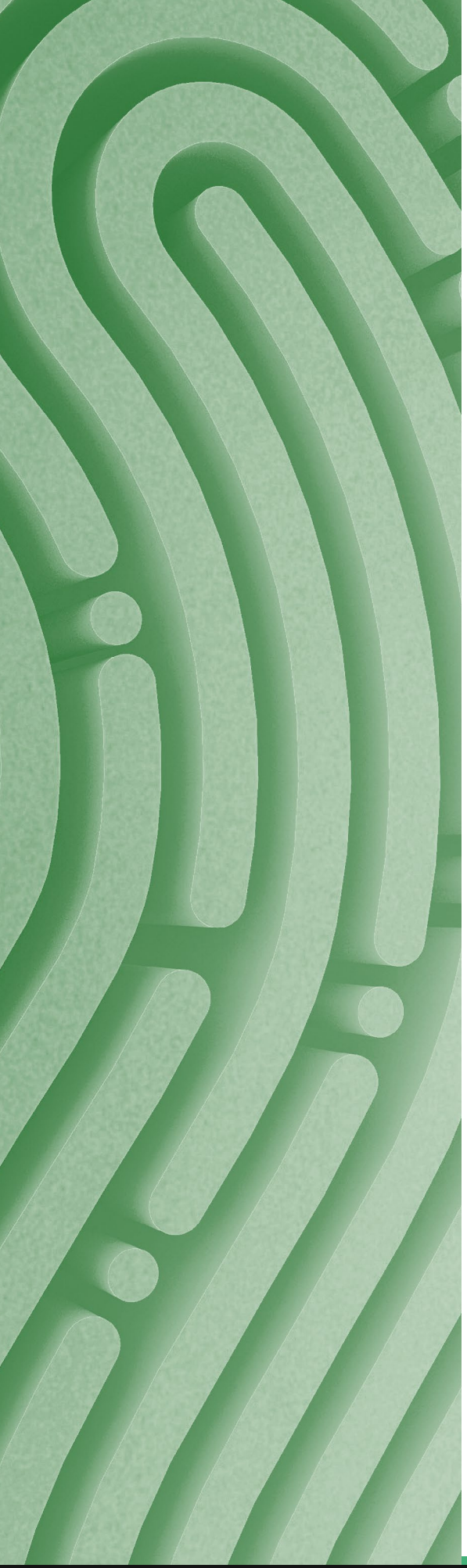


ERDEM & ERDEM

Personal Data Protection Bulletin

2023
Fourth Quarter

Sevgi Ünsal Özden
Gülnur Çakmak Ergene
Defne Pırıldar
Doğukan Kalınoğlu
İlayda Salkım

www.erdem-erdem.av.tr

Recent Updates from Türkiye

Public Announcement Regarding the Processing of Personal Data by Sending a Verification Code via SMS to the Data Subjects During Shopping in Stores Has Been Published

On 13 November 2023, the Authority published the Public Announcement ("Announcement") on the Processing of Personal Data by Sending a Verification Code via SMS to Data Subjects during Shopping in Stores. Accordingly, (i) informing the recipients by the store authorities about the purpose of the SMS sent during the cashier transactions and the consequences that may arise if the code transmitted via SMS is given and providing the information channels to the recipients via SMS; (ii) separating the steps of the obligation to inform and obtaining explicit consent from each other; (iii) obtaining explicit consent separately for different activities that require explicit consent during cashier transactions; (iv) not offering the processing of personal data for the purpose of sending commercial electronic messages as a condition for the completion of the shopping; and (v) in case the explicit consent for sending commercial electronic messages is obtained via SMS verification code, it must meet the conditions sought in the PDPL.

You may find the announcement published by the Authority here and our announcement on this subject here.

Recommendations on Protecting Privacy in Mobile Applications Published

On 22 December 2023, the Authority published Recommendations for the Protection of Privacy in Mobile Applications ("Mobile Application Guideline"). With the Mobile Application Guideline, which addresses the existing and potential risks to the protection of privacy in mobile applications by way of example, general recommendations were made for data subjects and data controllers in terms of personal data processing activities carried out through mobile applications used on smartphones and tablets.

You may find the Mobile Application Guideline here.

