

Personal Data Protection Bulletin

2026
Third Quarter

Sevgi Ünsal Özden
Gülnur Çakmak Ergene
Tuğçe Polat
Emre Gürdal

www.erdem-erdem.av.tr

Current Developments from Türkiye

Principle Decision on Personal Data Sharing by Public Institutions on the Internet and KVKK Compliance Guide Published

The Personal Data Protection Board's (Board) Principle Decision dated 1 July 2026 and numbered 2026/1301 was published in the Official Gazette dated 28 July 2026 and numbered 33323. The Board stated that personal data shared on the websites of institutions such as municipalities, universities, and special provincial administrations must be based on one of the conditions for processing personal data set out in the Personal Data Protection Law No. 6698 (KVKK) and must be relevant to, limited to, and proportionate to the purposes for which they are processed. Emphasizing the need to establish how long such data should remain publicly accessible, fulfill the obligation to inform, and implement appropriate security measures, the Board called for an urgent review of existing disclosures. On 28 July 2026, the Personal Data Protection Authority (Authority) also published a KVKK compliance guide for public institutions and professional organizations with public institution status.

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

Public Announcement on the Use of Personal Data Obtained from Third Parties for Marketing Purposes Published

In its announcement dated 21 July 2026, the Authority emphasized that the use of personal data obtained from third parties for marketing purposes must be based on one of the conditions for processing personal data set out in Article 5 of the KVKK, such as explicit consent. It stated that the obligation to inform must be fulfilled within a reasonable period, or at the time of the first contact where the data is used for contact purposes, and separately from the explicit consent procedures, and that continuing a conversation or not communicating an objection does not, in itself, constitute explicit consent. Similarly, by its Decision dated 10 June 2026 and numbered 2026/1183, the summary of which was published on 10 August 2026, the Board imposed an administrative fine of TRY 1,000,000 for breach of the data security obligations under Article 12 of the KVKK on a savings finance company that had used contact information collected through a brand ambassador program for marketing via SMS messages and phone calls without relying on any condition for processing personal data.

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

Compliance Period under the Principle Decision on Loyalty Cards Extended

The Board's Principle Decision dated 11 February 2026 and numbered 2026/266 had required the establishment of mechanisms to prevent third parties from using loyalty cardholders' telephone numbers or card numbers without verification by 28 August 2026. Following requests from industry representatives, the Board extended the compliance period until 28 February 2027 through its Decision dated 22 July 2026 and numbered 2026/1491.



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

Public Announcement on the Principle Decision on Biometric Attendance Tracking Published

In its announcement dated 27 August 2026, the Authority recalled that, under the Board's Principle Decision dated 29 April 2026 and numbered 2026/921, processing biometric data solely for attendance tracking is contrary to the principle of proportionality, even where explicit consent is obtained. It stated that no explicit statutory provision provides for the use of biometric systems for this purpose and that converting biometric data into mathematical codes does not change its biometric nature. It emphasized that use for security and access control purposes requires a separate assessment of whether the processing is limited to the areas and individuals for which it is necessary, whether alternative methods are insufficient, and whether the processing is proportionate. It also recalled that the exemption under Article 28 of the KVKK does not permit unrestricted use.

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

Decision Summary on the Territorial Scope of the KVKK Published

The summary of the Board's Decision dated 28 March 2025 and numbered 2025/601 was published on 10 August 2026. Examining a data breach notification submitted by a hotel company based in Hong Kong, the Board emphasized that the scope of the KVKK must be assessed separately for each processing activity. In assessing the effects principle, it considered not only whether individuals residing in Türkiye were affected by the breach, but also whether they benefited from the services in Türkiye. As the company had no establishment in Türkiye, processed the data in Hong Kong, and its services were not used in Türkiye, the Board concluded that the specific processing activity fell outside the scope of the KVKK, that no breach notification obligation arose, and that no further action was required at that stage.

> You may access the decision summary in Turkish here.

Summaries of 47 Board Decisions Published

On 10 August 2026, the Authority published summaries of 47 Board decisions. The summaries primarily concern data security and breach notification, as well as explicit consent, data subject requests, camera surveillance, and the obligation to inform.

