BİÇER GÜNER

Attorneys-at-Law







QUARTERLY DATA PROTECTION AND PRIVACY BULLETIN
Q3 2026

www.bicerguner.com



Developments in Türkiye

- **Principle Decision on the Processing of Personal Data of Accident Victims Published.**

The Personal Data Protection Board's ("**Board**") Principle Decision No. 2026/1095, published in the Official Gazette dated 1 July 2026 and numbered 33297, sets out the principles governing the processing of personal data of victims of occupational accidents, traffic accidents or similar incidents. The Decision states that the personal data of accident victims must be processed in accordance with the processing conditions set forth under Personal Data Protection Law No. 6698 ("**Law**") and that the necessary technical and administrative measures must be taken during the processing of personal data. The Decision further states that the authorizations of persons having access to the personal data of accident victims must be restricted and that training and awareness-raising activities must be conducted for such persons.

- **Public Announcement on the Use of Personal Data Obtained from Third Parties for Advertising and Marketing Purposes Published.**

In the announcement published by the Personal Data Protection Authority ("**Authority**") on 21 July 2026, practices concerning the use of contact information obtained from existing customers or third parties for advertising and marketing purposes were addressed. The announcement states that the mere fact that personal data has been obtained from third parties does not, in itself, constitute a legal basis for processing such data for advertising and marketing purposes and that the conditions stipulated under the Law and the obligations of data controllers must be complied with when processing personal data.

It was further stated that, in respect of personal data not obtained directly from the data subject, the obligation to inform must be fulfilled within the periods stipulated under the Communiqué on the Procedures and Principles to Be Followed in Fulfilment of the Obligation to Inform and that, where processing is based on explicit consent, the processes of providing information and obtaining explicit consent must be carried out separately.



- **Guideline on Compliance with the Personal Data Protection Law for Public Institutions Published.**

The "*Guideline on Compliance with the Personal Data Protection Law for Public Institutions and Organizations and Professional Organizations Having the Status of Public Institutions*", prepared by the Authority, was published on 28 July 2026. The Guideline addresses the obligations of public institutions and organizations and professional organizations having the status of public institutions arising from their capacity as data controllers; the general principles and processing conditions applicable to the processing of personal data; the obligation to inform; ensuring data security; data subject rights; retention and destruction obligations; the obligation to register with VERBİS; transfers of personal data between public institutions; methods for domestic and international data transfers; technical and administrative measures; and exceptional circumstances in which the Law does not apply, either wholly or partially.

- **Principle Decision on the Online Disclosure of Personal Data by Data Controllers Having Public Legal Personality Published.**

The Board's Principle Decision dated 1 July 2026 and numbered 2026/1301 sets out the principles governing the online disclosure of personal data by public institutions and organizations, municipalities, universities and other data controllers having public legal personality. The Board stated that publishing documents containing personal data online constitutes personal data processing under the Law and that such disclosures must be based on a valid processing condition. However, the existence of a valid processing condition alone is not sufficient; in particular, pursuant to the principle of being relevant, limited and proportionate to the purpose, only the minimum personal data necessary should be disclosed, masking or anonymization measures should be applied where necessary, and personal data should remain available online only for the period necessary. It was further stated that currently published content should be reviewed without delay and that disclosures lacking a legal basis or failing to comply with the general principles should be removed or appropriately masked. For announcements such as examination and lottery results, secure methods such as e-Government or two-factor authentication, enabling only the relevant individuals to access their own results, should be preferred to the extent possible.



- ## New Rules on Targeted Advertising and AI-Generated Advertisements Entered into Force.

The Regulation Amending the Regulation on Commercial Advertising and Unfair Commercial Practices, published in the Official Gazette dated 1 July 2026 and numbered 33297, introduced new obligations in the field of digital advertising, which entered into force on 1 August 2026. Accordingly, in targeted advertising, clear and easily accessible information must be provided regarding the criteria used to display advertisements to consumers and how those criteria may be modified, while targeted advertising to children through profiling based on personal data has been prohibited. In addition, where AI-generated digital characters that are indistinguishable from humans are used in advertisements, this must be clearly disclosed, and advertisements creating the impression that AI-generated digital replicas of real persons have experienced or recommended a product have been prohibited.

- ## Constitutional Court Found Failure to Provide Access to Disciplinary Documents to Constitute a Violation of the Right to an Effective Remedy in Connection with the Right to Protection of Personal Data.