Cooperation Protocol Signed Between the Personal Data Protection Authority and the Competition Authority

A "Cooperation and Information Sharing Protocol" ("Protocol") was signed between the Authority and the Competition Authority on 26 October 2023. With this cooperation between the authorities, it is aimed to prevent the practices of undertakings that

may harm both the privacy of personal data and the establishment of effective competition through big data technologies, to establish active and effective competition and to strengthen the control of consumers over their personal data.

You may find the Authority's announcement here and our announcement on this subject here.

The 2024 Presidential Annual Program Published

The 2024 Presidential Annual Program was published in the Official Gazette dated 25 October 2023 and numbered 32350 (Bis). This program includes a number of measures regarding the protection of personal data, such as the completion of the European Union ("EU") harmonization process, determination of national standards for the protection of personal data by taking into account international standards in the digital transformation of the business and investment environment within the scope of the studies before the European Commission, preparing and implementing the National Data Strategy and Action Plan, and conducting studies that set out the basic approach and rules regarding cross-border data transfers.

The 2024 Presidential Annual Program is available here.

Guideline on the Processing of Genetic Data Published

On 13 October 2023, the Personal Data Protection Authority ("Authority") published the Guideline on Matters to be Considered in the Processing of Genetic Data ("Guideline"). The Guideline addresses the concept of "genetic data", which is characterized as sensitive personal data pursuant to Protection of Personal Data Law ("Law" or "PDPL") and is subject to special protection, but is not comprehensively defined. After providing the definition of genetic data, the Guideline addresses the obligations of data controllers under the headings of genetic data principles and data security, and provides recommendations on administrative and technical measures that can be taken.

You may find the Guideline here.

Click here for the related Exlibris article:

The Guidelines on Processing of Genetic Data has been Published

Defne Pırıldar / November 2023

Board Decision Summaries

The Personal Data Protection Board ("Board") published 31 (thirty-one) new decision summaries on December 27, 2023. We have compiled the prominent decision summaries for you:

1. Board Decision on the Mandatory Recording of Credit/Debit Card Information for Shopping on E-Commerce Sites

In the case at hand, in order to shop on an e-commerce website, it was mandatory to register the credit/debit card information of the customers on the payment screen. At the same time, the relevant e-commerce website did not inform the data subjects and did not obtain their explicit consent for this processing activity. The Board emphasizes that the e-commerce website may process the card information for the completion of the shopping, but the continued processing of the card information in the membership account after the shopping constitutes a change of purpose and the card information can only be stored with the explicit consent of the data subject.

You may find the summary of the Board's decision here.

Key Actions:

- ✓ Explicit consent for transactions that are not directly related to a service should not be required for the provision of that service.
- ✓ If data processing is to be carried out for a purpose other than the purpose for which the personal data was obtained, the appropriate data processing condition should be determined by making a separate assessment for this purpose. If other grounds of lawfulness are not applicable for the new purpose, the explicit consent of the data subject must be obtained.
- ✓ Data subjects should always be informed about the processing of their personal data.

2. Board Decision on Sending a Text Message by the Cargo Company Employee to the Related Person's Phone After Delivery

In the case subject to the decision, a harassing message was sent to the data subject by the courier who delivered the product after shopping from an online shopping website. As a result of the investigation initiated by the data controller against the online website, the Board firstly assessed that the data controller is responsible for the breach in question within the scope of the provisions of the employer liability under the Turkish Code of Obligations (No. 6098) and the responsibility of the main employer under the Labor Law (No. 4857).

The Board imposed an administrative fine due to the fact that the data controller who is the main employer, did not provide any training and necessary information on the protection of personal data and data security to the person working on its behalf at the time of the incident.

You may find the summary of the Board's decision here.

Key Actions:

- ✔ Data controllers must periodically provide training on personal data protection and data security to all employees, including sub-employer's employees, who come into direct contact with personal data, ensure that these trainings are provided and carry out periodic audits.

3. Board Decision on Access to the E-mail Account of the Relevant Person Who Left the Company Partnership

In the case where the e-mail messages sent to the corporate e-mail account of the data subject who left the partnership at the data controller company were read, the Board determined that messages continued to be sent to the previously used and inactive e-mail address of the data subject and that the e-mail data is personal data. In the decision, it is evaluated that by not preventing the sending of messages to the e-mail address of the data subject who left the job, it is possible to view the messages sent, and this situation is considered to be a data breach.

You may find the Board's decision summary here

Key Actions:

- ✔ The option of forwarding the e-mail account of employees and partners who left the job to a different company employee should be avoided to the extent possible; sending messages to these accounts should be prevented and the possibility of unauthorized access to messages should be eliminated.

