ERDEM & ERDEM

Personal Data Protection Bulletin

2023
Second Quarter

Sevgi Ünsal Özden
Gülnur Çakmak
Defne Pırıldar
Melis Uslu

Recent Updates from Türkiye

Principles and Procedures on Social Network Providers

The decision dated 28/03/2023 and numbered 2023/DK-ID/119 on the Procedures and Principles on Social Network Providers prepared by the Information Technologies and Communications Authority, determining the obligations of social network providers such as determining representatives, responding to applications, hosting data, and the procedures and principles regarding the application of these obligations was published in the Official Gazette on 01.04.2023 and entered into force on the date of publication.

You may find the text of the decision here.

The Personal Data Protection Board Decision Summaries

The Personal Data Protection Board ("Board") published 40 new decision summaries on 24.04.2023. We have compiled the highlights for you.

- **The Board Decision regarding a cargo package containing personal data being delivered to a third party:**

  The cargo sent by a branch of an electronic retail chain in a shopping centre (data controller) to the distributor that contains the data subject's personal data was delivered to a third party due to incorrect delivery by the cargo company. The Board evaluates that there is no violation by the data controller since the data controller provided the cargo in a manner to be delivered to the correct recipient. In addition, it has been evaluated that the cargo company, which cannot be expected to have control over the cargo content, does not bear the titles of data controller or data processor in terms of cargo content. However, the Board drew attention to the fact that minimum personal data should be shared in the forms inside the cargo packages and that the personal data shared should be masked as much as possible.

  In the decision, it is also emphasised that in the event that the personal data of the data subject is unlawfully obtained by a third party due to the cargo company's incorrect cargo delivery, the data controller's obligation to notify the data subject and the Board pursuant to Art. 12/5 of the PDPL ("Personal Data Protection Law") continues

You may find the summary of the Boards decision here.

Key Actions:

- ✓ Documents containing as little and/or masked personal data as possible should be shared in shipments made through cargo companies.
- ✓ In the event that personal data is obtained unlawfully by a third party independent of the subject, the data controller has a notification obligation to notify both the data subject and the Board pursuant to Article 12/5 of the PDPL.

- **The Board Decision on sending a notice containing personal data of multiple recipients to other employees by the data controller providing payroll services:**

  In the case subject to the decision, the identity and communication data of more than one employees were included in the same notice, and the said notice was sent to all recipients through a notary public. Thus, since the personal data of eight different employees were collectively included in the same notice, the personal data of each of them were shared with each other. The Board evaluated the sharing of the identity and communication data of the employees in question through a notary public by including them in the notice within the scope of the processing requirement stipulated in Article 5/2 of the PDPL that ”data processing being mandatory for the establishment, exercise or protection of a right”.

  On the other hand, the fact that the personal data of the employees are collectively included in the same notice, and that no action such as darkening the notice or separate notification to the recipients is not based on any data processing requirement. Based on these assessments, the Board decided to impose an administrative fine of TRY 100.000 on the data controller.

You may find the summary of the Boards decision here.

Key Actions:

- ✔ Notifications to be sent to more than one recipient should be sent separately or measures such as darkening etc. should be applied when sending notifications containing the information of more than one recipient

- **The Board Decision on posting photographs taken during surgery on the social media account of a doctor working at the hospital:**

  In the case subject to the decision, during a nose surgery performed in a private hospital, photographs were taken of the data subject while they were unconscious without their consent and shared on the social media account of the doctor who performed the surgery. It was claimed that advertising and marketing activites

were carried ot by sharing the photographs in question on the hospital's social media account for approximately two years.

The Board evaluated that although the eyes of the data subject were covered, the image in question renders the data subject identifiable since other features, such as eyebrows and mustache, that can identify the data subject were not anonymized and considered the photographs as personal data.

The data subject has given explicit consent to the hospital that carried out the treatment for the use of the images, but the images were shared by a doctor working in the hospital. The Board concluded that the hospital did not take sufficient technical and administrative measures to prevent unlawful access to personal data. The Board also pointed out that the relevant provisions of the Turkish Criminal Code may be applied against the doctor for sharing without consent.

You may find the summary of the Boards decision here.

