ERDEM & ERDEM

Personal Data Protection Bulletin

2024
Second Quarter

Sevgi Ünsal Özden
Gülnur Çakmak Ergene
Orhan Emin Erdem
Elvan Galatalı

Current Developments from Türkiye

Amendments to the Law on the Protection of Personal Data Entered into Force

Law No. 7499 on the Amendment of the Code of Criminal Procedure and Certain Laws and Law No. 6998 on Amendments to the Law on the Protection of Personal Data (LPPD Amendments) entered into force as of 01.06.2024.

Thus, the amendments made to the articles of the LPPD regulating the processing of special categories of personal data, the transfer of personal data abroad, and the objection authority to the penalties to be imposed by the Personal Data Protection Board (Board) have become binding. However, the new provisions regarding the transfer of personal data abroad will be applied together with the old provisions until 01.09.2024.

Key Actions:

Data controllers and data processors should review their data processing activities and ensure the continuity of compliance by determining the necessary actions to harmonize their activities with the new LPPD systematics by 01.09.2024 at the latest.

Regulation on Procedures and Principles Regarding the Cross-Border Transfer of Personal Data, Standard Contracts and Documents on Binding Corporate Rules Have Been Published

The Personal Data Protection Authority (Authority) published the Regulation on the Procedures and Principles Regarding the Cross-Border Transfer of Personal Data (Regulation) on 10.07.2024. The Regulation includes the procedures and principles regarding the innovations introduced to the provision of cross-border transfers within the scope of the LPPD Amendments, particularly concerning the cross-border transfer of personal data through standard contracts.

In addition, standard contracts to be used in the cross-border transfer of personal data, application forms for binding corporate rules, and auxiliary guidelines on binding corporate rules were also announced on the website of the Authority.

You can access the Regulation published in the Official Gazette here and the documents announced by the Authority here.

What Has Changed in the Personal Data Protection Law Numbered 6698?

Defne Pırıldar

Latest Developments Regarding Personal Data Transfers Abroad

Defne Pırıldar

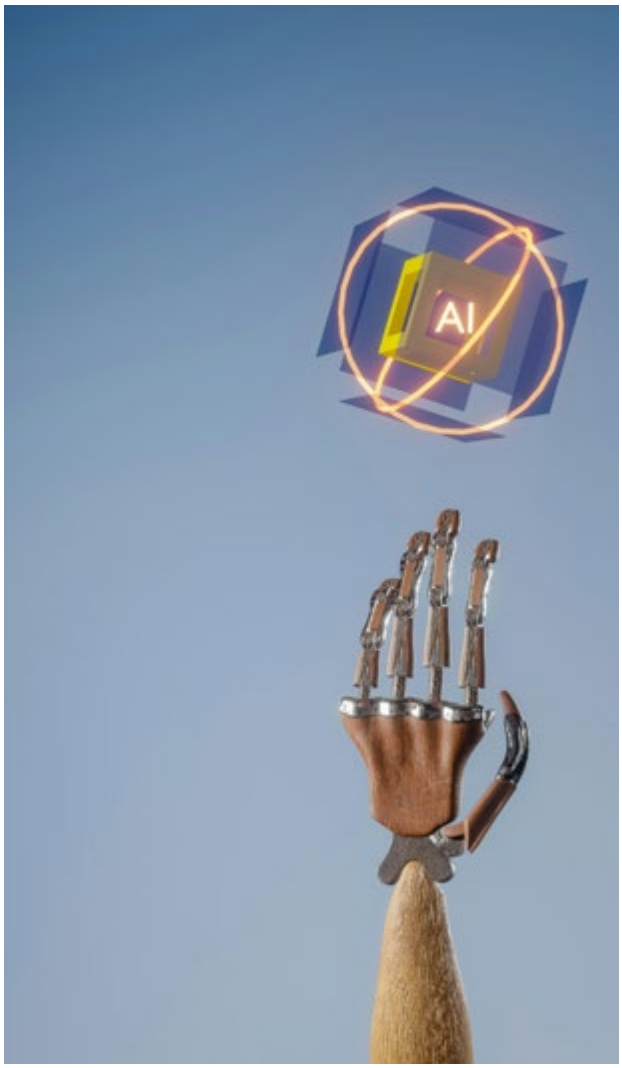
Key Actions:

- ✔ Data controllers and data processors should conduct a review of processes involving international data transfers, identify processes where transfers occur, and clarify the recipient groups involved.
- ✔ For each transfer identified, a roadmap should be drawn by determining the most appropriate option between signing standard contractual clauses, signing binding company rules, or relying on one of the exceptional transfer situations.
- ✔ All compliance documents related to the protection of personal data, including clarification texts, should be revised to ensure proper information and compliance with the requirements for international data transfers.