4. Board Decision on the Submission of Images of Employee's Worship by the Employer to the Case File

In a case where a company employee's images inside a place of worship were recorded by the employer without his/her consent and submitted to the lawsuit file between the parties, the Board determined that the employer, the data controller, processed data regarding the religious belief of the data subject, which is a sensitive personal data, through the video recordings of the employee inside the place of worship by means of cameras. The Board once again emphasized its view that the explicit consent given by the employee will not be valid in cases where the employee is not provided with the opportunity not to give consent directly due to the existing power imbalance in the employment relationship and did not accept the explicit consent obtained retrospectively by the employer in the case at hand.

The Board also considered that the employees had a reasonable expectation of privacy in terms of changing rooms, toilets, showers, prayer rooms, restrooms, and breastfeeding rooms and that the visualization of these areas by the employer violated this expectation and invaded the private areas of the employees. Finally, the Board stated that the monitoring activity was unlawful, stating that the masjid did not have any characteristics that would oblige it to be monitored within the framework of the working area.

You may find the summary of the Board's decision here.

Key Actions:

- ✔ Taking into account the existing power imbalance in the employment relationship, the employee should always be given the opportunity not to give consent and the option of not giving consent should not be tied to a negative outcome.
- ✔ Areas where employees have a reasonable expectation of privacy should not be monitored and video recorded unless there is a justifiable reason to compel this situation.

5. Board Decision on the Unlawful Processing of Personal Data by the Data Controller, Who is the Distributor and Sole Authorized Agent in Turkey of a Widely Participated Online Game

In the case at hand, the Board conducted an on-site inspection at the headquarters of the data controller gaming company and the company from which it receives services, and made important assessments on the fulfillment of the disclosure obligation and the use of cookies. Accordingly, it was evaluated that the presentation of 3 (three) different disclosure texts ("Sign Up Disclosure Text", "Privacy Policy" and "Personal Data Protection Policy") on the website of the data controller created a complex situation for the data subjects; it was reiterated that ambiguous expressions such as "shareable" should not be included and the disclosure texts should be in compliance with the PDPL and secondary legislation. Finally, it was determined that the disclosure texts were not compatible with each other and with

Data Controllers Registry ("VERBIS") records, and that they did not accurately reflect the transfer activities of the data controller.

In the decision, it was determined that under the pop-up description of cookies on the website, 2 (two) options, "use only necessary cookies" and "allow all cookies", were offered, and thus, collective explicit consent was obtained from the data subjects. The Board emphasizes that it is necessary to obtain explicit consent through the "opt-in" method by providing options for each type of cookie that requires explicit consent. On the other hand, in cases where third-party cookies are placed on the website, both the website owner and the third party are obliged to inform users about the cookies. in f services are received from third-party cookie providers located abroad, it is stated that the consent of the website users regarding the transfer abroad should be obtained or other transfer methods stipulated in the PDPL should be applied.

You may find the Board's decision summary here.

Key Actions:

- ✓ Multiple disclosure texts under different names should not be prepared for a single data processing activity.
- ✓ For each type of cookie other than mandatory cookies, the data subject should be given the option to give or not to give consent separately by the "opt-in" method. Consent should not be obtained collectively as "Allow all cookies".
- ✓ In the case of working with third-party cookie providers located abroad, the transfer conditions regulated in the PDPL must be fulfilled for the transfer abroad.

6. The Constitutional Court Finds the Rejection of the Objection to the Administrative Fine Imposed by the Board by the Criminal Judgeships of Peace without Justification Unconstitutional

In the case subject to the decision, the Board decided to impose an administrative fine of 1.450.000,00 TL against the data controller because the necessary technical and administrative measures to ensure data security were not taken. The applicant appealed against the administrative fine before the Criminal Judgeship of Peace on various grounds. However, as a result of the examination made by the Criminal Judgeship of Peace, the objection was rejected without justification, considering that the administrative fine was appropriate.

The Constitutional Court ruled that the applicant's allegations were important allegations that affected the entire judicial process and had to be met, and therefore the fact that no evaluation was made about the applicant's objections violated the property right.

You may find the Constitutional Court's judgement here.