> You may access the decision summaries in Turkish here and our announcement on these topics here.

Practical Guide on Personal Data Protection for Attorneys Published

On 22 September 2026, the Authority published the "Practical Guide on the Protection of Personal Data in Attorneys' Professional Activities." The Guide states that independent attorneys act as data controllers, while substitute attorneys may be considered data processors when following instructions and data controllers when processing data independently beyond those instructions. It emphasizes that uploading files containing personal data to generative AI tools must be assessed under Articles 8 and 9 of the KVKK, considering the locations of the service provider and sub-processors, the technical infrastructure, and the location of processing. It also recalls that an exemption from VERBİS (*Data Controllers' Registry Information System*) registration does not eliminate the obligations relating to informing data subjects, data security, retention, and notification to the Board within 72 hours of becoming aware of a breach.

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

Constitutional Court Upholds Ex Officio Prosecution of the Offense of Unlawfully Disclosing or Acquiring Personal Data

The Constitutional Court's Decision dated 16 April 2026, Case No. 2026/34, Decision No. 2026/81 (Decision), was published in the Official Gazette dated 14 July 2026 and numbered 33310. The Constitutional Court unanimously rejected the request to annul the phrase in Article 139 of the Turkish Criminal Code that removes the complaint requirement for the investigation and prosecution of this offense. Stating that the offense protects not only individual privacy but also the collective security of personal data and public order, the Court found that subjecting it to a different prosecution procedure from the offense of violating the confidentiality of private life does not violate the principle of equality.

> You may access the Decision in Turkish here.

Timetable for Alignment with EU Legislation on Artificial Intelligence and Personal Data Protection Established

The Medium-Term Program (2027–2029), approved by Presidential Decision No. 11752, was published on 6 September 2026. Annex 3 to the Program identifies the first quarter of 2027 as the target for developing the national legislative framework on artificial intelligence with a view to alignment with the European Union (EU), and the third quarter of 2027 for completing the alignment of the KVKK with the EU General Data Protection Regulation (GDPR).

The Program also aims to strengthen domestic AI production capacity under the Türkiye Artificial Intelligence Action Plan (2026–2030). Presidential Circular No. 2026/9 on the Action Plan was published on 18 August 2026. Adopting a human-centered approach, the Plan aims to raise public awareness of AI, develop a skilled workforce, strengthen data and computing infrastructure, expand applications in the public and private sectors, and establish an internationally competitive and trustworthy AI ecosystem.

> You may access the Medium-Term Program in Turkish here, the Circular in Turkish here, the Action Plan in Turkish here and our announcement on this topic here.

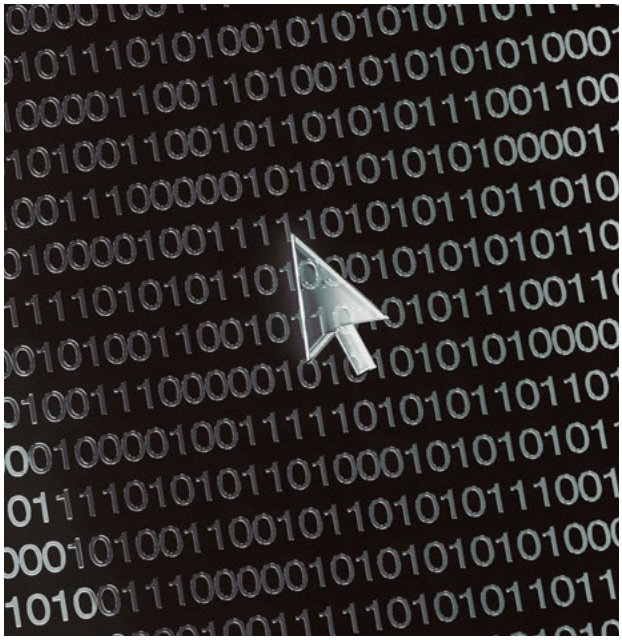
Regulations on Remote Identification in the Financial Sector Updated

The Capital Markets Board's (CMB) amending Communiqué No. III-42.1.b (Communiqué), published in the Official Gazette dated 3 September 2026 and numbered 33359, established rules for the remote identification of non-Turkish nationals using NFC-enabled passports and of legal entities registered in the trade registry through their representatives. Amendments by the Central Bank of the Republic of Türkiye (CBRT), published on 4 September 2026, permit identity verification through biometric methods or documents with electronic identity verification capabilities in remote customer onboarding and framework agreement processes at payment and electronic money institutions. Information and documents obtained in these processes must be legible and verifiable, and their accuracy and authenticity must be checked before services are provided. The CBRT amendments entered into force upon publication.