Türkiye's First Artificial Intelligence Draft Bill Was Submitted to Parliament

On 24.06.2024, a brief draft bill (Bill) containing regulations on artificial intelligence (AI) technology was submitted to the Grand National Assembly of Türkiye. When compared to the European Union's Artificial Intelligence Act (AI Act), the Bill includes more general and limited regulations. Although it does not fully meet the legislative needs in the field of AI, it is significant as the first legislative proposal. The Bill aims to ensure the safe, ethical, and fair use of AI technology, protect personal data, and prevent violations of privacy rights. The proposal is designed to apply to providers, distributors, deployers, importers, and distributors of AI systems. It also requires adherence to fundamental principles of safety, transparency, fairness, accountability, and privacy, but lacks detailed regulations. It is unclear which authorities will conduct inspections or how these inspections will be carried out in terms of oversight and sanctions.

You can access the Bill here.



Advertising Board Imposed Administrative Sanctions on E-Commerce Platforms

At its meeting dated 12.03.2024, the Advertising Board examined the membership, personal data processing, targeted advertising and marketing processes of 12 different e-commerce platforms and decided to impose administrative sanctions. The Advertising Board focused on various practices of the companies such as membership agreements, clarification and explicit consent texts, privacy texts and cookie policies. Within the scope of the review, unfair and deceptive practices were identified, such as the mandatory request of personal data that is not necessary, forcing consumers to accept the use of their personal data for marketing purposes, not obtaining their explicit consent and not providing guidance for membership cancellation. The Advertising Board emphasized that these commercial practices negatively affect consumers' will to make decisions or choices, that consumers are not clearly informed, and that consumers are not given the opportunity to leave their mark on the platform after purchasing a product.

Key Actions:

- ✔ If consumers' personal data will be used for marketing purposes, consumers must be informed under the law and their explicit consent must be obtained. Consent applications should be designed in a way that consumers can easily understand and withdraw their consent when necessary.
- ✔ Consumers should be provided with easy and accessible guidance on cancellation of membership; cancellation of membership should be organized as a process that consumers can perform effortlessly.
- ✔ Consumers should be allowed to leave no trace on the platform after purchasing a product.

You can access the relevant decisions of the Advertising Board here.

Council of Higher Education Published Ethical Guidelines on the Use of Productive Artificial Intelligence

The Council of Higher Education (YÖK) published the "Ethical Guide on the Use of Productive Artificial Intelligence in Scientific Research and Publication Activities of Higher Education Institutions" (Guide) to contribute to the understanding and

evaluation of the risks and opportunities of AI technology and to take measures against such risks. In the Guide, it is emphasized that one of the main ethical problems that may be encountered in the use of productive AI in scientific research and publications is the processing of personal data in violation of the legislation. YÖK stated that personal data should not be entered into these systems unless they are anonymized or masked outside of productive AI systems, and that before starting to use productive AI systems, it is necessary to have detailed information about how the systems work and their potential risks.

> The full Guide is available here.

The Constitutional Court (CC) Annulled the Provision on the Announcement of Name Change within the Scope of Personal Data Protection.

With its decision dated 22.02.2024 and numbered F. 2023/34, D. 2024/60, the Constitutional Court annulled the rule in Article 27 of the Turkish Civil Code regarding the announcement of the court decision to change the name. The decision firstly emphasizes that a person's name is personal data and that the impugned rule restricts the right to request the protection of personal data by requiring the change of name to be announced.

As a result of its evaluations, the Constitutional Court annulled the rule, which does not contain a clear regulation on the scope, content, form, and procedure of the announcement of the name change, by finding it contrary to Articles 13 and 20 of the Constitution. The relevant decision will enter into force on 16.02.2025, 9 months after its publication.

> You can access the Constitutional Court Decision here.

The Authority's Annual Report for 2023 has been published

The Authority published its Annual Report for 2023 (Report), which contains detailed explanations of its goals, objectives, and activities. According to the Report, 51 Board meetings were held in 2023 and a total of 2,242 decisions were taken as a result of these meetings. 41 of the decisions taken were published in summary form on the official website of the Authority. In addition, in 2023, the Board imposed administrative fines on 531 data controllers, including 279 for reports and complaints, 124 for data breach notifications, and 128 for registration and notification obligations in the Data Controllers Registry. The total amount of these administrative fines reached 241,082,000 TL.

> You can access the annual report published by the Authority here.

