relevant transparency obligations apply as of 2 August 2026 with respect to AI systems placed on the market as of that date; the labelling and detection obligations applicable to providers of systems placed on the market before that date will apply as of 2 December 2026.

> You may access the Code of Practice here and our previous bulletin containing detailed information on its content here.

## European Commission Opens Draft Guidelines on High-Risk AI Systems for Public Consultation

On 19 May 2026, the European Commission published draft guidelines on the classification of high-risk AI systems under the AI Act and opened them for public consultation. The draft guidelines aim to assist providers and deployers in determining whether an AI system should be classified as high-risk.

The draft guidelines include explanations and examples concerning the high-risk categories set out in Article 6 of the AI Act. Following the conclusion of the initial consultation on 23 June 2026, the Commission revised the draft considering the feedback received and the input of the AI Board and conducted a second targeted consultation, which remained open until 23 July 2026. The final guidelines have not yet been adopted.

> You may access the draft Guidelines here, and our article provides detailed information on the content of the initial draft here.

## EU AI Omnibus Regulation Enters into Force

Regulation (EU) 2026/1744, commonly referred to as the AI Omnibus, entered into force on 27 July 2026. While maintaining the core safeguards established under the AI Act, the Regulation aims to simplify compliance obligations, enhance legal certainty and support innovation in the field of artificial intelligence.

Under the Regulation, the application dates of certain obligations concerning high-risk AI systems have been postponed, the scope of regulatory sandboxes has been expanded, and certain requirements relating to AI literacy, conformity assessment procedures and registration in the EU database have been simplified.

> You may access the text of the Regulation here and the European Commission's explanations on the Regulation here, and our brochure providing detailed information on this topic here.

## The European Commission Announced That the European Union Age Verification Solution is Ready for Use

The European Commission announced that the age verification solution developed to support the implementation of the Digital Services Act (DSA) and the protection of children in the online environment became technically ready for use as of 15 April 2026. The solution enables users to prove that they meet the required age threshold without sharing their identity, exact age, or other personal information with online platforms.

The open-source solution is based on the same technical specifications as the European Digital Identity Wallets. By its Recommendation dated 29 April 2026, the Commission called on Member States to make the solution available by the end of 2026, either as a standalone application or by integrating it into digital identity wallets.

> You may access the European Commission's announcement here, and the text of the Recommendation here.

## The U.S. Department of Defense Expanded Its Artificial Intelligence Collaboration with Eight Companies, Including Google

The United States (U.S.) Department of Defense announced on 1 May 2026 that it had entered into agreements with eight technology companies, including Google, for the use of their artificial intelligence systems in classified military networks. Under the agreements, artificial intelligence systems are intended to be used for lawful operational purposes in classified networks at IL6 and IL7 levels.

> You may access the official announcement published by the U.S. Department of Defense here.

## The EDPB Published Draft Guidelines on the Processing of Personal Data for Scientific Research Purposes

On 16 April 2026, the European Data Protection Board (EDPB) adopted Draft Guidelines 1/2026 on Processing of Personal Data for Scientific Research Purposes and opened them for public consultation until 25 June 2026. The Draft Guidelines aim to clarify the application of the GDPR provisions relating to scientific research.

The Draft Guidelines address the main criteria to be considered in determining whether an activity qualifies as scientific research, further processing activities carried out for scientific research purposes, broad and dynamic consent, data subject rights, and safeguards such as anonymization and pseudonymization.

> You may access the Draft Guidelines here.

## The French Data Protection Authority Published a Guide on Retention Periods for Human Resources Data

The French Data Protection Authority (CNIL) published, on 2 April 2026, the Reference Guide on Retention Periods for Personal Data in Human Resources Processes (*Référentiel – Durées de conservation des données personnelles – Gestion des ressources humaines*). The Guide sets out the mandatory retention periods under French legislation applicable to common human resources activities, as well as the active retention and intermediate archiving periods recommended by the CNIL.

For example, the Guide states that the personal data of unsuccessful job applicants may be retained in intermediate archives for five years from the date on which the position is filled for use as evidence in potential discrimination claims. It also states that the personal data of individuals included in a candidate pool may be retained actively for up to two years from the last contact, provided that the individual does not object or consent to such retention.

> You may access the French announcement published by the CNIL here.

## CNIL Highlights Privacy Risks Associated with Smart Glasses and Announces Its Action Plan

In a statement published on 29 June 2026, CNIL published its assessments on the risks posed by smart glasses equipped with sensors such as cameras and microphones and capable of operating in integration with artificial intelligence systems to the protection of personal data and privacy and launched an action plan aimed at ensuring the compliance of such devices with the applicable legislation. CNIL noted that the ability of smart glasses to record the images and voices of individuals in their surroundings without their awareness poses significant risks in terms of the violation of privacy and the normalization of widespread surveillance.

