BİÇER GÜNER

Attorneys-at-Law

Bimonthly Data Protection and Privacy Bulletin

SEPTEMBER 2025

Latest News from Türkiye and the World!

📌 Developments in Türkiye

- **The Medium-Term Program included the objective of aligning the Law on the Protection of Personal Data with the GDPR and EU AI Act.**
    - The Medium-Term Program ("**MTP**") for the 2026–2028 period, which includes the objective of aligning the Law on the Protection of Personal Data No. 6698 ("**Law**") with the European Union ("**EU**") General Data Protection Regulation ("**GDPR**"), was published in the 1st duplicate issue of the Official Gazette on 7 September 2025. According to the MTP, the harmonization process between the Law and the GDPR is targeted to be completed in the third quarter of 2026. The MTP further stipulates that the efforts to align the national legal framework with the EU Artificial Intelligence Act are also planned to be finalized by the third quarter of 2026.

- **The Personal Data Protection Authority has revised the "Questions on VERBIS" and the "VERBIS Guide," introducing new security and accessibility features to the system.**
    - The Personal Data Protection Authority ("**Authority**") has revised the "Questions about Data Controllers' Registry Information System (**VERBIS**)" and the "VERBIS Guide" to streamline registration and notification processes, introducing new security features, accessibility improvements, and procedural clarifications in line with recent system changes.

- **Micro-Scale Data Controllers Exempted from VERBIS Registration Obligation**
  - The Personal Data Protection Board ("**Board**"), taking into account the economic conditions, the limited resources and personnel structure of micro-enterprises, and the relatively small volume of personal data they process, has decided, by Decision No. 2025/1572 dated 04.09.2025, to exempt data controllers whose main activity is the processing of special categories of personal data but who employ less than 10 employees and have an annual balance sheet total of less than 10 million Turkish Lira from the obligation to register with the VERBİS. Thus, it was aimed to reduce the disproportionate administrative and financial burdens that micro-scale data controllers may encounter in fulfilling their obligations and to uphold the principle of proportionality and balance in the implementation of the Law.

- **Draft Law Submitted to Parliament to Exempt Lawyers' Personal Data Processing Activities from the Data Protection Law**
  - A draft law proposal has been submitted to the Grand National Assembly of Türkiye proposing that personal data processed by lawyers within the scope of their professional activities be exempted from the Law. In the general preamble of the proposal, it is argued that compliance obligations under the Law have rendered the practice of law almost impracticable and have undermined lawyers' ability to collect evidence. It was particularly emphasized that, in criminal proceedings, there is a situation contrary to the principle of equality of arms between lawyers and the other party acting on behalf of the public, and that this situation is not compatible with the right to a fair trial.

- **The Financial Crimes Investigation Board Updates the Guide on Obligations of Crypto Asset Service Providers**

    - The Financial Crimes Investigation Board ("**FCIB**") has updated and published the "Guidelines on Crypto Asset Service Providers", prepared to clarify the obligations of crypto asset service providers (**CASPs**) under the Law No. 5549 on the Prevention of Laundering Proceeds of Crime and the Law No. 6362 on Capital Markets Law. The Guide provides detailed information on issues such as customer identification and verification processes, remote identification methods, enhanced measures, the application of the Travel Rule, transfer time and limits, measures to be taken in business relationships with politically exposed persons, as well as suspicious transaction reporting and compliance program obligations. The Board emphasized that it is of vital importance for crypto asset service providers to fully implement these obligations set out in the guide through a risk-based approach, in order to prevent the use of the financial system for illegal activities such as money laundering and financing of terrorism.

- **Council of State Annuls the Data Protection Officer Certification Programme and the Related Communiqué**
    - 1.The Tenth Chamber of the Council of State annulled the Communiqué on the Procedures and Principles Regarding the Personnel Certification Mechanism ("**Communiqué**") published in the Official Gazette dated 06.12.2021 and numbered 31681 and the Data Protection Officer Certification Programme ("**Programme**") adopted by the Personal Data Protection Board, following a lawsuit filed by the Union of Turkish Bar Associations. The annulment was based on the grounds that the Communiqué and Programme introduced the concept of a "data protection officer" and related provisions not provided for under the Law No. 6698, and that these activities fell within the exclusive professional remit of lawyers, thus violating the Attorneys' Act.
    - In its reasoning, the Council of State found that the Communiqué and the Programme were inconsistent with the enabling legislation, thereby infringing the principles of the hierarchy of norms, legality of administration, and subsidiarity of regulatory powers. In the decision, it was also emphasized that the failure to clearly define the duties and responsibilities of the "data protection officer" constituted a breach of the principle of legal certainty.