Key Actions:

- ✓ When sharing visual data of natural persons, the parts that can identify the data subject should be anonymized.
- ✓ The consent given by people is only valid for the relevant data controller.

- **The Board Decision on disclosing information regarding a job interview and various information about the content of the interview by the potential employer with the current employer of the employee candidate**

  In the decision, the statements of his current workplace of a person who was employed by one company and had a job interview with another company were shared with the current workplace.

  The Board stated that the data controller processed the data subject's information in his CV as per Article 5 of the PDPL on the grounds that *"It is necessary to process personal data belonging to the parties to the contract, provided that it is directly related to the establishment or performance of a contract"* and *"It is mandatory to process data for the legitimate interests of the data controller, provided that it does not harm the fundamental rights and freedoms of the data subject"*. Subsequently, it is stated that the employer has the right to process data in order to determine the suitability of employee candidates, within the scope of the interests required by the job and the employer's management right prior to the establishment of the employment contract, in connection with the purpose of the job interview, in a limited and measured manner.

  On the other hand, it has been evaluated that the data controller unlawfully transferred information on the job interview of the employee candidateand his statements about his current workplace during the job interview to the company where the data subject worked at the time.

You may find the Boards decision summary here.

Key Actions:

- ✓ Personal data of the employee candidate obtained by the potential employer during job interviews and the details of the interview cannot be transferred to the current employer without the transfer conditions stipulated in the PDPL being present.

- **The Board Decision regarding the sending of personal data of a member by a legal betting platform to a third party's e-mail address:**

  The legal betting platform sent two e-mails to the e-mail address of a person who is not even a member of the platform, including the name-surname and membership number of another member. The Board found that the fact that the data controller did not establish any control mechanism during the personal data processing activity (sending e-mails) violated the general principles of *"being in compliance with the law and good faith"*, *"being accurate and up-to-date when necessary"* and "being relevant, limited and proportionate to the purpose for which they are processed" stipulated in the PDPL. In fact, the data controller has assessed that the betting platform has not designed the electronic systems of the betting platform in accordance with these basic principles. In response to the betting platform's defence that *"mobile number is used as the main communication channel, therefore e-mail verification is not performed during the membership application"*, the court drew attention to the principle of data minimisation and pointed out that e-mail data that is not used as the main communication channel should not be obtained at all.

  The Board determinedthat the e-mail address of theperson who is not a member, and name-surname and membership number of the applicant were processed without relying on a condition for personal data processing; and stated that the data controller did not take active steps to comply with the principle of being accurate and, where necessary, up-to-date while processing data. The Board imposed an administrative fine of TRY 250,000 on the platform.

You may find the summary of the decision here.

Key Actions:

- ✓ The data controllers should create appropriate mechanisms to verify that the information is accurate and up-to-date before reaching out to data subjects using the contact information provided during membership.
- ✓ If only one of the communication channels is sufficient for the intended purpose, no additional personal data should be obtained in excess of the purpose.

- **The Board Desicion regarding the Customer services of a bank calling the data subject by phone without fulfilling the obligation to inform and without obtaining their consent:**

  In the complaint received by the Authority, it was reported that following the transfer of money from the account of the data subject at another bank to an account belonging to a third party at the data controller bank, the data controller bank made a telephone call for promotional purposes without informing the data subject and without obtaining their explicit consent. The complainant stated that they applied to the data controller bank in this regard, but the bank did not respond. The data controller bank, on the other hand, stated that the postal and e-mail addresses in the application petition are different from the addresses in the bank records, the official signature samples in the bank records and the signatures in the application petition do not match, the bank's reply was sent by ordinary mail to the customer's address registered in the system and therefore it could not be confirmed whether the reply reached the customer.

  The Board assessed that sending letters by "ordinary mail" creates a security gap within the scope of Article 11 of the PDPL since there is a risk for third parties receiving the mail which contains personal information.

  In addition, the Board determined that the data subject has been a customer of the bank since 2015, which is before the effective date of the PDPL, and even has a communication consent, and stated that the consent obtained in accordance with the existing legal rules before the publication of the PDPL are valid unless the relevant persons declare a contrary will within one year.

