ERDEM & ERDEM

Personal Data Protection Bulletin

2023
First Quarter

Sevgi Ünsal Özden
Gülnur Çakmak
Defne Pırıldar
Melis Uslu

Recent Updates from Türkiye

On 23.02.2023, The Turkish Personal Data Protection Authority ("Authority") Published A Public Announcement on Personal Data Processed by Political Parties and Independent Candidates Within the Scope of Election Activities and A Memorandum on the Said Activities

The key points of the public announcement are summarized as follows:

- Within the framework of the legislation they are subject to, political parties carry out many activities such as establishment, membership, nomination of candidates, election of their authorized bodies, and for these reasons, they are accepted as data controllers for the personal data they process.

- Pursuant to the provisions of the relevant legislation, including the Constitution of the Republic of Turkey, the Law No. 2820 on Political Parties, the Law No. 298 on the Main Principles of Elections and Voter Registers ("Law No. 298"), the Law No. 2839 on Parliamentary Elections, the Law No. 2972 on the Election of Local Administrations and Neighborhood Headman Offices and Board of Elderman and the Law No. 6271 on Presidential Elections, it is possible to carry out personal data processing activities that cause the processing of political opinion of the real persons, which qualify as sensitive personal data, without the explicit consent of data subject in accordance with Article 6/3 of the Personal Data Protection Law ("PDPL").

- Pursuant to Article 55/B of Law No. 298, political parties may process communication data without explicit consent in order to send audio, video or written messages to their members. However, pursuant to the aforementioned article, propaganda by sending audio, video or written messages to citizens is prohibited and the processing of their personal data for these purposes is prevented.

- Since the Law No. 298 and the decisions taken by the Supreme Electoral Board state that propaganda cannot be made by sending messages to individuals, it is considered that there is no legal basis for independent candidates to become data controllers by processing the contact information of individuals.

- Political parties are required to comply with the data processing conditions regulated under Articles 5 and 6 of the PDPL in their personal data processing activities; to fulfill their obligation to inform; and to ensure data security. On the other hand, since political parties are exempted from the obligation to register with VERBIS, political parties are not obliged to register with VERBIS.

You can access the memorandum here.

The Administrative Fines Regulated Under Article 18 of the PDPL Have Been Recalculated. The Updated Amounts Were Announced by The Authority on 17.01.2023

Article	Violated Article	Explanations	Fines for 2022		Fines for 2023 (Increase rate: 122,93%)	
			Min	Max	Min	Max
18/a	10	Failure to fulfill the obligation to inform	13.391	267.883	29.852	597.191
18/b	12	Failure to fulfill obligations regarding data security	40.179	2.678.863	89.571	5.971.989
18/c	15	Failure to implement board decisions	66.965	2.678.863	149.285	5.971.989
18/ç	16	Violation of the obligation to register with the Registry of Data Controllers and the notification obligation	53.572	2.678.863	119.428	5.971.989

You can access the announcement here.

The Personal Data Protection Board's ("Board") Decision Numbered 2023/134 on Tiktok Pte. Ltd., Was Published on The Website of the Authority

As per the decision concerned, the Board decided to impose an administrative fine of TRY 1,750,000 on the grounds that the data controller company did not take the necessary technical and administrative measures to ensure the appropriate level of security.

The main assessments of the Board are as follows;

- Displaying personal information of users under the age of 13 before the update of the Company's privacy policy in January 2021 and collecting data regarding users under the age of 13 without parental consent has an adverse risk for children,

- In the confidentiality agreement on the website of the data controller, all of legal grounds stipulated under Article 5 of the PDPL are stated, but no clear information is provided about which personal data are processed for which purposes and based on which legal ground, and thus the principles of "processing for specified, explicit and legitimate purposes" and "being relevant, limited and proportionate to the purpose of processing" are violated,

- For those who want to create a user account, when obtaining approval, the relevant text was not translated into Turkish, accordingly, there is a risk that the terms of use may be accepted by users without being fully understood,

- Explicit consent was not obtained during the creation or active use of the account, the company used the privacy policy as both clarification text and explicit consent text to fulfill the disclosure obligation and to replace the explicit consent text, and the obligation to fulfill the explicit consent separately from the disclosure obligation is not fulfilled,

- The Company uses cookies but does not obtain explicit consent for them.

You may access the summary of the Board's decision **here**.

Key Actions:

- It should be checked whether there is parental consent for the processing of personal data of data subjects under the age of 13.
- The clarification obligation must be fulfilled in a manner that data subjects can easily understand.
- The clarification texts and explicit consent texts must be submitted separately to the data subjects.
- Which personal data are used for which purposes should be clearly stated in the clarification texts.
- Privacy policies, clarification texts and explicit consent texts available on websites should be reviewed.