- **The Personal Data Protection Authority Shared Recommendations for Parents on Children's Use of Social Media**
    - The Authority has shared several recommendations to parents regarding children's use of social media in its latest bulletin (2025 issue: 9) . Parents were advised to talk to their children about the long-term effects of social media and digital footprints and to help them gain online awareness. Among the recommendations were that children should be guided on the privacy of personal data, the use of strong passwords, regular checking of privacy settings, and avoiding communication with strangers, and that a safe environment should be created in which children can openly share their online experiences.

- **The Personal Data Protection Authority Announced Sharing Personal Data of Debtors' Reatives' by Creditors' Attorneys May Constitute Unlawful Act**
    - The Authority has made an announcement, following complaints alleging that creditor attorneys accessed the contact information of debtors' relatives and shared debt information. The Authority stated that such practices may violate the Law and that sharing the personal data of third parties without explicit consent or a valid data processing condition may result in administrative fines. In the announcement, it was emphasized that creditor attorneys should process only the data relating to the debtor while carrying out debt collection activities and should not share information concerning the debtor's relatives. The Authority has underlined the importance of ensuring that personal data processing activities are carried out in accordance with the principles set forth in the Law and in compliance with the law and the rules of good faith and warned that otherwise sanctions may be imposed.

🌍 Global Developments

- **Italy Becomes the EU member to Incorporate the EU Artificial Intelligence Act into National Legislation**
    - Italy has become the first country in the EU to adopt an artificial intelligence law under the EU Artificial Intelligence Act. The Law dated 23 September 2025 and numbered 132 ("**Italian AI Act**") provides that artificial intelligence systems must be developed in accordance with fundamental rights, EU law, and the principles of transparency, proportionality, security, and non-discrimination. Pursuant to the Italian AI Act, in areas such as health, working life, and justice, artificial intelligence will only play a supportive role; the final decision will remain with human discretion. In terms of child protection, certain provisions have been introduced, the use of artificial intelligence systems by individuals under the age of 14 has been made subject to permission, and age verification systems have been made mandatory. Amendments to the Criminal Code provide for prison sentences for crimes committed through artificial intelligence and for the misleading dissemination of AI-altered (deepfake) content.
- **European Commission Fines Google €2.95 Billion for Anti-Competitive Conduct in the Ad Tech Sector**
    - The European Commission has imposed a €2.95 billion fine on Google for breaches of EU competition rules in the advertising technology ("adtech") sector. The Commission concluded that Google had favored its own online display advertising services over competing tech providers, advertisers, and online publishers, thereby distorting competition.
    - Google has been instructed by the Commission to cease self-preferencing practices and to implement measures that eliminate conflicts of interest throughout the ad tech supply chain. Google must report to the Commission within 60 days on how it intends to comply with these obligations.

- **EU Data Act: Introducing Fair Access to IoT Data, Data Sharing Rights, and Provider Switching in Cloud Services**
    - The EU Data Act (Regulation (EU) 2023/2854), which entered into force on 11 January 2024, however, most of its provisions became applicable as of 12 September 2025, establishes uniform rules on fair access to and use of data; especially defines the rights of users of connected products and related services (IoT) to access and share the data generated by such products and services with third parties. The Data Act ensures the protection of trade secrets and personal data, while imposing fair, reasonable and non-discriminatory (FRAND) conditions for B2B data sharing and providing for the nullity of unfair contractual terms unilaterally imposed on weaker parties. With respect to cloud and data processing services, the Data Act introduces customer-friendly switching and data porting obligations, abolishes technical and contractual barriers that may hinder switching, and prohibit exit or switching fees entirely as of 12 January 2027, following a three-year transitional period. Member States are required to establish effective, proportionate, and dissuasive sanctions as well as competent authorities to enforce the regulation. Where a violation involves personal data, sanctions equivalent to those under the GDPR may apply.