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

Recommendation Guide on the Use of Artificial Intelligence for Attorneys Published

In its guide published on 28 August 2026, the Union of Turkish Bar Associations emphasized a risk-based approach, client confidentiality, human oversight, and attorneys' ultimate responsibility. It stated that client information that has not been anonymized must not be entered into publicly available tools or tools lacking adequate contractual safeguards, and that the principle of data minimization and the rules on the conditions for processing personal data, the obligation to inform, and cross-border transfers must be observed where personal data is involved. It recommended reviewing providers' terms on data retention and use for model training, informing clients, obtaining their consent where necessary, and establishing a written policy for the law firm.



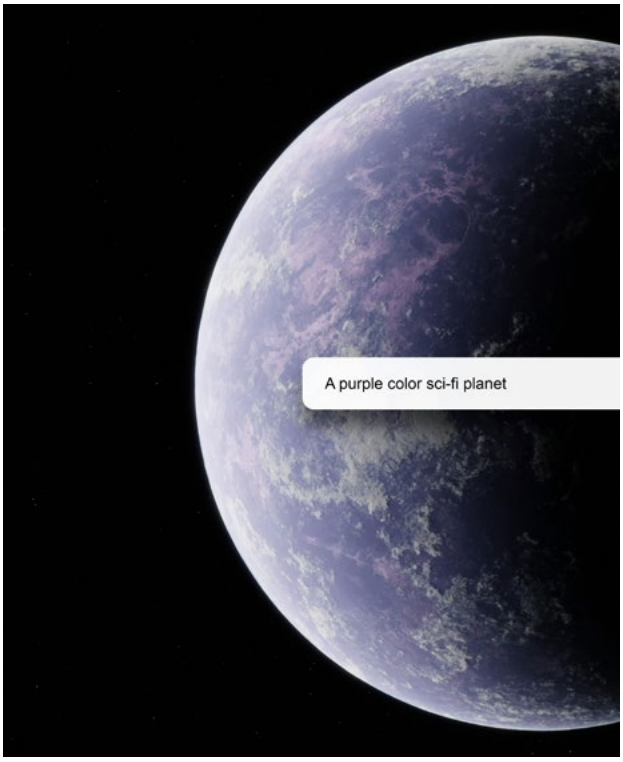
> You may access the Guide in Turkish here.

Current Developments in the World

European Commission Designates ChatGPT as a Very Large Online Search Engine under the Digital Services Act

In its announcement dated 31 August 2026, the European Commission (Commission) announced that it had designated ChatGPT as a very large online search engine, and Reddit and Roblox as very large online platforms, under the EU Digital Services Act (DSA). The services must comply with additional obligations within four months after notification of the decision. These include assessing and mitigating systemic risks relating to illegal content, the protection of minors, users' physical and mental health, fundamental rights, electoral processes, and public security.

> You may access the Commission's announcement in English here.



Transparency Obligations under the EU AI Act Become Applicable

The transparency obligations under Article 50 of the EU Artificial Intelligence Act (AI Act) became applicable on 2 August 2026. The provision requires providers to disclose interactions with AI systems and to mark generated or manipulated content in a machine-readable format. It also establishes disclosure obligations for deployers in relation to emotion recognition, biometric categorization, deepfakes, and AI-generated text published on matters of public interest. GDPR obligations remain unaffected. Providers of systems placed on the market before 2 August 2026 were granted a transitional period until 2 December 2026 solely for the content-marking obligation. On 20 July 2026, the Commission published guidelines explaining the scope of the obligations and applicable exemptions.

> You may access the Commission's announcement on the guidelines in English here and its explanations in English here.