Recent Developments from the World

On 8 December 2023, European Parliament Reached a Provisional Agreement with the Council on the Artificial Intelligence Act

As a result of 2 (two) years' worth of discussions and intense final negotiations which the European Union trialogues concluded on 8 December 2023, the provisional agreement on the Artificial Intelligence Act ("AI Act") was reached.

The AI Act divides artificial intelligence ("AI") systems into various risk categories to which different rules apply and impose obligations on manufacturers, importers, deployers and operators of AI systems, even if they are not based in the European Union ("EU"). Sanctions for breach of obligations are important for deterrence. In order for the agreed text to become EU law, it must first be formally adopted by the European Parliament and the Council.

You can read the announcement on the provisional agreement here.

Key Actions:

- ✓ The Artificial Intelligence Act is a legal regulation that will be directly applicable in Member States without the need for additional regulation by national legislators and also has a cross-border application area. Therefore, it is important for the parties falling within the scope of the Artificial Intelligence Act to identify their obligations and start preparations without delay to harmonize with the legal regulations.

Click here for more details:

The European Union AI Act

03.01.2024

The Data Act Entered into Force

The Regulation (EU) 2023/2854 of the European Parliament and of the Council of 13 December 2023 on harmonized rules on fair access to and use of data and amending Regulation (EU) 2017/2394 and Directive (EU) 2020/1828 ("Data Act") entered into force on 11 January 2024, after the European Parliament endorsed the final version on 9 November 2023. This legislation is designed to govern the sharing and utilization of personal and non-personal data within the EU. It responds to challenges posed by Internet of Things (IoT) devices, aiming to cultivate an effective, equitable, and innovative data economy. The Data Act will be will start to apply in 20 months, on 12 September 2025.

You may find more information and the EU Data Act here.

Key Actions:

- ✓ Businesses affected by the Data Act should proactively assess the impact of the regulation and establish an action plan to ensure full technical, legal, and administrative compliance.

Click here for more details:

The European Union Data Act

10.01.2024

The Court of Justice of the EU Has Decided that the Right of Access Takes Precedence over Local Legislation

On 26 October 2023, the Court of Justice of the European Union ("CJEU") ruled that under the General Data Protection Regulation ("GDPR"), patients have the right to receive a free copy of their medical records, even if regulated otherwise under local law. In its decision, in the case C-307/22 (FT v DW), the CJEU declared that a provision in German law allowing doctors to charge patients for access to their medical records is not in line with EU law. The case involved a patient who requested access to his dental records to check for errors. The CJEU emphasized that, in general, exercising the right of access under the GDPR should not incur costs for the individual. The court clarified that the GDPR does not require individuals to provide reasons for their access request, and rejection based on this ground is not permitted. Furthermore, the CJEU reiterated that data subjects must receive a complete and understandable reproduction of their data, including full copies of relevant documents. This is essential for individuals to comprehend and verify the accuracy of data processing.

You may see the CJEU's press release here.

On 27 October 2023, the European Data Protection Board Adopted an Urgent Binding Decision on Processing of Personal Data for Behavioral Advertising by Meta

The European Data Protection Board ("EDPB") made an urgent binding decision instructing the Irish Data Protection Authority ("Irish DPA") to finalize measures within two weeks regarding Meta Ireland Limited (Meta IE). The decision requires the Irish DPA to impose a ban on processing personal data for behavioral advertising across the entire European Economic Area ("EEA") based on contract and legitimate interest. The ban will take effect one week after the Irish DPA notifies Meta of the final measures. The EDPB acknowledges Meta's proposal to rely on a consent-based approach and notes that the Irish Data Protection Commission is currently evaluating this, along with Concerned Supervisory Authorities (CSAs).

You may find the news here.

On 3 October 2023, the United Kingdom's Information Commissioner's Office Issued New Guidance on Lawful Monitoring in the Workplace

The main purpose of the Information Commissioner's Offices ("ICO") guidelines is to offer clarity on regulatory certainty, safeguard workers' data protection rights, and foster trust between employers, employees, customers, and service users.

They cover monitoring activities on and off premises, during and outside of working hours, with a specific focus on remote workers who are likely to have a heightened expectation of privacy. The guidelines underscore that employers must adhere to the data protection principles of the UK General Data Protection Regulation ("UK GDPR") regardless of the monitoring technology employed. It emphasizes the importance of choosing the least intrusive methods to achieve monitoring objectives.

You may read the full Guidance here.