Current Developments from the World

The AI Act Entered Into Force

On 12.07.2024, the AI Act was published in the European Union (EU) Official Journal and came into force on 01.08.2024. The AI Act bans certain AI practices and sets regulations for "high-risk" AI systems, AI systems with transparency issues, and general-purpose AI (GPAI) models. The AI Act's implementation will occur in phases: prohibitions start on 02.02.2025; GPAI model regulations begin on 02.08.2025; and transparency and high-risk AI system obligations take effect on 02.08.2026. Starting from 02.08.2027 certain GPAI obligations relevant to high-risk AI systems, especially those that serve as safety components within products governed by EU product safety legislation, will start to be enforced. By 2030, additional AI systems, mainly in the public sector, will need to comply with all remaining obligations.

The Act also requires the European Commission (Commission) to issue guidelines or secondary legislation on various aspects, including definitions, transparency obligations, and relationships with existing EU legislation.

You may find the AI Act here.

Key Actions:

- Sector actors that fall within the scope of the AI Act should review and understand the specific obligations of the AI Act relevant to their AI systems.
- They should develop a timeline and action plan to meet the phased implementation deadlines and monitor updates from the Commission regarding guidelines and secondary legislation.

The European Data Protection Supervisor (EDPS) Orders Commission to Suspend Microsoft 365 Data Transfers Due to Breaches in EU Data Protection Rules

On 08.03.2024, the EDPS has decided that the Commission violated several key data protection rules while using Microsoft 365. The EDPS has found that the Commission failed to ensure appropriate safeguards for personal data transferred outside the EU/European Economic Area (EEA) and did not clearly specify the types and purposes of data collected in its contract with Microsoft. According to the EDPS, it is the responsibility of EU institutions, bodies, offices, and agencies (EUIs) to ensure that any processing of personal data outside and inside the EU/EEA, including in the context of cloud-based services, is accompanied by robust data protection safeguards and measures. As a result, the EDPS has ordered the Commission to suspend all data transfers from Microsoft 365 to countries outside the EU/EEA not covered by an adequacy decision as of 09.12. 2024, and to bring its data processing practices into compliance with EU data protection laws by the same date.

You may find the full decision here.

Key Actions:

- ✔ Robust data protection safeguards should be implemented for cross-border transfers of personal data including clear contractual terms with service providers.
- ✔ Types of personal data and purposes should be clearly specified in contracts with data processors to ensure compliance with data protection laws.
- ✔ Regular assessments should be conducted, including Data Protection Impact Assessments and Transfer Impact Assessments.

Information Commissioner's Office (ICO) Publishes A New Guidance on Data Protection Fines

On 18.03.2024, the ICO published a new guidance on data protection fines, detailing its decision-making process and criteria for issuing penalties and calculating fines. The guidance sets out the circumstances in which the ICO would consider it appropriate to exercise administrative discretion to issue a penalty notice, the maximum penalty amount that may be imposed, the ICO's approach in cases where there is more than one infringement, and how the value of a penalty is determined. The new guidance replaces the penalty notice sections in the November 2018 Regulatory Action Policy.

You may reach the full guidance here.

The French Data Protection Authority (CNIL) Publishes Latest Edition of the Practice Guide for the Security of Personal Data

On 26.03.2024, CNIL released the 2024 version of its Practice Guide for the Security of Personal Data (Practice Guide). The Practice Guide serves the purpose of reinforcing the necessary safety protocols to be implemented. The newly updated version overhauls its predecessor, introducing new fact sheets covering pivotal areas like AI, mobile applications, cloud computing, and application programming interfaces. The Practice Guide serves as a reference for Data Protection Officers, Chief Information Security Officers, computer scientists, and legal experts in their pursuit of ensuring data security.

> You may reach the full Practice Guide here.

Data Governance Framework Recommendation Report for Türkiye Has Been Published

On 01.04.2024, United Nations Development Programme (UNDP) Türkiye Country Office and the Central Digital Office issued the Data Governance Framework Recommendation Report for Türkiye (Report) to guide Türkiye's data-driven digital transformation. The Report emphasizes the urgent need to strengthen data legislation, develop a comprehensive national data strategy, and improve sector-specific policies, among other areas. It also highlights Türkiye's growing significance in global development, driven by the rapid daily increase of data across diverse sectors.

> You may find the full Report here.

ICO Sets Out Priorities to Protect Children's Privacy Online

On 03.04.2024, the ICO released its 2024 - 2025 Children's Code Strategy, which outlines priorities for protecting children's personal data online. Building on the 2021 Children's Code, the updated Children's Code Strategy advances existing efforts and identifies key areas where social media and video-sharing platforms must enhance their practices over the next year.

