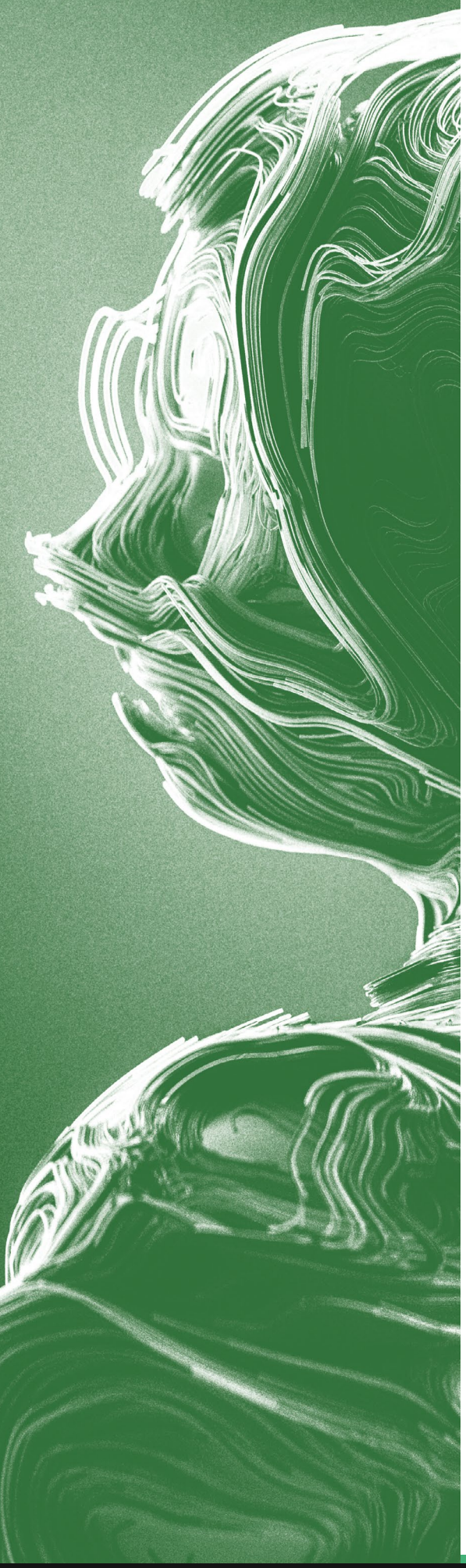


ERDEM & ERDEM

Personal Data Protection Bulletin

2024
Fourth Quarter

Sevgi Ünsal Özden
Gülnur Çakmak Ergene
İpek Ertem

www.erdem-erdem.av.tr

Current Developments from Türkiye

The Personal Data Protection Authority (Authority) Published the Guide on Cross-Border Transfer of Personal Data

The Authority published the long-awaited Guide on Cross-Border Transfer of Personal Data on January 2, 2025. The Guide details the principles and procedures for implementing the comprehensive amendments made to Article 9 of the Personal Data Protection Law No. 6698 (KVKK), which regulates the transfer of personal data abroad. It outlines the mechanisms for cross-border data transfers and guides relevant parties through specific examples to ensure compliance with the prescribed requirements.

> You can access the Guide in Turkish here and our related announcement here.

Key Actions:

- ✓ Data controllers based in Türkiye that transfer personal data abroad or operate as part of a global group company should carefully review the Guide on Cross-Border Transfer of Personal Data and its examples. They should promptly implement appropriate transfer mechanisms to align their cross-border data transfer processes with the updated regulations.

The Authority Published the Information Note on the Application of Misdemeanors in Terms of Time

The Information Note on the Application of Misdemeanors in Terms of Time, published by the Authority on December 19, 2024, provides comprehensive explanations regarding the temporal application of new regulations introduced to processing special categories of personal data and cross-border transfers under the KVKK amendments. The information note includes a guiding table containing criteria to be considered in determining the applicable provisions, taking into account the time differences between the occurrence of acts of misconduct, the dates of data subject complaints, and the decisions to be made by the Personal Data Protection Board (the Board).

> You can access the Information Note in Turkish here and our related announcement here.

The Authority Published the Information Note on ChatGPT and Similar Chatbots

The Information Note on Chatbots (ChatGPT Example), published on November 8, 2024, provides key insights into the personal data processing activities of Artificial Intelligence (AI)-powered chatbots. According to the note, chatbots simulate human conversation and may process user data to provide services, enhance user experience, and fulfill legal obligations. In this context, it is emphasized that clear information must be provided to users regarding how their personal data will be processed, with whom it will be shared, and the retention period. Additionally, it is highlighted that issues such as age verification for AI chatbots, raising user awareness, risk assessment, data security measures, and compliance with the KVKK are of critical importance.