You may find the Boards decision summary here.

Key Actions:

- ✓ The applications made by the data subject should not be responded to by ordinary mail.
- ✓ Explicit consents obtained before the effective date of the PDPL and not withdrawn within one year from the effective date are valid.

- **The Board Decision on the continued processing of personal data by the former employer:**

  In the case subject to the decision, the image of an interior designer working in the furniture and decoration sector in live broadcasts on social media was used for advertising and marketing purposes on TV screens, websites and printed materials for promotion even after the termination of the employment contract. The Board found it lawful to keep the images of the data subject in the archives of the data controller. However, it was stated that there would not be a valid processing condition within the scope of the PDPL regarding the use of the images of the former employee for advertising and marketing purposes after the termination of the employment contract. As a result, it was decided to impose an administrative fine of TRY 250,000.

  You may find the summary of the Board Decision here.

Key Actions:

- ✔ Images of employees whose employment relationship has ended should not be used on the website and/or social media accounts, promotional printed materials.

- **The Board Decision on the request to remove from the index the results of a search made by name and surname in the search engine regarding an announcement accessible on the website of the Official Gazette:**

  In the concrete case, it was stated that the page *https://www.resmigazete.gov.tr/arsiv/*****.pdf* was reached when a search was made through the data controller search engine with the name of the data subject, and it was requested that the page that appeared as a result of the search be removed within the scope of the *"right to be forgotten"*. In its assessment of the complaint, the Board concluded that there is no public interest, noting that the purpose of the announcement in the Official Gazette is to notify the person. In addition, more than 20 years have passed since the aforementioned announcement and therefore the content is outdated. Although the information contained in the content confirms that the person concerned was acquitted of the offence charged against him, it is of a nature that may cause prejudice against the person concerned. The relevant content was not published by the person concerned and could not be considered within the scope of journalistic activity.

  In its assessment, the Board refers to the *Costeja Gonzales/La Vanguardia* decision by the Spanish Data Protection Authority. In the relevant decision, it is stated that it is mandatory to publish announcements under national legislation and that it is in the interest of the data controller to have many people access this information. It rejected the complaint against the newspaper and ordered Google to remove the relevant links. The case was referred to the Court of Justice of the EU ("CJEU"):

  → If the results of a search on a search engine are *"invalid, incomplete, completely irrelevant or subsequently rendered irrelevant"*, the search engines must delete the personal data in question and the information contained in the list of results for exceeding the purpose for which they were uploaded on the internet;

  → The right to privacy of an individual is above the economic interest of the search engine and the public's right to access to information. This rule does not apply only if the public has an overriding interest in knowing the information.

  The Board refers also to Article 17 of the General Data Protection Regulation numbered 2016/679 ("GDPR"). Accordingly, the right to be forgotten is considered within the scope of the obligation to erase.

→ You may find the Board's Decision summary here.

- **The Board Decision on processing blood type databy the data controller gym operator, without explicit consent of the data subject**

  In the case subject to the decision, it is claimed that the data controller, which is the operator of a gym, processes the health data (detailed fat, weight and performance measurement, blood group, number of annual hospital visits, smoked cigarettes, etc.), biometric data (fingerprint taken at the entrance to the gym) and camera images of its members, but does not provide clarification and obtain consent regarding these data. The noteworthy point in the Board's assessment is that the disclosure and explicit consent texts should not be included in the contract content provided to the members, but should be organised separately and the explicit consent should be presented in a way to include the options to give or withhold consent for each data processing activity.

  Anotheroutstanding evaluation in the said decision is regarding commercial text messages. The Board evaluated that in addition to the statement in the contract *"I allow SMS marketing activities"*, cannot be deemed as explicit consent but is only a statement limited to the processing of the personal data of the data subject within the scope of marketing activities. Moreover, the Board stated that the option *"I do not allow SMS marketing activities"* should also be provided in the contract to ensure that the preferences of the data subject are reflected in the text.

You may find the Boards decision summary here.

Key Actions:

- ✓ When obtaining explicit consent for electronic commercial messages, persons should be given two separate options as **"I give consent"** and **"I do not give consent".**
- ✓ Contracts, disclosure texts and consent declarations should not be intertwined; disclosure and explicit consent processes should be separated from the content of the contract.