Reporting Obligations under the Cyber Resilience Act Become Applicable

Reporting obligations under the EU Cyber Resilience Act (CRA) became applicable on 11 September 2026 for manufacturers of products with digital elements placed on the EU market. Actively exploited vulnerabilities and severe incidents affecting the cybersecurity of products must be reported to the European Union Agency for Cybersecurity (ENISA) and the competent national computer security incident response team through ENISA's single reporting platform. The phased reporting process requires an early warning within 24 hours and a detailed notification within 72 hours of becoming aware of the vulnerability or incident.

On 27 July 2026, the Commission also published nonbinding guidance explaining the scope of the Regulation, manufacturers' responsibilities, and reporting procedures. The Regulation's main obligations will apply from 11 December 2027.

> You may access the Commission's explanation of the reporting obligations in English here and its announcement on the guidance in English here.

ENISA Publishes a Cyber Resilience Maturity Model for SMEs

On 13 July 2026, ENISA published a model to help small and medium-sized enterprises (SMEs) that manufacture and place products with digital elements on the market assess their readiness for the CRA. The model covers governance and documentation, risk management and secure design, vulnerability and patch management, the product lifecycle, and awareness and skills. The accompanying Excel tool calculates maturity scores to track progress. Reaching an advanced maturity level does not constitute evidence of regulatory compliance.

> You may access the model and the assessment tool in English here.

Design Obligation for Connected Products under the EU Data Act Becomes Applicable

The design obligation under Article 3(1) of the EU Data Act became applicable to connected products and related services placed on the market after 12 September 2026. Connected products and related services must be designed to provide easy, secure, and free access by default to data and the necessary metadata. Data must be provided in a comprehensive, structured, commonly used, and machine-readable format and, where relevant and technically feasible, must be directly accessible. The provisions of the GDPR remain applicable; where the user is not the data subject, a valid legal basis is required for sharing personal data.

> You may access the Data Act in English here and the Commission's explanation in English here.

EDPB Opens Draft Guidelines on Anonymization and Web Scraping for Consultation and Finalizes Blockchain Guidelines

On 8 July 2026, the European Data Protection Board (EDPB) opened draft Guidelines 02/2026 on anonymization and draft Guidelines 03/2026 on web scraping for training generative AI models to public consultation until 30 October 2026. The draft on anonymization explains that the assessment of anonymity may differ depending on the data holder's means of identifying the data subject. The draft on web scraping focuses on legal bases, legitimate interests, transparency, data minimization, and the conditions for processing special categories of personal data under the GDPR. The EDPB also adopted the final version of Guidelines 02/2025 on blockchain, addressing data protection measures and data subject rights.

> You may access the EDPB's announcement in English here.

EDPB Requests Assessment of US Supreme Court Judgment in Relation to the EU–US Data Privacy Framework

In its judgment of 29 June 2026 in Trump v. Slaughter, the Supreme Court of the United States (US) eliminated the protection under which members of the US Federal Trade Commission (FTC) could be removed only for specified causes. In its letter dated 31 July 2026, the EDPB requested that the Commission assess the impact of this development concerning the FTC's independence on the functioning of Adequacy Decision 2023/1795 underpinning the EU–US Data Privacy Framework. The letter does not suspend or invalidate the adequacy decision.

> You may access the letter in English here.

EDPB Opens Draft Guidelines on Administrative Fines for Consultation and Finalizes DSA–GDPR Guidelines

On 17 September 2026, the EDPB adopted draft Guidelines 04/2026 on the imposition of administrative fines and final Guidelines 03/2025 on the interplay between the DSA and the GDPR. The draft, announced on 21 September 2026, was opened for consultation until 13 November 2026. Complementing Guidelines 04/2022 on the calculation of fines, the draft addresses infringements subject to fines and the parties responsible, intent or negligence, aggravating and mitigating factors, and the requirement for fines to be effective, proportionate, and dissuasive. The final guidelines address data minimization in recommender systems and age verification. They state that a valid legal basis for processing under the GDPR does not override the prohibition on online platforms displaying advertisements based on profiling using special categories of personal data.

> You may access the EDPB's announcement in English here.