> You can access the Information Note in Turkish here and our related announcement here.

The Authority Published a Public Announcement on the Standard Contract Notification Module

Under the KVKK amendments, standard contracts have been defined as an appropriate safeguard for cross-border transfers, and parties must notify the Authority within five business days of signing a standard contract. Such notifications may be submitted physically, via Registered Electronic Mail (KEP), or through other methods determined by the Board. Accordingly, it was announced with the Board's decision dated October 17, 2024, that the Standard Contract Notification Module has been launched to facilitate swift and efficient notifications.

> You can access the Public Announcement in Turkish here and our client alert with further details here.

The Authority Published the 2024 Annual Activity Information Note

The Authority released its 2024 Annual Activity Information Note, which provides detailed explanations regarding its objectives, targets, and activities. According to the note, in 2024, the Authority received 281 personal data breach notifications, 1.345 standard contract notifications, and concluded 6.958 out of 8.186 complaints and notifications. Additionally, three undertakings regarding cross-border data transfers were approved, administrative fines totaling 552.668.000,00 TL were imposed under the KVKK, and 110 legal opinions were issued on matters within the Authority's jurisdiction.

> You can access the Activity Information Note in Turkish here.

The Grand National Assembly of Türkiye (TBMM) Established a Parliamentary Inquiry Commission on AI

"The Decision on the Establishment of a Parliamentary Investigation Commission for Determining Actions to be Taken for the Achievements of Artificial Intelligence, Establishing the Legal Framework in this Field, and Identifying Measures to Prevent the Risks Associated with the Use of Artificial Intelligence" was published in the Official Gazette, issue 32683, dated October 5, 2024.

According to the decision, the commission, consisting of 22 members, will continue its work for 3 months starting from the election of the President, Vice President, Spokesperson, and Secretary, and will carry out its activities outside of Ankara if necessary. In this regard, the decision regarding selecting members was published in the Official Gazette, issue 32784, dated January 16, 2025.

> You can access the relevant decision in Turkish here and the decision on member selection in Turkish here.

The Turkish Constitutional Court Found the Rejection of an Employee's Request to Access Their Personnel File Unconstitutional

In the case subject to the Constitutional Court's decision dated July 17, 2024, the applicant's request for access to the performance records and evaluation notes in their personnel file was rejected, which was considered a violation of the right to respect for private life and the right to request the protection of personal data. The decision emphasized that the Constitution guarantees the right to request the protection of personal data and can only be limited based on 'confidentiality' with a legal foundation. As a result, the applicant was awarded 30.000,00 TL in moral compensation.

> You can access the relevant decision in Turkish here.

Key Actions:

- ✔ In responding to access requests regarding personal data, data controllers should only reject such requests if an explicit legal provision allows it. In cases where an access request is denied, data controllers must clearly and transparently inform data subjects of the legal grounds for the rejection.

Board Decision Summaries:

Board Decision on the Unlawful Processing of Personal Data for Subscription Establishment

In the case at hand, the data subject mistakenly accessed a fraudulent website during the commitment renewal process for their internet subscription and shared their personal information, resulting in an unintended subscription to another brand (Brand X). The data subject claimed that the website closely resembled the official website of their current service pro-

vider, leading to deception and the unlawful processing of their personal data. The accused Company B (the owner of Brand X), argued that the personal data had been unlawfully collected and added to the system by its subsidiary, Company C, and therefore, the responsibility lay with Company C.

According to the decision, Company C, despite being classified as a data processor under its contract with Brand X and being required to act by the main company's instructions and contract provisions, misled potential customers by using visuals belonging to another company. By unlawfully processing personal data, Company C was deemed a data controller. The data subject's consent was found invalid due to deception, and the processing activity lacked a legal basis. Consequently, Company C was fined 450,000 TL for failing to fulfill data security obligations.

> You can access the Board decision summary in Turkish here.