- **The Board Decision on processing personal data by monitoring, accessing and storing the content of the corporate e-mail address allocated by the data controller to its employees:**

  The complaint states that the data subject's employment contract was terminated by the data controller. The reason for termination is that internal data was sent to his personal e-mail address via the corporate e-mail address and the phone call with another employee of the company was secretly recorded and sent to his personal e-mail address and his lawyer's e-mail address.

  The Board evaluated the personal data processing activity carried out through e-mail control within the scope of the processing conditions that *"data processing is mandatory for the establishment, exercise or protection of a right"* and *"data processing is mandatory for the legitimate interests of the data controller, provided that it does not harm the fundamental rights and freedoms of the data subject"*.

  Regarding the surveillance of communication, a distinction must be made between the surveillance of the flow of communication and the content of communication. Surveillance of the content of communication is subject to stricter conditions. When supervising the content, to the extent appropriate to achieve the employer's objective, the content of the communication should be supervised primarily for detecting circumstances that may constitute a breach of security, loyalty, and use contrary to the interests of the employer, before supervising the content of the communication.

  The periods of 6 days and 1 year stipulated under the Labor Law to exercise the right of immediate termination are related to the exercise of the right of termination. It is not important for the retention of personal data.

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

Key Actions:

- ✔ Employees' communication content should not be monitored unless a breach of security, loyalty, and use is detected, which would be contrary to the employer's interest.
- ✔ The obligation to inform must be fulfilled during the surveillance of communication.

Recent Developments from the World

The United States of America (“USA”) and United Kingdom (“UK”) agreed a commitment in principle for a UK/US “Data Bridge”, the announcement was made on 08.06.2023 by the UK

The commitment reached by two countries will create a data bridge between them to facilitate personal data flows. The understanding of the parties is likely to create a support mechanism for the EU-US Data Privacy Framework. Meanwhile, the European Commission is working on an adequacy decision under GDPR in relation to the EU-US Data Privacy Framework. This announcement aligns the UK and the EU standpoints as regards the data transfers.

You may find the announcement here.

The Office of the Privacy Commissioner of Canada (“OPC”) has released new guidance for employers subject to privacy regulation

The guidance published by the OPC is intended to provide awareness and support to employers subject to privacy regulations, in particular the Privacy Act, regarding their confidentiality obligations. It covers topics such as respect for employee privacy, competing interests of employee and employer, employee monitoring, and controlling employee communication as well as practical recommendations.

You may find the guidance here.

Singapore is appointed as the deputy chair of the Global Cross-Border Privacy Rules (“CBPR”) Forum’s policymaking body Global Forum Parlement on April 13, 2023

Singapore, one of the co-founders is appointed as the deputy chair of the CBPR Forum’s policymaking body, the Global Forum Assembly. The Forum offers an international certification system with respect to the APEC Cross Border Privacy Rules and Privacy Recognition for Processors Systems which already facilitate free flow of data and data protection. The forum is also accepting other jurisdictions which are interested in participating.

You may read more about the appointment here.

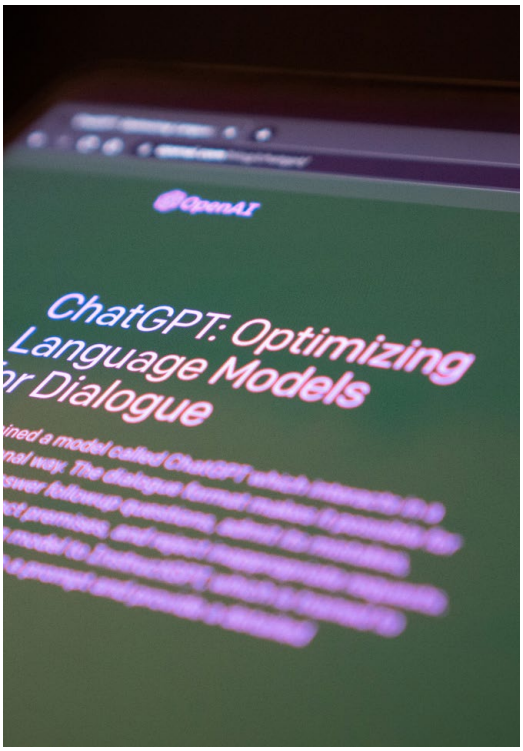
UK applied to the CBPR Forum on April 17, 2023

The UK applied to join the CBPR Forum as an associate, and became first country who applied to the forum that was established in 2022.