At its chamber meeting held on 21 July 2026, the Constitutional Court ("**Court**") assessed, within the scope of the right to protection of personal data, the failure to respond positively to the applicant's request to be provided with a copy of the documents relating to disciplinary penalties imposed on the applicant. The Court found admissible the allegation that the failure to respond positively to this request violated the right to an effective remedy in connection with the right to protection of personal data and held that the right to an effective remedy guaranteed under Article 40 of the Constitution, in connection with the right to protection of personal data guaranteed under Article 20 of the Constitution, had been violated.



QUARTERLY DATA PROTECTION AND PRIVACY BULLETIN
Q3 2026

- **Personal Data Protection Board Extended the Compliance Period for Loyalty Card Practices.**

By its decision dated 22 July 2026 and numbered 2026/1491, the Board extended the compliance period stipulated under its Principle Decision dated 11 February 2026 and numbered 2026/266 concerning the use of a loyalty card holder's mobile phone number or loyalty card number by a third party during a purchase. The Principle Decision had required the implementation of necessary technical and administrative measures to prevent the use of a loyalty card holder's personal data without their knowledge and consent and to verify that purchases are made with the card holder's knowledge and intention. The compliance period, which was scheduled to expire on 28 August 2026, was extended until 28 February 2027 in response to requests from the sector.

- **Authority Provided Clarifications on Circumstances in Which Biometric Data May Be Processed for Purposes Other Than Attendance Tracking.**

Following requests for opinions received after the publication of the Principle Decision dated 29 April 2026 and numbered 2026/921 on the Processing of Biometric Data for Attendance Tracking Purposes, the Authority provided further clarifications regarding the processing of biometric data. The Authority stated that converting data obtained through methods such as fingerprint or palm scanning into mathematical codes and storing such codes does not remove their classification as biometric data. It also reiterated the assessment in the Principle Decision that biometric data processing carried out solely for attendance tracking purposes does not rely on any of the processing conditions stipulated under Article 6 of the Law and, even where valid explicit consent exists, does not satisfy the proportionality criterion set forth under Article 4 of the Law. However, it clarified that biometric data processing activities carried out for purposes other than attendance tracking do not fall within the scope of the Principle Decision. In particular, biometric data processing for identity verification, authorization and control of access to critical areas in facilities and operational areas involving security risks should be assessed separately, taking into account the inadequacy of alternative methods, the necessity and proportionality of the processing activity, and the specific security need.



- **Procedures and Principles for Monitoring Corporate E-Mail Accounts Assigned to Employees Determined.**

By its Principle Decision dated 16 September 2026 and numbered 2026/2035, the Board established the fundamental principles governing employers' monitoring of corporate e-mail accounts and other communication channels assigned to employees. The Decision states that the fact that communication tools belong to the employer does not grant an unrestricted right to monitor them; employees must be informed in advance in a clear and specific manner, and monitoring must be conducted for a specific and legitimate purpose and in a manner that is relevant, limited and proportionate to that purpose. It was further emphasized that content monitoring should, as a rule, be conducted only where there is a legitimate purpose connected with a specific suspicion or particular incident and that general and continuous reviews of content should be avoided.

- **Obligation to Comply with the Personal Data Protection Law in the Processing of Students' Personal Data Expressly Regulated.**

The Regulation Amending the Regulation of the Ministry of National Education on Preschool Education and Primary Education Institutions, published in the Official Gazette dated 28 July 2026 and numbered 33323, introduced a new provision to Article 78 of the Regulation. Accordingly, it has been expressly stipulated that, for the purpose of protecting fundamental rights and freedoms, particularly the right to privacy, all acts and procedures carried out by school administrations in relation to the processing of students' personal data must be conducted in accordance with the Law.



- **Practice Guideline on the Protection of Personal Data in Lawyers' Professional Activities Published.**

On 22 September 2026, the Personal Data Protection Authority published the "*Practice Guideline on the Protection of Personal Data in Lawyers' Professional Activities*", prepared with the opinions and contributions of the Union of Turkish Bar Associations. The Guideline addresses the legal bases for personal data processing activities carried out by lawyers, the conditions for processing personal data, domestic and international data transfers, the use of generative artificial intelligence tools, the obligations of data controllers, and data security.

- **Personal Data Protection Board Assessed the Principles of Territoriality and Effects.**

In its decision numbered 2025/601, the Board assessed the applicability of the Law to a data controller located outside Türkiye following a cyberattack and personal data breach affecting the reservation databases of a Hong Kong-based hotel operator. Taking into account that the data controller had no legal entity, employees, group company or technological infrastructure in Türkiye, that the personal data was collected and processed in Hong Kong, and that the data subjects did not benefit from the relevant services in Türkiye, the Board held that the Law was not applicable to the specific case under the "effects doctrine".