The Children's Code Strategy will focus on the issues of default privacy and geolocation settings, profiling children for targeted advertisements, using children's information in recommender systems, and using the information of children under 13 years old.

> You may find the announcement regarding the priorities here.

The American Data Privacy and Protection Act Draft Legislation (Draft Data Privacy Act) Was Published

On 05.04.2024, United States (US) Congress members introduced the Draft Data Privacy Act. The Draft Data Privacy Act aims to become a national data privacy and security standard that gives people the ability to enforce their data privacy rights. The primary objective of the Act is to provide a uniform, nationwide standard for data privacy, superseding the patchwork of state laws with a single federal regulation.

Entities subject to the Draft Data Privacy Act include those controlling data collection, processing, or transfer, particularly those under the Federal Trade Commission Act, with some exceptions like government entities and small businesses. The Draft Data Privacy Act foresees data minimization, transparency, consumer control, and data security obligations for entities to follow. These include limiting data processing to necessary purposes, providing clear privacy policies, granting consumer rights such as data access and opt-out options, and maintaining robust security practices.

> You may find the Draft Data Privacy Act here.

The Court of Justice of the European Union (CJEU) Decided That the Violation of the European Union General Data Protection Regulation (GDPR) Does Not Automatically Constitute Non-Material Damage

On 11.04.2024, the CJEU decided on a case concerning compensation for damages claimed by a data subject due to the unauthorized processing of personal data for marketing purposes, despite the objections sent to the data controller.

The CJEU clarified that a mere infringement of the GDPR is not sufficient, in itself, to constitute 'non-material damage', since the existence of damage is one of the conditions of the right to compensation. There must be actual proof of damage, regardless of its severity, to claim compensation. Furthermore, the CJEU highlighted that it is not sufficient for the controller, to be exempted from liability, to claim that the damage in question was caused by the failure of a person acting under its authority who failed to follow instructions. Lastly, the CJEU emphasized that administrative fines are punitive, whereas compensation under GDPR is compensatory, thus different criteria are required to determine amounts. Each member state must establish criteria for compensation, adhering to EU law principles, and multiple infringements by the controller cannot influence the compensation assessment.

> You may find the full decision here.

ICO's Released Guidance on Transparency When Processing Health Data

On 15.04.2024, the ICO issued a guidance to clarify transparency expectations for organizations that process health and social care information. The guidance applies broadly to private and third-sector organizations that provide health and social care services or process health and social care information, including for secondary purposes, such as research and planning.

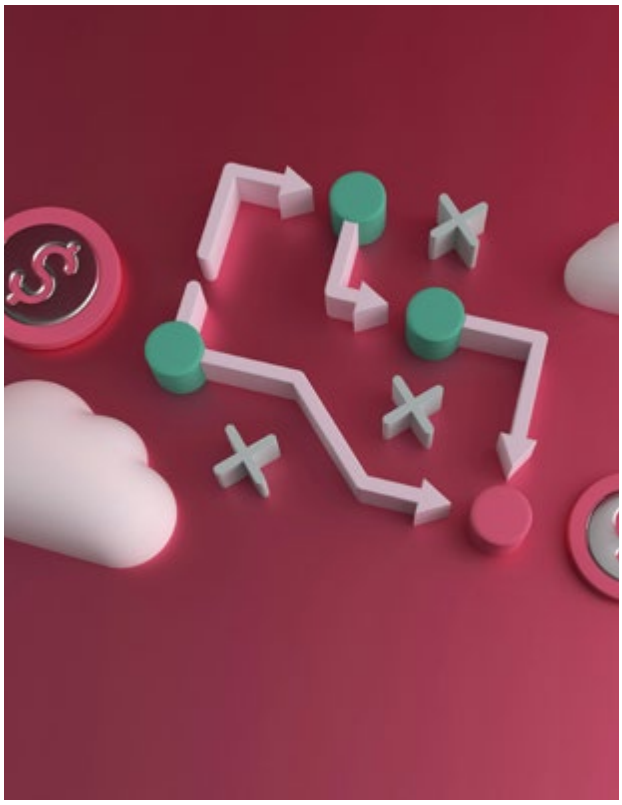
The guidance particularly emphasizes the importance of providing privacy and transparency information, to comply with data protection laws and enhance transparency practices. The new guidance may be especially useful for organizations for implementing new data collection systems, establishing a shared care record across a region to support direct care, introducing personal health record apps, conducting research programs, and creating a new system that shares hospital discharge data with social care providers.

> You may find the guidance here.