You may read more about the application here.

ChatGPT service is blocked in Italy until further notice

The Italian Data Protection Authority announced the immediate temporary limitation on the processing of Italian users’ data by OpenAI on 31.03.2023. This limitation by the authority resulted with the blocking of the services by ChatGPT on the grounds that OpenAI does not adequately inform data subjects on data processing activities. With this decision, Italy became the first country to block this service, and the authority.



You may read more about the announcement here.

The European Court of Justice ("CJEU") rules that the live streaming of classes falls within the scope of the GDPR.

On 30.03.2023, the CJEU announced a preliminary ruling as response to a request by the Administrative Court of Wiesbaden, Germany ("Court"). The request concerns the lawfulness of live streaming service for classes that students couldn't attend during Covid-19 without explicit consents of teachers lecturing during these classes.

During Covid-19 pandemic, the Minister for Education and Culture of the Land Hessen ruled that the students themselves or for younger students, their parents should consent, on the contrary, the consent of teachers involved was not addressed. An action before the Court was brought to object to live streaming of classes by videoconference without obtaining the consent of the teachers concerned.

The CJEU concluded that member states' authority to adopt specific rules under Article 88 of the GDPR is discretionary, and a Member State may adopt such rules with the objective to protect employees' rights and freedoms. The CJEU also addresses the concerns whether if a national rule not meeting the requirements under Article 88/2 of the GDPR can remain applicable, and states that where the Court finds incompliance with national provisions on the processing of personal data and the conditions under Article 88 of the GDPR, it shall verify whether those provisions constitute a legal basis under Article 6/3 of the GDPR.

You may read more about the decision here.

Key Actions:

- ✓ Employers should apply and consider the GDPR rules when it comes to "classic" data processing in the employment relationship.

The European Data Protection Board ("EDPB"), updates data subject access guidance

On 17.04.2023, the EDPB, the body tasked with ensuring the consistent application of data protection law across the EU, announced that it had adopted a finalised version of its data subject access request (DSAR) guidance. The updated guidance includes clarifications on a data controller's DSAR responsibilities; when data controllers may refuse a DSAR; and the interplay between DSARs and data retention periods.

You may find the relevant announcement here.

The EDPB published the Guidelines numbered 9/2022 on personal data breach notifications under the GDPR

The guidelines were published on 28.03.2023 and aim to update the guidelines on personal data breach notification under the GDPR. From now on, the guidelines numbered 9/2022 will be taken as a reference for breach notifications under the GDPR. The guidelines emphasize that there was a need for clarification regarding data breaches at non-EU establishments, and specific improvements were made in this regard.

You may find the guidelines here.

The EDPB published the Guidelines numbered 4/2022 on the calculation of administratice fines under the GDPR

The guidelines were published on 24.05.2023 to harmonise the method to be used by tthe supervisory authorities for calculating of the amount of the fine under tthe GDPR. This guidelines is adopted as a complementary document for prior guidelines on the application and setting of administrative fines.

You may find the guidelines here. On the other hand, the final document was accepted on 07.07.2023. You can reach the related announcement here.

On 26 April 2023, the European General Court (“EGC”)published its judgment for the Case T-557/20, Single Resolution Board (SRB) v European Data Protection Supervisor (EDPS), in relation to the threshold between pseudonymous and anonymous data.

On 26.04.2023, the EGC overturned the SRB’s decision dated 24.11.2020, which found that the SRB had breached its transparency obligation and qualified the sharing of personal data, even under a pseudonym, as personal data sharing. In its judgment, the EGC held that pseudonymised data will not be considered personal data if the recipient of the data does not itself have the means to re-identify the data subjects. It has been clarified that an individual’s views and opinions alone are not personal data and a case-based assessment is also required. Accordingly, it concluded that in order to determine whether an individual’s views and opinions constitute personal data, it is necessary to examine *“whether an opinion is connected to a particular person by content, purpose or effect”*. The fact that disclosing party has the means to re-identify individuals does not necessarily mean that data will be automatically deemed to be personal data.