The ICO Has Published Detailed Guidance for Employers on Handling Workers' Health Data

The guidance aims to assist employers in understanding their data protection obligations under the UK GDPR and Data Protection Agreement 2018 when handling the health information of the employees. The guidance also provides greater regulatory certainty, protects workers' data protection rights, and helps employers to build trust with workers.

It commences by explaining the fair use of workers' health data and subsequently delves into specific topics, covering the handling of sickness and injury records, the utilization of occupational health programs, medical examinations, drugs and alcohol testing, genetic testing, and health monitoring. The guidance also addresses instances when workers' health information can be shared. Each section concludes with practical checklists, providing a convenient summary and reference point.

You may find the full guidance here.

The Spanish Data Protection Authority Published a Set of Guidelines on the Use of Biometric Systems for Access and Employee Attendance Control

On 23 November 2023, the Spanish Data Protection Authority ("AEPD") published a guide on the use of biometric data for presence and access control. The AEPD's guide on biometric data usage for access control emphasizes compliance with GDPR. It requires legal authorization for processing employment-related biometric data, cautioning against relying solely on consent due to power imbalances. The guide also restricts automated decisions affecting individuals and mandates a pre-processing Data Protection Impact Assessment to ensure suitability, necessity, and proportionality.

You may find the full guidance here in Spanish and further information here.

The French Data Protection Authority Confirmed the Compatibility of AI with the GDPR

On 12 October 2023, the French Data Protection Authority ("CNIL"), issued its first set of guidelines addressing compliance with the GDPR in the development of AI systems involving personal data. The primary objective of the guideline is to reassure the industry that the development of AI systems can align seamlessly with privacy considerations. Purpose limitation, data retention, data minimization and data reuse are the main aspects. The guidance provides practical insights into the application of core GDPR principles during the developmental stages of AI systems.

For more information please see here.

Financial Services Companies Fined £170,000 for Breaches in Direct Marketing

On 2 November 2023, 3 (three) financial services companies collectively faced fines amounting to £170,000 from the ICO for violating the Privacy and Electronic Communications Regulations through illegal direct marketing practices. The practices that form the basis of the fines can be briefly summarized as engaging in marketing activities without obtaining valid consent from data subjects.

You may find the news here.

Key Actions:

- ✓ Prior to marketing and promotional activities, data subjects must be informed and their consent must be obtained.
- ✓ Data subjects should be allowed to withdraw their consent at any time and electronic commercial messages should not be sent to persons who withdraw their consent.
- ✓ Consents obtained must be periodically reviewed and renewed.

UK Extension to the EU-US Data Privacy Framework Takes Effect

The UK Extension to the EU-U.S. Data Privacy Framework, commonly referred to as the UK-US Data Bridge, came into force on 12 October 2023. This extension facilitates the transfer of personal data from the United Kingdom ("UK") to the United States ("US") by eliminating the requirement for additional safeguards.

You may find more information here and further explanations at our previous bulletin here.

The White House Releases an Executive Order on AI

In the US, President Joe Biden issued an executive order on AI on 31 October 2023. As outlined in the White House fact sheet, the order focuses on establishing fresh standards for AI safety and security, safeguarding the privacy of American citizens, promoting equity and civil rights, advocating for consumers, patients, and students, supporting employees in the workplace, fostering innovation and competition, bolstering U.S. leadership internationally, and ensuring the responsible and effective utilization of AI by the government.

You may find the announcement here.

The CNIL Issues Ten New Penalties Utilizing Its Streamlined Protocol

In the recent series of 10 (ten) decisions rendered by CNIL under its updated sanction procedure, specific attention was given to 2 (two) key issues: geolocation tracking of employee vehicles and continuous video surveillance of employees.

Regarding geolocation, CNIL emphasized that the continuous recording of geolocation data, without providing employees the option to halt or suspend the system during breaks, constitutes an unjustifiable intrusion into employees' freedom of movement and right to privacy, unless there exists a compelling justification.

On the matter of continuous video surveillance of employees at their workstations, CNIL reiterated its stance. It clarified that permanent surveillance without a specific rationale infringes on employee privacy rights. While workplace safety

and evidence collection are legitimate reasons, they do not warrant perpetual video surveillance. In such cases, the personal data generated lacks appropriateness and relevance. The routine surveillance of employees, with limited exceptions, is deemed disproportionate to the intended objectives.

You may find the news here.