European Commission Presents EU KIDS Act Proposal on the Protection of Children Online

On 17 September 2026, the Commission presented a proposal for the EU KIDS Act Regulation on the protection of children online. The proposal provides for a minimum age of 15 for opening independent accounts on certain social networking and video-sharing services, and for parent-managed accounts limited to one hour per day for 13- and 14-year-olds. It also proposes privacy-preserving age verification methods, safe default settings, and prohibitions on designs that encourage addiction. The proposal also includes design obligations intended to prevent AI chatbots from creating emotional dependency in children.

> You may access the Commission's explanation in English here and the proposed Regulation in English here.

European Commission Fines Google EUR 890 Million for DMA Infringements

In two decisions dated 23 July 2026, the Commission imposed administrative fines totaling EUR 890 million on Google. A fine of EUR 460 million was imposed for the preferential treatment of Google's own services over those of competitors in Google Search, while a fine of EUR 430 million was imposed for restrictions on app developers directing users to alternative purchasing channels in Google Play. The Commission ordered Google to remedy these infringements of the Digital Markets Act (DMA) within 60 days.

> You may access the Commission's announcement in English here.

CNIL Recalls the Rules on Processing Location Data in Mobile Applications

In its statement dated 7 July 2026, the French Data Protection Authority (CNIL) stated that consent is required where location data is not necessary to provide the service, particularly where it is used for advertising and marketing. It emphasized that permission to access location data granted through the operating system does not constitute consent to such uses. Even where consent is obtained, the granularity of the data, its collection in the background, and the retention period must be limited to what is necessary. Users must be informed and must be able to easily exercise their rights of access, erasure, and withdrawal of consent.

> You may access CNIL's statement in French here.

CJEU Defines the Limits of the Journalistic Exemption for a Criminal Convictions Database

In its judgment of 9 July 2026 in Legal Newsdesk Sweden (C-199/24), the Court of Justice of the European Union (CJEU) assessed a database offering paid access to criminal conviction judgments in light of the journalistic exemption under Article 85 of the GDPR. The Court held that, although charging for access does not exclude a journalistic purpose, making judgments available without editorial processing, verification, or compliance with journalistic ethical standards does not constitute data processing for journalistic purposes. It also emphasized that data subjects cannot be offered only the possibility of filing defamation lawsuits in place of the rights to lodge complaints, seek judicial remedies, and obtain compensation under Chapter VIII of the GDPR.

> You may access the judgment in English here.



CJEU Emphasizes Proportionality in the Public Disclosure of Doping Violations

In its judgment of 14 July 2026 in NADA Austria and Others (C-474/24), the CJEU held that the publication by anti-doping organizations of athletes' names, the rules infringed, and the sanctions imposed is subject to the GDPR. The Court stated that, where national legislation does not ensure proportionality in every case, a balancing exercise must take account of the specific circumstances, such as the seriousness of the violation, the athlete's public profile, and how long the information remains published. It stated that data concerning doping violations does not, as a rule, qualify as health data, but may do so where information on prohibited substances and methods, combined with other data, can reveal an individual's health status. It held that data concerning the disciplinary sanctions at issue does not constitute data relating to criminal convictions and offenses under Article 10 of the GDPR.

> You may access the judgment in English here.

CJEU Defines the Limits of Competition Authorities' Powers to Access Business Emails

In its judgment of 16 July 2026 in *Imagens Médicas Integradas and Others* (Joined Cases C-258/23 to C-260/23), the CJEU stated that business emails are protected by the safeguards under Article 7 of the Charter of Fundamental Rights of the European Union (Charter), which protects respect for private life and communications, and Article 8, which protects personal data. Seizure without prior judicial authorization may be permitted subject to strict limits and effective subsequent judicial review. By contrast, access to data on devices used for both private and professional purposes that constitutes a serious interference must be subject to prior review by a court or an independent administrative authority.

> You may access the judgment in English here.

CJEU Finds Unconditional Public Access to Shareholding Data Contrary to the GDPR

In its judgment of 3 September 2026 in Jautiva (C-798/24), the CJEU assessed national legislation providing for unconditional public access to all shareholders' personal data. The Court held that making shareholders' identity and contact details, as well as data on their shares and voting rights, accessible to everyone without any access condition, such as demonstrating a legitimate interest, violates the GDPR. It emphasized that legitimate objectives, such as combating money laundering and terrorist financing, cannot justify unrestricted access where less intrusive options are available, such as limiting access to persons with a legitimate interest.