    - The territorial scope of the Data Act is broad. Manufacturers of connected products or providers of related services made available on the EU market, as well as providers offering data processing or cloud services to customers in the EU, fall within the scope of the Regulation regardless of their place of establishment. Accordingly, for example, manufacturers established in Türkiye selling IoT products in the EU will be required to adopt contractual and technical measures enabling users to access and share product-generated data under FRAND terms and with adequate trade secret protection. Likewise, cloud and SaaS providers based in Türkiye will be obliged to ensure the practical feasibility of provider switching and data porting for EU clients and to abolish egress and switching fees as of 12 January 2027. In conclusion, non-EU companies engaging in business with the EU must align their contracts, technical infrastructures, and internal compliance mechanisms with the requirements of the Data Act to ensure full regulatory conformity.

- **FTC Announces $2.5 Billion Settlement with Amazon Over Prime Subscription Practices**
    - The investigation initiated by the U.S. Federal Trade Commission ("**FTC**") against Amazon—on allegations that it enrolled consumers in Prime subscriptions without their consent and deliberately made cancellation difficult—has been resolved by way of a settlement.
    - According to FTC, Amazon designed misleading and confusing user interfaces to enroll consumers unknowingly into the subscription system called "Prime" and established complex and discouraging cancellation procedures. As part of the settlement, Amazon has undertaken to implement comprehensive changes to its Prime subscription processes. Accordingly, the changes will include: providing an explicit and conspicuous option to decline the subscription; clearly and intelligibly disclosing the general terms and conditions to consumers; and enabling subscriptions to be cancelled with the same ease and without undue burden as enrollment.
    - As part of the settlement, Amazon has undertaken to pay an administrative fine of USD 1 billion, to pay USD 1.5 billion in compensation to consumers harmed by deceptive Prime subscription practices, and to cease unlawful enrollment and cancellation practices relating to the Prime service. This amount constitutes the second-highest award of consumer redress in the FTC's history.

- **European Commission Publishes Draft Guidance on Reporting Serious Incidents in High-Risk AI Systems**
    - The European Commission has published draft guidelines on critical artificial intelligence cases. The Commission has published a draft guide and reporting template on serious artificial intelligence incidents (serious AI incidents) and opened it to public consultation.
    - The draft guidelines, published under the EU Artificial Intelligence Act (AI Act), establishes the framework for defining, reporting, and investigating "serious incidents" in high-risk artificial intelligence systems. The document emphasizes that artificial intelligence is no longer just a technical tool, but an element that must be monitored in terms of human rights, public safety, and social order. The concept of "serious incident" covers not only physical harm such as death or injury, but also violations of fundamental rights, discrimination, and algorithmic unfairness. Pursuant to the draft guidelines, for instance, discrimination by an employment or credit scoring system based on race, gender, or region will now become a "reportable incident."
    - The draft guidelines also clearly separate the responsibilities of providers and users; the providers are generally required to report incidents within 15 days, and within 2 to 10 days in cases such as death or disruption of critical infrastructure. This system aims not only at technical safety but also at ethical supervision and transparency. As a result, the document clearly reveals that the EU aims to shape artificial intelligence technologies on the basis of accountability and innovation.

- **Court of Justice of the European Union Rules That Personal Opinions May Constitute Personal Data by Nature**
    - The Court of Justice of the European Union, in the case of EDPS v. SRB, ruled that personal opinions may, by their nature, constitute personal data and that the controller's obligation to provide information must be assessed before the transfer of data to a third party and from its own perspective, overturning the decision of the General Court. The Court held that although anonymized or pseudonymized data may not be considered personal data in all cases, personal opinions that reflect the identity of the data subject and can be attributed to them are by their nature still personal data because they are closely linked to the data subject. Developing this interpretation based on its settled case law that the assessment of "identifiability" in data protection law should be made in the context in which the data are processed and from the controller's perspective, the Court of Justice stated that the identifiability of the data subject should be assessed according to the circumstances at the time the data are collected and from the controller's point of view.

- **European Commission Announces Adequacy Decision for Personal Data Transfers with South Korea**
    - The European Commission has announced in a joint press release with South Korea that the adequacy decision for the transfer of personal data between the two parties has entered into force. The statement said that the decision would complement and enhance the benefits of the EU-Korea Free Trade Agreement and the newly signed Digital Trade Agreement.