Key Actions:

- ✔ Surveillance of employees, whether through geolocation systems or CCTVs, should be limited in duration and even location, considering the purpose and legal basis of the surveillance. Employees should not be recorded routinely and uninterrupted unless there is special justification.

The California Privacy Protection Agency Unveils Initial Draft of Regulations for Opting Out and Accessing Automated Decision-Making

The California Privacy Protection Agency ("CPPA") has been actively advancing rulemaking for the California Consumer Privacy Act, focusing on cybersecurity audits, risk assessments, and automated decision-making. The latest development includes the release of a draft regulation on automated decision-making opt-out and access rights. On 8 December 2023, the CPPA voted 5-0 to advance a legislative proposal to require browser vendors to include a feature that permits users to exercise their privacy rights through opt-out preference signals.

The draft defines *"automated decision-making technology"* broadly, encompassing systems using machine learning, statistics, or AI for decision-making. It introduces opt-out rights for California residents, allowing them to refuse the use of automated decision-making technology for decisions with legal or significant effects, profiling during employment, and profiling in publicly accessible places. If the proposal is adopted, California would be a pioneer in requiring browser vendors to offer consumers the option to enable opt-out preference signals.

You may find more information here.

CJEU Decided that Credit Ranking Industry's Common Practice of Automatic Assignment of Credit Scores is Inconsistent with the GDPR

CJEU has issued 2 (two) key rulings against a German credit reference agency, which have implications for the credit ranking industry. Firstly, the CJEU confirmed that national courts can review data protection authorities, strengthening the rights of data subjects. Secondly, the argument presented by the agency, claiming that it merely provided assessments while the final loan decision was made by banks, was dismissed by the court. Instead, the court ruled that the agency's automated establishment of a probability score based on personal data, which assesses an individual's future payment capability, falls under the category of *'automated individual decision-making'* under Article 22 of the GDPR.

This challenges credit agencies' business models, emphasizing the need for transparency and consent in automated credit scoring and granting individuals more rights to dispute credit scores. These rulings also have broader implications, clarifying that the GDPR complaints from data subjects are crucial mechanisms for safeguarding individuals' rights. Overall, the CJEU has significantly enhanced data subjects' rights, highlighting transparency, consent, and the ability to challenge decisions in the realm of data protection.

You may read the decisions here and here.

The CJEU Decided That Only a Wrongful Infringement of the GDPR May Result in an Administrative Fine Being Imposed

CJEU has made a groundbreaking decision simplifying the process of imposing administrative fines for GDPR violations. This decision clarifies the circumstances under which national supervisory authorities may impose an administrative fine on 1 (one) or more controllers for breaching the GDPR. Specifically, it stipulates that imposing such a fine necessitates evidence of wrongful conduct,

implying that the infringement was committed either intentionally or negligently. Additionally, if the recipient of the fine is part of a corporate group, the fine calculation must be based on the turnover of the entire group.

This landmark decision is anticipated to strengthen GDPR enforcement, facilitating Member States' data protection authorities in imposing fines and potentially resulting in higher fines based on company turnover in the future.

You may read the decision here.

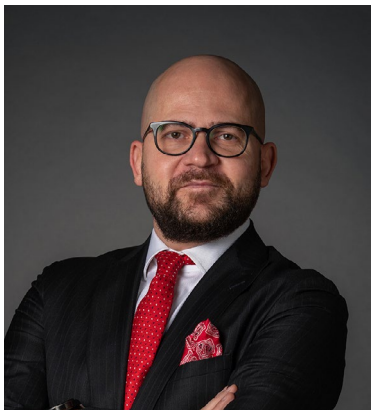
On 12 December 2023, The EDPB Has Adopted a Report on Effective Application of the GDPR

During its recent plenary session, the EDPB presented a report to the European Commission on the effective application of the GDPR. While acknowledging the success of the GDPR in its initial 5.5 years, the EDPB deems it premature to revise the GDPR, despite anticipating significant challenges ahead. Instead, it urges swift adoption of a new regulation by co-legislators, outlining additional procedural rules for cross-border enforcement of the GDPR.

Additionally, the EDPB underscores the importance of providing adequate resources for data protection authorities and the EDPB to fulfill their responsibilities.

You may read the report here.

Key Contacts



Mert Karamustafaoğlu
Partner, Competition and Compliance Leader

mertkaramustafaoglu@erdem-erdem.av.tr

Sevgi Ünsal Özden
Managing Associate

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