Board Decision Regarding a Cyber Attack on an E-Commerce Platform

The decision states that unauthorized individuals accessed the seller portal of an e-commerce platform using usernames and passwords obtained from other platforms. As a result, the identities, contact details, financial, and transaction data of 673 sellers and 7.202 customers were affected. It was revealed that cyber attackers carried out targeted attacks by exploiting a vulnerability in the platform, and that the "Bot" traffic prevention system was insufficient. Critical security measures, such as one-time passwords, were only activated after the breach. Despite numerous login attempts from the same IP address, the breach could not be detected in time, and effective measures like two-factor authentication were not implemented beforehand. These lapses were considered negligence on the part of the data controller. Due to these deficiencies, an administrative fine of 3.250.000,00 TL was imposed on the data controller.

> You can access the Board decision summary in Turkish here.

Key Actions:

- ✓ On online platforms, strong authentication methods should be implemented for username and password security; existing vulnerabilities should be identified, and effective measures should be taken against cyber-attacks. Unusual login attempts to the system should be monitored, and breaches must be detected in a timely manner.
- ✓ Data controllers should establish rapid response protocols for security vulnerabilities; regular security audits and risk analyses should be conducted.
- ✓ Technical support should be sought when determining personal data security measures.

Current Developments from the World

The Turkish Brochure of The Council of Europe Framework Convention on Artificial Intelligence and Human Rights, Democracy, and The Rule of Law (Framework Convention) Has Been Published

As detailed in our previous bulletin, the Framework Convention, opened for signature on September 5, 2024, is the first international agreement to ensure AI systems align with human rights, democracy, and the rule of law. It enters into force 3 months after at least 5 signatories, including at least 3 Council of Europe member states, have ratified it.

The Council of Europe has published the Turkish brochure of the Framework Convention. The brochure serves as a concise and comprehensible guide for public authorities and the private sector, outlining the necessary measures for compliance, risk and impact assessments, and principles for AI use aligned with human rights and democracy.

> You can access the brochure published by the Council of Europe in Turkish here.

The United Kingdom Information Commissioner's Office (ICO) Published A Report on AI-Assisted Recruitment Tools

On November 6, 2024, ICO published the results of a series of voluntary audits conducted on AI-assisted recruitment tools. The audits revealed that some AI tools failed to conduct accuracy and bias testing, collected excessive data, and breached data protection responsibilities. However, successful practices such as transparency and data minimization were also observed. ICO has issued 7 key recommendations focusing on fairness, transparency, data minimization, and Data Protection Impact Assessments (DPIA).

The report summarizes good practices and issues while publishing a list of questions for organizations procuring AI recruitment tools.

> You can access the report here and the list of questions here.

Hamburg Commissioner for Data Protection and Freedom of Information Fines Debt Management Company €900,000 for Failure to Comply with Data Destruction Obligations

During sector-wide audits, the Hamburg Commissioner for Data Protection and Freedom of Information discovered that a debt management company had retained the personal data of debtors for approximately 5 years, even though the legal retention periods had expired. Due to the company's failure to develop and implement an appropriate data destruction policy according to the mandated retention periods, the authority imposed a €900.000,00 administrative fine.

The Hamburg Data Protection Authority also found similar deficiencies in other audits and emphasized the need for companies to develop more effective policies to ensure compliance with data minimization and destruction processes.

> You can access the relevant decision in German here.

Key Actions:

- ✔ Data controllers should establish or review policies to ensure compliance with legal retention and deletion periods and periodically identify and delete data whose retention period has expired.

2024/2847 Numbered Cyber Resilience Act (CRA) Enters into Force

The CRA, which sets cybersecurity requirements for products with digital elements to ensure their secure placement on the market, was published in the Official Journal of the European Union on November 20, 2024, and entered into force on December 10, 2024. The CRA establishes mandatory cybersecurity requirements for the design, development, production, and market placement of products containing digital elements, including software and hardware.

> You can access the CRA here and our announcement on this topic here.

European Commission Publishes First Two Drafts of the General-Purpose AI (GPAI) Code of Practice

On November 14, 2024, the European Commission published the first version of the GPAI Code of Practice Draft. The second version of the draft was prepared by independent experts based on feedback received on the first draft and was published on December 19, 2024. The draft details the responsibilities of GPAI providers on issues such as transparency, copyright obligations, and systemic risk assessments, while aiming to ensure compliance with the new rules that will come into effect after August 2, 2025. Additionally, special measures, model evaluations, and cybersecurity obligations for the most advanced GPAI

models carrying systemic risk are addressed. The draft aims to specify the obligations of the European Union (EU) AI Act in more detail and seeks to strike a balance between flexibility and clear commitments. Work on the second draft is ongoing, and the third draft is expected to be published on February 17, 2025.