Global Developments

- **European Commission Published Guidelines on Transparency Obligations under the AI Act.**

On 20 July 2026, the European Commission ("Commission") published its guidelines on the transparency obligations set forth under Article 50 of the AI Act. These transparency obligations became applicable as of 2 August 2026. In this context, users of certain AI systems must be informed that they are interacting with an AI system, and certain AI-generated or manipulated content must be marked in a detectable manner. Additional information obligations will also apply to deepfake content, emotion recognition and biometric categorization systems, and certain public-interest content generated or manipulated using AI. While the Guidelines provide explanations regarding the scope and implementation of these obligations, the Commission also published an updated Frequently Asked Questions document concerning the Guidelines on 24 July 2026.

- **European Data Protection Board Adopted a New Methodology for the Imposition of Administrative Fines under the General Data Protection Regulation.**

On 21 September 2026, the European Data Protection Board ("EDPB") adopted a new methodology for the imposition of administrative fines under the General Data Protection Regulation ("GDPR"). Under the five-step methodology, in addition to determining whether the infringement warrants a fine and identifying the responsible party, consideration will be given to whether the infringement was committed intentionally or negligently, any aggravating and mitigating factors, and whether the fine is effective, proportionate and dissuasive. The Guidelines also provide explanations regarding the exercise of other corrective powers, such as warnings, reprimands, orders and withdrawal of certification, as well as 14 practical examples.



- 23andMe Reached USD 18 Million Settlement in the U.S. over Data Breach Affecting Genetic Data.

A coalition of attorneys general from 42 U.S. states reached an USD 18 million settlement with genetic testing company 23andMe in connection with a 2023 data breach affecting the genetic data of 6.9 million consumers. The settlement, announced on 14 July 2026, stated that 23andMe had failed to implement adequate data security measures and that the breach resulted in the exposure of sensitive personal data, including genetic ancestry information. The settlement also imposed obligations on the entity acquiring the company's data regarding enhanced data security measures, risk assessments, data security governance mechanisms and the protection of consumers' rights to delete their data.

- EDPB Adopted Final Guidelines on the Interplay Between the Digital Services Act ("DSA") and the GDPR.

On 21 September 2026, the EDPB adopted its final guidelines on the interplay between the DSA and the GDPR. Following a public consultation, the Guidelines provide explanations regarding the concurrent application of the DSA and GDPR, particularly in relation to personal data processing activities carried out by intermediary service providers, as well as circumstances in which the DSA refers to concepts and definitions under the GDPR.

- UK Information Commissioner's Office ("ICO") Launched a Consultation on Draft Guidance on Anonymisation and Pseudonymisation in Research.

The ICO opened its draft guidance on anonymisation and pseudonymisation in research for public consultation. The Guidance addresses the roles of anonymisation and pseudonymisation in research processes, applicable technical and administrative measures, the establishment and operation of trusted research environments, and the use of synthetic data in research. Comments may be submitted until 19 October 2026.



- **European Union Agency for Cybersecurity ("ENISA") Published Secure-by-Design and Secure-by-Default Guidance for SMEs.**

ENISA published guidance on secure-by-design and secure-by-default approaches for small and medium-sized enterprises ("SMEs"). The Guidance sets out key principles regarding secure design and secure default settings that may be applied throughout the lifecycle of products, together with practical guidance for SMEs on implementing these principles.

- **Luxembourg Data Protection Authority ("CNPD") Addressed Privacy Considerations Relating to Camera-Equipped and AI-Powered Smart Glasses.**

On 26 August 2026, the CNPD published guidance concerning the protection of personal data arising from the use of smart glasses incorporating cameras, microphones and AI technologies. The guidance addresses privacy risks that may arise from the ability of such devices to perform real-time data analysis, as well as data protection obligations to be considered by manufacturers, suppliers and professional users.

- **European Commission Designated ChatGPT, Reddit and Roblox as Very Large Online Services under the DSA.**

On 31 August 2026, the Commission designated ChatGPT as a Very Large Online Search Engine ("VLOSE") and Reddit and Roblox as Very Large Online Platforms ("VLOPs") under the DSA. It was stated that these services had exceeded the threshold for designation as VLOSEs and VLOPs under the DSA by reaching at least 45 million average monthly users in the European Union. Accordingly, ChatGPT, Reddit and Roblox are required to comply with the additional DSA obligations applicable to VLOSEs and VLOPs within four months of notification of the designation decisions, by January 2027. These obligations include assessing and mitigating systemic risks arising from the services and algorithmic systems, particularly risks relating to the dissemination of illegal content, adverse effects on children, users' physical and mental well-being, fundamental rights, electoral processes and public security.