CNIL announced that it plans to address the matter with other European data protection authorities within the EDPB, as well as with other relevant public authorities. CNIL also published a set of initial good practice recommendations for users, including informing individuals in the vicinity about the use of smart glasses, disabling device functionalities when they are not necessary, refraining from using such devices in areas where individuals have a heightened expectation of privacy, and obtaining individuals' consent for the use of photographs or videos in which they appear.

> You may access CNIL's announcement here.

## The Belgian Data Protection Authority Imposed an Administrative Fine on a Public Water Utility for Call Recordings and Employee Monitoring Applications

In its decision dated 12 May 2026, the Belgian Data Protection Authority (APD) identified several GDPR infringements in connection with the recording and monitoring of calls by the public water utility (*Société Wallonne des Eaux* - SWDE) for quality control and employee training purposes. While the APD accepted that routine call recording could be based on the performance of a task carried out in the public interest, it found that three calls recorded for the purpose of testing the system were unlawful. It was also concluded that employees and callers had not been adequately informed that appropriate measures had not been implemented to ensure the deletion of recordings within one month, and that the data protection impact assessment had not been carried out in a timely manner.

> You may access the French text of the decision here.

## The Romanian Data Protection Authority Imposed an Administrative Fine on ING Bank for the Unauthorized Disclosure of an Account Statement

Following an investigation concluded in March 2026, the Romanian Data Protection Authority (ANSPDCP) found that ING Bank NV Amsterdam – Bucharest Branch had breached the data security requirements under Article 32 of the GDPR and imposed an administrative fine of EUR 4,000.

The investigation revealed that a bank employee had provided an unauthorized third party with an account statement containing the data subject's name, address, IBAN and account transactions. The Authority considered that the bank had failed to implement appropriate technical and organizational measures to ensure the confidentiality of personal data. The bank was also ordered to bring its processing activities into compliance with the GDPR, adopt the necessary safeguards and provide regular training for employees who process personal data.

> You may access the Romanian text of the decision here.

## Italian Data Protection Authority Fines Poste Italiane and Postepay EUR 12.5 Million

By its decision dated 17 April 2026, the Italian Data Protection Authority imposed administrative fines of EUR 6,624,000.00 on Poste Italiane and EUR 5,877,000.00 on Postepay for the unlawful processing of the personal data of millions of users through the BancoPosta and Postepay mobile applications. The Authority considered monitoring, for fraud prevention purposes, of data relating to applications installed and running on users' mobile devices to be disproportionate and excessively intrusive.

The decision also identified GDPR infringements arising from inadequate information provided to users, the failure to conduct an appropriate data protection impact assessment, insufficient data security and retention measures, and shortcomings concerning the appointment of the data processor. By its decision dated 17 July 2026, the Rome Court granted an interim injunction in respect of the decision.

> You may access information on the status of the decision here.

## The EDPB Adopted a Common Personal Data Breach Notification Template

At its plenary meeting held on 8–9 June 2026, the European Data Protection Board (EDPB) adopted a common Personal Data Breach Notification Template for use in personal data breach notifications under Article 33 of the GDPR. The Template aims to harmonize and facilitate the notification procedures of data controllers and data protection authorities.

The Template aims to facilitate the timely submission of notifications by data controllers and the assessment of notifications by data protection authorities by standardizing the information to be included in personal data breach notifications. In addition, through predefined options and completion instructions, it is intended to save time and costs, particularly for small organizations that do not have a data protection officer or a dedicated legal department. The template was open for public consultation until 5 August 2026.

> You may access the Template here.

## The ICO Published Its Final Guidance on Storage and Access Technologies

The UK Information Commissioner's Office (ICO) published, on 29 April 2026, its final guidance on cookies, tracking pixels, device fingerprinting, and similar storage and access technologies. The Guidance explains the rules to be complied with under the Privacy and Electronic Communications Regulations (PECR) in the use of these technologies and how the UK General Data Protection Regulation (UK GDPR) applies where personal data are processed. The Guidance also addresses the amendments introduced by the Data (Use and Access) Act 2025.

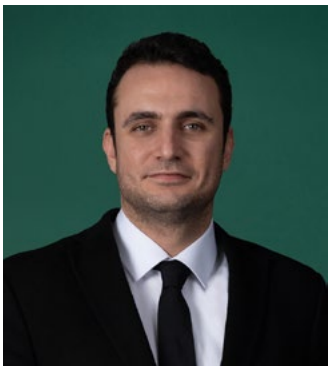
The ICO also stated that it will continue its supervisory and enforcement activities aimed at increasing transparency in the online tracking ecosystem and strengthening individuals' control over their personal data.

> You may access the relevant announcement published by the ICO here.

# Key Contacts

**Sevgi Ünsal Özden**
**Managing Associate and Mediator**

sevgiunsal@erdem-erdem.com



**Ozan Akman**
**Senior Associate**

ozanakman@erdem-erdem.av.tr

## Disclaimer


**ISTANBUL**

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

**IZMIR**

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