You can access detailed information on the Code of Practice here.

European Data Protection Board (EDPB) Published Draft Guidelines on the Application of the Legitimate Interest Processing Condition

EDPB, Avrupa Birliği Genel Veri Koruma The EDPB has published Draft Guidelines 1/2024 on the situations where the legitimate interest processing condition under the EU General Data Protection Regulation (GDPR) may be applied. The guidelines update the previously published Opinion 06/2014 of the Working Group in light of the GDPR and European Court of Justice rulings, providing practical information on assessing the legitimate interest processing condition. Specifically, it addresses whether legitimate interest can be considered a valid legal basis in fraud prevention, direct marketing, and information security cases.

The guidelines also propose a three-step assessment process to conduct a balancing test between the legitimate interests of the data controller or third party and the fundamental rights and freedoms of the data subject that may be affected by the data processing activity. It emphasizes that appropriate accountability documentation should be prepared at each step.

You can access the Draft Guidelines here.

Key Actions:

- ✓ Data controllers should conduct the three-step balancing test before relying on legitimate interest as a legal basis. If individuals' fundamental rights and freedoms outweigh the data controller's legitimate interest, personal data should not be processed based on this condition, and an alternative lawful basis should be considered.

European Commission Launched Investigation into Temu under the Digital Services Act (DSA)

The European Commission has formally investigated whether Temu, designated as a Very Large Online Platform (VLOP), has violated the DSA. The review will focus on issues such as the sale of illegal products, addictive design risks, content and product recommendation systems, and access to data for researchers. Based on Temu's risk assessment report submitted in September 2024 and information from national authorities,

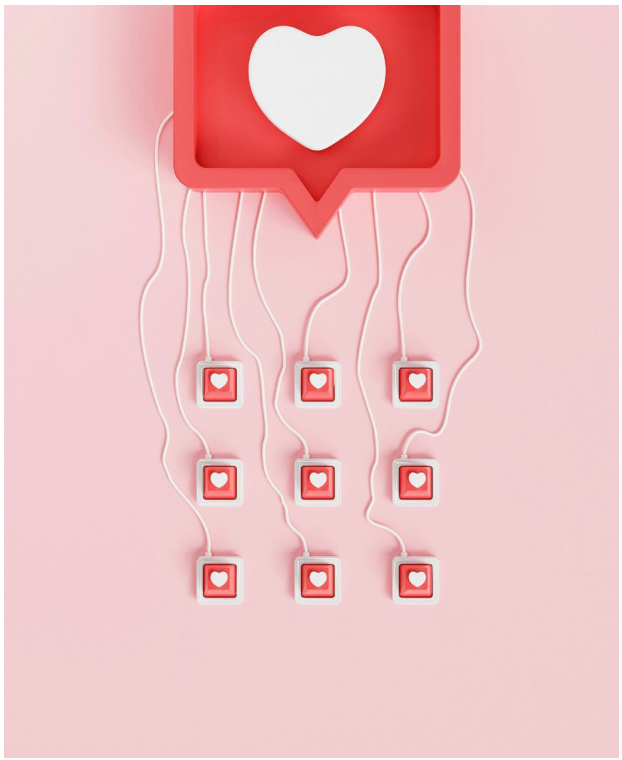
the Commission will evaluate whether the platform's past violation prevention mechanisms and transparency obligations align with DSA requirements.

> You can access the European Commission's announcement here.

European Commission is Examining Recommendation Systems of YouTube, Snapchat, and TikTok under DSA

The European Commission has requested information from YouTube, Snapchat, and TikTok regarding operating their recommendation systems under the DSA. Under DSA, platforms must assess whether their algorithms pose risks related to user mental health, harmful content dissemination, addiction, and child protection and take steps to mitigate such risks. YouTube and Snapchat have been asked for details on content recommendation algorithms and illegal content prevention measures, while TikTok has been requested to clarify steps taken to prevent manipulative practices and mitigate risks during elections. Further investigations may follow if necessary, and administrative fines may be imposed for incomplete or misleading responses.

> You can access the Commission's announcement here vand details on follow-up questions here.



Dutch Data Protection Authority Fines Netflix €4.750.000,00 for Transparency Violations

The Dutch Data Protection Authority found that between 2018 and 2020, Netflix failed to provide users with sufficient and precise information regarding the processing of their personal data. As a result, the streaming platform was fined €4.750.000,00. Netflix has since appealed the decision and updated its privacy policy to enhance transparency and user notification practices.