> You may access the judgment in English here.

Italian Data Protection Authority Imposes Administrative Fine on Character.AI for GDPR Infringements

By its decision dated 3 July 2026, announced on 9 July 2026, the Italian Data Protection Authority imposed an administrative fine of EUR 158,000 on US-based Character Technologies Inc., the operator of Character.AI, which provides a chat service featuring AI-powered virtual characters. The Authority found GDPR infringements relating to deficiencies in privacy notices, delays in conducting a data protection impact assessment and in appointing an EU representative, and inadequate safeguards for children and age verification mechanisms. The company was ordered, within 120 days of notification of the decision, to ensure the effectiveness of its age verification systems and mechanisms preventing blocked children from registering again, set children's profiles to private by default, and report the measures taken to the Authority.

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

Dutch Data Protection Authority Imposes Administrative Fine of Nearly EUR 825 Million on Uber for Automatically Deactivating Driver Accounts

In its decision announced on 21 August 2026, the Dutch Data Protection Authority imposed an administrative fine of nearly EUR 825 million on Uber for automatically deactivating driver accounts between 2018 and 2022 on grounds such as suspected fraud or low user ratings, without human review. The Authority concluded that this practice, which caused drivers to lose income, infringed Article 22 of the GDPR on decisions based solely on automated processing, and that drivers were not adequately informed. The announcement stated that Uber had ended the infringements and objected to the fine.

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

Irish Data Protection Commission Imposes Administrative Fine of EUR 403 Million on Google for GDPR Infringements Concerning Location Data

In its decision announced on 21 September 2026, the Irish Data Protection Commission (DPC) imposed an administrative fine of EUR 403 million on Google Ireland Limited. The inquiry, covering the period from 25 May 2018 to 4 February 2020, found infringements of the principles of lawfulness and fairness in relation to Web & App Activity and Location History, as well as the retention of location data for longer than necessary. In relation to Location Accuracy, it found a breach of the accountability obligation due to a failure to demonstrate compliance with those principles and transparency requirements. Finding infringements of transparency obligations in relation to all three features, the DPC ordered Google to bring its processing activities into compliance with the GDPR within six months.

> You may access the DPC's announcement in English here.

European Data Protection Supervisor Highlights Data Breach Risks of Shadow AI

In a blog post dated 15 June 2026, the European Data Protection Supervisor (EDPS) addressed the risks of shadow AI, meaning employees' use of AI tools without their organization's official approval. The post stated that such use may make it more difficult to track data processing and respond to data subject requests, and may create risks relating to lawful processing, international transfers, and data security. The EDPS recommended establishing rules for use and approval procedures, implementing technical controls, providing employees with safe and approved alternatives, and offering regular training.

> You may access the EDPS's blog post in English here.

Hamm Higher Regional Court Holds Company Liable for Misleading Statements by Its Chatbot

In its judgment of 12 May 2026, the Hamm Higher Regional Court held that an AI-powered chatbot on the website of a company providing aesthetic treatment services infringed the German Act Against Unfair Competition by presenting physicians as holding specialist qualifications they did not possess. Stating that the chatbot cannot be regarded as a third party and that its responses constitute the company's own commercial statements, the Court prohibited the use of the misleading titles. It also emphasized that the defense that the chatbot had been trained only on accurate data does not relieve the company of liability.

> You may access the analysis published by the US Library of Congress in English here.

French Data Protection Authority Imposes Administrative Fine on EXTIA for Failure to Comply with Erasure Requests

By its decision dated 21 July 2026, announced on 9 September 2026, CNIL imposed an administrative fine of EUR 300,000 on EXTIA for failing to comply with erasure requests from job applicants and former employees or to inform them of the outcome in a timely manner. CNIL emphasized that the requester must be informed of the outcome even where the data is automatically erased.

> You may access CNIL's announcement in English here.