European Data Protection Board (EDPB) Issues an Opinion On "Consent or Pay" Models

On 17.04.2024, the EDPB issued an opinion in response to a request from the Dutch, Norwegian, and Hamburg Data Protection Authorities concerning the validity of consent in "consent or pay" models used by large online platforms for behavioral advertising. In its opinion, the EDPB emphasized that users must be given a real choice, as current models often force users to either consent to data processing or pay a fee, which can undermine the validity of their consent. Furthermore, the EDPB provides elements to assess the criteria of informed, specific, and unambiguous consent that large online platforms should consider when determining whether consent is valid. The EDPB's stance reinforces the idea that personal data should not be treated merely as a commodity and emphasizes the need for clear, granular consent processes that do not leverage power imbalances or obscure the implications of user choices.

Notably, the opinion specifically addresses "consent or pay" consent used only by large online platforms for data processing in behavioral advertising. However, the EDPB plans to develop broader guidelines on "consent or pay" models and engage with stakeholders to ensure comprehensive understanding and implementation.



Key Actions:

Data controllers should ensure that data subjects have a genuine choice and are not forced to either consent to data processing or pay a fee, maintaining the validity of their consent. The EDPB's guidance is critical for large online platforms, which may need to reassess their consent models and business practices to ensure compliance with GDPR and respect for user privacy.

You may find the full opinion here.

The Spanish Data Protection Agency (AEPD) Fines Caixabank S.A. For Not Obtaining Data Subject's Consent

On 18.04.2024, the AEPD imposed a €1,200,000 fine on Caixabank S.A. for accessing an individual's General Treasury of the Social Security (TGSS) data without proper consent.

Caixabank used a mandatory subscription procedure, via a "framework contract," to collect and verify customer data with the TGSS. The AEPD found that this procedure does not meet GDPR's consent requirements, which mandate consent to be freely given, specific, informed, and unambiguous. The framework contract enacted a mandatory model clause and failed to ensure that explicit consent was obtained by only referring to legal obligations to prevent money laundering and terrorist financing. In its decision, the AEPD clarified that the law does not mandate verifying personal data with the TGSS; instead, customers must provide such information, and banks must then verify it based on risk levels.

> You may find the decision, only in Spanish here.

ICO Publishes Its Strategic Approach To AI

On 01.05.2024, the ICO published its strategic approach to AI regulation, in response to a request by the Secretary of State for Science, Innovation and Technology.

The ICO's strategy, titled "Regulating AI: The ICO's strategic approach", highlights the opportunities and risks of AI, particularly about fairness, bias, transparency, safety, and accountability. Key areas of focus include foundation models, high-risk AI applications, facial recognition, biometrics, and children's AI use. It includes a roadmap for organizations to evaluate their data protection obligations and details the ICO's AI-specific guidance, enforcement actions, and resources. The ICO also notes upcoming consultations on generative AI, biometric classification, and updates to its AI and data protection guidance.

> You may find the ICO's strategic approach here.

CJEU Issues Opinion on the Use of Publicly Available Data for Targeted Advertising

On 25.04.2024, the Advocate General of the CJEU released an opinion in Case C-446/21 concerning the use of public statements for personalized advertising. The case originated when Maximilian Schrems, who accepted Facebook's 2018 terms of service, received advertisements targeted at homosexuals based on his interests rather than his sexual orientation. Schrems filed a complaint in the Austrian court, which in essence, directed two questions to the CJEU: (1) Whether all personal data obtained by a platform like Facebook can be aggregated, analyzed, and processed for targeted advertising indefinitely and without limitation on the type of data; and, (2) whether a public statement about one's sexual orientation, made during a panel discussion, permits processing other related data for personalized advertising.

The Advocate General opined that the GDPR prohibits indefinite processing of personal data for targeted advertising, emphasizing that national courts must assess the proportionality of data retention periods and data amounts against the legitimate aim of personalized advertising. Additionally, he noted that a public statement about sexual orientation does not permit the processing of such data for targeted advertising, even if the data is publicly known.

The opinion provides clarity on the limitations of data processing within social networks, emphasizing the need for data controllers to justify the extent and manner of data usage strictly within the bounds set by the GDPR.

Key Actions:

- ✔ Any data processing must be proportional and justified concerning its purpose.
- ✔ Making sensitive personal data publicly known, does not automatically allow for further processing for unrelated purposes like advertising. Therefore, any subsequent processing needs to comply with GDPR principles including lawfulness, fairness, and purpose limitation.

You may find the opinion here.

Key Contacts

Mert Karamustafaoğlu
Partner, Competition and Compliance Leader

mertkaramustafaoglu@erdem-erdem.av.tr

Sevgi Ünsal Özden
Managing Associate and Mediator

sevgiunsal@erdem-erdem.com

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