- **Canadian Privacy Commissioner Finds TikTok Failed to Adequately Protect Children's Personal Data**
    - Following an investigation, the Office of the Privacy Commissioner of Canada ("**OPC**") has concluded that TikTok failed to implement adequate safeguards to protect the personal data of child users, thereby violating its obligations under the Personal Information Protection and Electronic Documents Act ("**PIPEDA**"). Although the TikTok platform prohibits individuals under the age of 13 from creating accounts, the investigation has revealed that deficiencies in age verification mechanisms allowed younger users to access the platform. While TikTok reported that it deletes approximately 500,000 underage user accounts annually; however, the report found that the personal data of these users had been collected and used for targeted advertising and content recommendation purposes. It was concluded that this practice led to children being exposed to age-inappropriate advertising, which could increase the risk of identity theft, might adversely affect healthy development, and could result in outcomes such as negative body perception.

- **French Data Protection Authority Issues Recommendations and Compliance Checklist on GDPR-Compliant AI Training**
    - The French Data Protection Authority ("**CNIL**") has issued a set of recommendations addressing the applicability of the GDPR to artificial intelligence models, the security obligations arising therefrom, and the requirements for labelling training datasets used in AI development. The recommendations recall that, given the memorization capacity of AI systems, the training of such systems using personal data falls within the material scope of the GDPR. CNIL also published, alongside the recommendations, a compliance checklist outlining the key considerations to be observed when training AI systems in conformity with the GDPR. In addition, sector-specific guidance has been provided with respect to the use of AI systems in education, healthcare, and employment, highlighting the risk mitigation measures that must be implemented in these fields.
- **Dutch Data Protection Authority Publishes Guidance on Ensuring Meaningful Human Intervention in Automated Decision-Making**
    - The Dutch Data Protection Authority has issued guidance on ensuring meaningful human intervention in automated decision-making processes carried out through algorithms and artificial intelligence systems. The document emphasizes that human discretion must be genuinely integrated into such processes and not merely nominal. Accordingly, user interfaces and technical systems should be designed to enable reviewers to access all relevant data in full and within the proper context. Organizations are further required to adopt appropriate administrative and procedural safeguards to ensure effective human oversight, including allocating sufficient time for evaluation, granting authority to override automated outcomes, developing internal policies, and providing the necessary training to personnel responsible for review and intervention.

- **Australia enacted new regulations establishing 16 as the minimum age requirement for users of social media platforms**
    - The Australian Government, in its announcement dated 30 July 2025, has declared the implementation of the Online Safety (Age-Restricted Social Media Platforms) Rules 2025 under the Online Safety Act 2021. Under these rules, the minimum user age for "age-restricted social media platforms"—including Facebook, Instagram, Snapchat, TikTok, X, and YouTube—has been set at 16 years. Online gaming platforms, messaging applications, and digital health and education services are expressly excluded from the scope of these rules. Accordingly, as of 10 December 2025, service providers falling within the scope will be required to take "reasonable/responsible steps" to prevent individuals under the age of 16 from creating accounts or accessing such services. In case of non-compliance, the relevant platforms may be subject to administrative fines of up to AUD 49.5 million.

- **The UK's Data Protection Authority (ICO), published a draft guidance on distributed ledger technologies (DLTs)**
    - The UK Information Commissioner's Office ("**ICO**") has published a draft guidance document on Distributed Ledger Technologies ("**DLT**"). The draft provides a comprehensive explanation of DLT systems and clarifies the circumstances in which data protection legislation applies to blockchain-based environments.
- **The Dutch Ministry of Economic Affairs published a guidance document outlining the obligations of organizations and companies under the EU Artificial Intelligence Act**
    - The Dutch Ministry of Economic Affairs has published a guidance document outlining the obligations of institutions and companies under the European Union Artificial Intelligence Act. The guidance outlines how artificial intelligence systems are categorized and sets out the data protection measures to be implemented, as well as the compliance obligations applicable to AI systems, with a particular focus on general-purpose and high-risk AI systems.

Contact

Burçak Kurt Biçer
Managing Partner
burcak.bicer@bicerguner.com

Uğurkan Şeber
Managing Asssociate
ugurkan.seber@bicerguner.com

Doğaç Karakurt
Associate
dogac.karakurt@bicerguner.com

Mert Yılmaz
Legal Intern
mert.yılmaz@bicerguner.com

Berke Özakca
Legal Intern
berke.ozakca@bicerguner.com

BİÇER GÜNER

Attorneys-at-Law