CNIL Fines Hospital for Deficiencies in Patient Data Security

In its decision announced on 3 September 2026, CNIL imposed an administrative fine of EUR 500,000 on Hôpital Privé de la Loire. Examining a cyberattack in which data relating to 524,867 patients was leaked, the Authority found that the absence of multi-factor authentication for remote access, the failure to restrict access to patient files based on the treatment relationship, and the failure to actively analyze access logs infringed Article 32 of the GDPR on the security of processing. Although patients were informed, it was also found that the failure to notify relatives designated by patients as trusted persons, whose data was also leaked, infringed the notification obligation under Article 34.

> You may access CNIL's announcement in English here.

New Zealand Privacy Commissioner Sets Out Expectations on the Use of Smart Glasses

In a statement dated 28 August 2026, the New Zealand Privacy Commissioner highlighted the risks that recording with smart glasses poses to personal data protection. The Commissioner stated that the personal and domestic use exemption under the Privacy Act does not apply where data is collected, used, or disclosed in a "highly offensive" manner. The statement emphasized that organizations are responsible for business use, must collect only the data necessary for lawful purposes connected with their activities, and must comply with transparency obligations. It recommended informing individuals that recording is taking place even where a recording indicator is present and establishing policies for organizational use.

> You may access the Commissioner's statement in English here.

DPC Fines HSE for Infringements Concerning Physical Health Records

In its decision announced on 2 September 2026, the DPC imposed an administrative fine of EUR 645,000 on Ireland's Health Service Executive (HSE). It found that paper health records were stored in insecure conditions and for longer than necessary, documents had been damaged, breach notifications were submitted late, and data subjects were not informed. The DPC ordered inspections of all storage facilities, the secure and traceable management of records, and the secure destruction of records no longer required.

> You may access the DPC's announcement in English here.

Danish Data Protection Authority Conditionally Authorizes Facial Recognition at a Stadium

In its decision published on 9 July 2026, the Danish Data Protection Authority (Datatilsynet) authorized Lyngby Boldklub to use automated facial recognition for stadium entry control. Based on the GDPR's substantial public interest exception, the authorization was limited to certain matches during the club's participation in the Superliga. It required that nonmatching data not be retained and that matching data be erased immediately after each match. In addition to requirements concerning the provision of information, encryption, and access control, it stipulated that a data protection impact assessment must be completed before processing begins.

> You may access the Authority's authorization in Danish here.

NCSC Shares Recommendations on the Secure Use of Agentic AI Systems

In a blog post dated 20 August 2026, the UK National Cyber Security Centre (NCSC) shared interim recommendations on the cyber risks of agentic AI systems. It recommended that systems access only the data and resources necessary for their task, operate in isolated environments (sandboxes), have their activities logged and monitored, and be capable of immediate shutdown when necessary. It emphasized that controls must be proportionate to the system's autonomy and risk level, that human oversight must be ensured for high-risk uses, and that organizations must not rely solely on a model's safeguards or the instructions given to it.

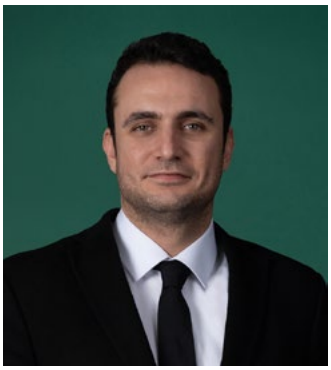
> You may access the NCSC's blog post in English here.

Key Contacts



Sevgi Ünsal Özden
Managing Associate and Mediator

sevgiunsal@erdem-erdem.com



Ozan Akman
Senior Associate

ozanakman@erdem-erdem.av.tr

Disclaimer

All of the information, documents and evaluations set forth in this bulletin have been prepared by the Erdem & Erdem Law Office for information purposes only. This bulletin cannot be used for advertising purposes, to solicit business, or for any other purpose that is contrary to the Professional Rules for Attorneys. Unless expressly permitted by Erdem & Erdem in writing, quoting, citing, or creating links to the content of this bulletin, or any other full or partial use of this bulletin, is strictly prohibited. Erdem & Erdem possesses all intellectual property rights attached to the information, documents, and evaluations in this bulletin and all rights are reserved.

ERDEM & ERDEM

40 YEARS



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