You may find the decision here.

The CJEU delivered an outstanding decision on a person's right to obtain a copy of their personal data under Article 15 of the GDPR

With its decision dated 04.05.2023 (Case C-487/21 F.F. v Österreichische Datenschutzbehörde), the CJEU provided important clarifications regarding Article 15 of the GDPR *(Right of access by the data subject)*. The Court notes that the right of access entitles the data subject to obtain an authentic copy of personal data processed by a data controller. It is emphasized that the term "copy" generally does not refer to a copy of an actual document, but only to the personal data being processed. In some cases, this may include the right to receive copies of extracts of documents or even entire documents or databases containing personal data, if this is necessary for the data subject to effectively exercise their rights under the GDPR.

You may read more about the decision here.

The CJEU decides that a mere infringement of the GDPR is not sufficient for non-material compensation

With its decision dated 04.05.2023 (Case C-300/21 UI v Österreichische Post AG), the court addresses non-material damages under Article 82 of the GDPR *(Right to compensation and liability)*. In the case subject to the decision, the data subject, who claimed that he was offended as a result of the processing of his personal data for political advertising purposes, requested compensation for his non-material damage. The court establishes that three conditions must be met for compensation, (i) an infringement of the GDPR; (ii) material or non-material damage resulting from that infringement; and (iii) a causal link between the infringement and the damage. Moreover, it is stated that there is no threshold of seriousness with respect to the right to compensation, and each Member State should set out its rules for safeguarding the rights under the GDPR.

You may find the decision of the CJEU here.
You may read our article about the decision here.

The Irish Data Protection Authority (Ireland DPA) announced its decision dated 12.05.2023 on Meta Platforms Ireland Limited (Meta Ireland) on 22.05.2023

Pursuant to the decision, an administrative fine of 1.200.000.000 Euros was imposed on Meta Ireland, which is another record fine in the history of the GDPR Following the decision of CJEU in *"Data Protection Commissioner v Facebook Ireland Limited v Maximillian Schrems"*, the DPA found that transfers made by Meta Ireland from the European Union and the European Economic Area to the United States infringed Article 46/1 of the GDPR. The DPA concluded that, although data transfers subject to the Decision were carried out on the basis of the updated Standard Contractual Clauses (SCCs) adopted by the European Commission in 2021 and on the basis of additional measures implemented by Meta Ireland, there is no sufficient protection regarding fundamental rights and freedoms.

You may access the full text of the press release regarding the decision here.
You may read our client alert here.

The Ireland DPA published a guidance note on data protection in the workplace for employers.

The said guidance has been prepared to provide clarifications for employers as data controllers covering their data processing obligations and duties for former, current and future employees. It is obvious that the guide, which includes detailed explanations on which data will be accepted as personal data, the basic principles governing data processing, legal grounds, highly sensitive employer practices such as CCTV, communication and computer monitoring, vehicle tracking systems and the rights of employees, will be an important guide in the employee-employer relationship.

You may find the guidance by the Ireland DPA here.

The CJEU issued an important decision on the obligation of data controller banks to provide information

On 22.06.2023, the CJEU ruled that banks are obliged to provide information on request on when and why data of data subjects was accessed. On the other hand, it considered that banks are not obliged to provide the names of the persons who accessed the data. While the CJEU stated that the right of access to information under the GDPR provides the right to obtain information as to why and when the data was accessed, it does not provide the right to know who accessed the data *(unless such information is necessary to enable the data subject to effectively exercise the rights granted to them*).

You can access the above-mentioned decision here.

Key Contacts

Mert Karamustafaoğlu
Partner, Competition and Compliance Leader

mertkaramustafaoglu@erdem-erdem.av.tr

Sevgi Ünsal Özden
Managing Associate

sevgiunsal@erdem-erdem.com

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

www.erdem-erdem.av.tr