- **Singapore Personal Data Protection Commission ("PDPC") Published Guidelines on the Processing of Personal Data in the Use of Generative AI.**

On 20 July 2026, the PDPC published its final advisory guidelines on the processing of personal data in connection with the development and use of generative AI systems. The Guidelines address the collection and use of personal data for the development of AI models, the allocation of data protection responsibilities throughout the lifecycle of AI systems, and the handling of data subject requests.

- **Irish Data Protection Commission Imposed a EUR 403 Million Administrative Fine on Google for Processing Location Data.**

On 21 September 2026, the Irish Data Protection Commission ("DPC") decided to impose an administrative fine of EUR 403 million on Google and issue a compliance order following its inquiry into Google's processing of location data. The inquiry, initiated by the DPC on its own initiative, commenced in February 2020 following complaints from various European consumer rights organizations concerning Google's processing of location data in connection with certain services and products. The decision assessed Google's location data processing activities under Articles 5, 6, 12 and 13 of the GDPR concerning the principles relating to the processing of personal data, lawfulness of processing, transparent information and the provision of information to data subjects. The decision was announced by the EDPB on 23 September 2026.

- **EDPB Adopted the Final Version of the Guidelines on the Processing of Personal Data through Blockchain Technologies.**

In its announcement dated 8 July 2026, the EDPB stated that it had adopted the final version of its guidelines on the processing of personal data through blockchain technologies following public consultation. The Guidelines address the implications of different types of blockchain technologies for the processing of personal data, the allocation of data protection responsibilities, data protection principles, data subject rights and the performance of data protection impact assessments. The Guidelines further state that personal data should not be stored on a blockchain where doing so would conflict with data protection principles.



- EDPB Adopted New Guidelines on Anonymisation.

On 8 July 2026, the EDPB opened its Draft Guidelines 02/2026 on anonymisation for public consultation. The Guidelines state that, for a dataset to be considered anonymous data falling outside the scope of the GDPR, it must not be reasonably possible to re-identify data subjects, either directly or indirectly. In this context, the risks of distinguishing individuals within a dataset, linking information across different datasets and drawing inferences about individuals should be taken into account when assessing anonymisation. The Guidelines also explain that anonymity should be assessed by taking into account the party accessing the data and the specific circumstances. The Guidelines will remain open for public consultation until 30 October 2026.

- EDPB Adopted Guidelines on the Processing of Personal Data through Web Scraping in the Context of Generative AI.

On 7 July 2026, the EDPB adopted Draft Guidelines 03/2026 on the collection of personal data from the internet through "web scraping" for the development of generative AI models. The Guidelines were opened for public consultation on 8 July 2026. The Guidelines address the assessment of personal data processing activities carried out through web scraping under the GDPR, the identification of an appropriate legal basis and, in particular, the need to conduct necessity and balancing assessments where processing is based on legitimate interests. They also provide explanations regarding data minimisation, transparency, data subject rights, the processing of special categories of personal data, and the fact that personal data being publicly available online does not mean that it may be processed without limitation. The Guidelines will remain open for public consultation until 30 October 2026.

Biçer Güner is a full-service, independent law firm based in Istanbul, Türkiye. As Biçer Güner, we offer a full spectrum of legal services for a diverse client base across all areas of law. For over 20 years, our partners have actively represented both private and public sector clients in numerous significant international transactions and foreign investments in Türkiye.

Our firm is widely recognized in prestigious legal directories. We are ranked by The Legal 500, one of the world's most reputable legal directory, for our expertise and client-focused approach. Also, our employment practice is distinguished in the International Employment Lawyer's Elite Guide and our Managing Partner, Burçak Kurt Biçer, has been named among the 2025 IEL Women Leaders, a recognition of outstanding female leadership in employment law worldwide. Moreover, as a proud member of the International Association of Privacy Professionals (IAPP)—the world's leading information privacy community— we remain at the forefront of global data protection trends and compliance standards.



BURÇAK KURT BİÇER
Managing Partner
burcak.bicer@bicerguner.com



BERKE ÖZAKCA
Legal Intern
berke.ozakca@bicerguner.com



YAĞMUR SAN
Yasal Stajyer
yagmur.san@bicerguner.com

Maslak Mah. AOS 55. Sok. 42 Maslak B Blok No: 4/558
34398 Sarıyer, İstanbul, Türkiye
www.bicerguner.com
+90 212 945 99 53