> You can access the decision in Dutch here.

Irish Data Protection Commission (DPC) Announces €251.000.000,00 Fine Against Meta

The DPC imposed a total fine of €251.000.000,00 on Meta Platforms Ireland Limited following investigations into security vulnerabilities in Facebook's video upload feature, which exposed user profiles to unauthorized access. The breach, which occurred in July 2017, affected 29 million accounts globally, including 3 million in the EU and EEA, compromising various types of personal data, including sensitive information. The DPC penalized Meta due to failures in breach notification, inadequate documentation of remedial actions, lack of integration of data protection principles into the system's design, and non-compliance with default data protection obligations.

> You can access the DPC's announcement here.

The Court of Justice of the European Union (CJEU) Confirms That Competitors Can Sue for GDPR Violations

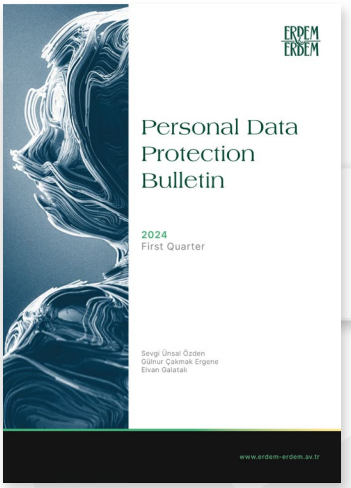
In the case C-21/23 before the CJEU, a competitor filed a lawsuit against the German *Lindenapotheke* pharmacy, which marketed pharmacy-only medicinal products on Amazon while collecting customers' personal data. The claimant requested that such sales be halted unless it was ensured that customers had given prior consent for processing their health data by asserting that this constituted an unfair commercial practice under German competition law.

The CJEU ruled that competitors may file lawsuits against GDPR violations under the scope of unfair commercial practices, and emphasized that GDPR enforcement mechanisms are not limited to consumer complaints and supervisory authorities. It acknowledged that lawsuits initiated by competitors may not always be motivated by data protection concerns but could aim to ensure fair competition. The Court further stated that such actions could contribute to GDPR compliance.

The CJEU had previously stated in the Meta v *Bundeskartellamt* case that national competition authorities may assess compliance with data protection rules. Lindenapotheke's case also emphasizes the importance of compliance with data protection rules to ensure fair competition. Therefore, this ruling is considered an example of the increasing interaction between competition law and data protection law.

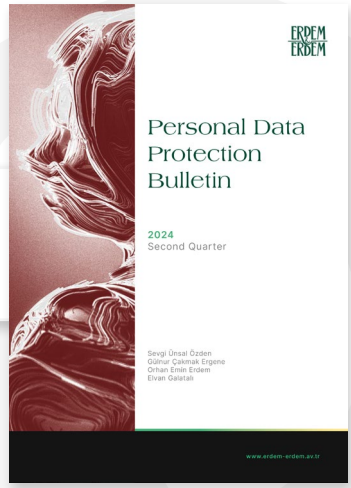
> You can access the CJEU's decision here.

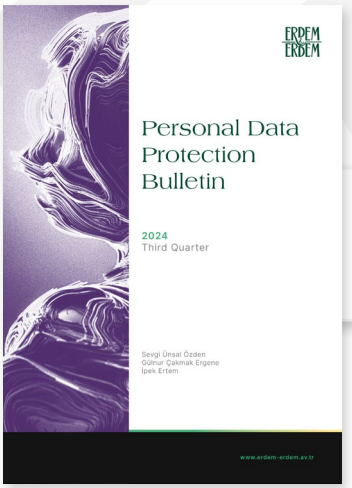
You can access the previous issues of Erdem & Erdem Personal Data Protection Bulletin below:



Personal Data Protection Bulletin
Q1 of 2024

Personal Data Protection Bulletin
Q2 of 2024



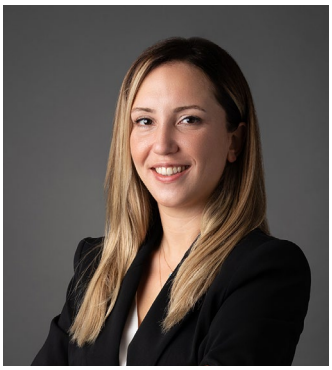


Personal Data Protection Bulletin
Q3 of 2024

Key Contacts

Özgür Kocabaşoğlu
Partner and Head of Corporate

ozgurkocabasoglu@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