Recent Developments from the World

The European Data Protection Board Issued Its Opinion on the EU-U.S. Data Privacy Framework

On 13 December 2022, the European Commission ("Commission") had released a draft adequacy decision ("Decision") for the EU-U.S. data protection framework ("DPF"). On February 14, 2023, The European Parliament Committee on Civil Liberties, Justice and Home Affairs opposed to the Decision in its draft motion stating that the DPF fails to create actual equivalence in the level of protection and urged the Commission not to adopt the decision. On 28 February 2023, European Data Protection Board ("EDPB") issued its nonbinding opinion on the Decision.

In its opinion, the EDPB stated that the proposed DPF includes substantial improvements and that a number of aspects need to be clarified, developed, or further detailed. The EDPB assessed that *"the specific purposes for which collection can and cannot take place, may be updated with additional purposes in the light of new national security imperatives", and criticized that "the collection of bulk data, lacks the requirement of prior authorization by an independent authority"*. The opinion of the EDPB is non-binding yet it is considered to have a direct impact on the assessment of the DPF by the representatives of the Member States and the European Parliament.

You may find the Decision here, the draft motion here and the opinion here.

On February 1, 2023, the Commission Published Questions and Answers on Identification and Counting of Active Recipients of the Service Under the Digital Services Act ("DSA")

The Commission has issued guidance to answer the questions received on the obligation to publish information, especially on active recipients of services, stipulated under DSA. The guidance aims to answer questions related to the obligation to publish information on the number of average monthly active recipients of the service for intermediary service providers. With the Guidance, it has been clarified that the service providers may fulfill their obligation by publishing the relevant information on their online interfaces and that the DSA does not require to notify the Commission or the competent Digital Service Coordinator, or any other competent national authority. However, for the initial period of the DSA, intermediary service providers are encouraged to communicate relevant information to the Commission's e-mail address. You may find the guidance here.

The Report Prepared by the Cookie Banner Taskforce is Published

EDPB had formed the Cookie Banner Taskforce in September 2021 in order to evaluate common complaints about cookies. The taskforce prepared and published a report on January 17, 2023 which reflects on the conclusions of the Taskforce in charge of coordinating the answers of European Union data protection authorities to the complaints filed by a non-governmental organization, None of Your Business. The report can be considered to be a kind of good practice guide on cookie banners, providing clear examples of correct and incorrect cookie banners, and therefore a providing guidance for website owners. For example, the report clearly states that the *"reject all"* button should be used or that pre-ticked boxes are not an appropriate method.

You may find the Report here.

Key Actions:

- ✔ All businesses and organizations with a website or application that uses cookies should review their compliance with the EDPB's good practice guidance on the design and features of cookie banners if they provide goods and services to natural persons resident in the European Union.

The Network and Information Security Directive 2.0 Entered into Force

On January 16, 2023, the Directive (EU) 2022/2555 ("NIS-2 Directive") entered into force and replaced the previous NIS Directive of 2016, aiming to strengthen the level of cyber resilience and the resilience of critical national infrastructures and to envision an integrated regime for cybersecurity risk management in the European Union. The NIS-2 Directive expanded the scope of the cybersecurity rules to new sectors and entities. Within this context, the scope of NIS-2 Directive is subject to different supervisory regimes divided into two categories: sectors of high criticality and other critical sectors. Energy, transport, banking, financial market infrastructure, health, drinking water, wastewater, digital infrastructure, ICT service management and public administration are considered as sectors of high criticality. The Directive was published in the Official Journal of the European Union on December 27, 2022 and entered into force on January 17, 2023. Member States have 21 months to transpose the Directive into their national legislation.

You may find the NIS-2 Directive here.

Key Actions:

- ✔ Businesses subject to the NIS-2 Directive and their suppliers should consider developing compliance programs in preparation for member states transposing the directive into national law.

The Commission Gathers Feedbacks in Order to Improve the Enforcement of the Regulation (EU) 2016/679 General Data Protection Regulation ("GDPR")

The Commission started to receive feedbacks regarding a new system for monitoring the GDPR enforcement by national data protection authorities, underlining that there are many divergences in approaches followed by the national data protection supervisory authorities on issues such as complaint handling, form of complaints, duration of proceedings and that these procedural differences affects the rights of data subjects.

You may read more about the Commission's work here.

The Belgian Constitutional Court Has Found the Lack of the Right to Appeal for Third Parties Against Decisions of the Data Protection Authorities as Unconstitutional

On January 12, 2023, the Belgian Constitutional Court rendered a decision that the Article 108 § 1 of the Law Establishing the Data Protection Authority violates the Belgium Constitution as it does not allow interested third parties to appeal decisions of the data protection authorities. The Belgian Constitutional Court defines third parties as persons who are not party to the proceedings before the data protection authorities and who are therefore not the addressee of the decisions, but who suffer adverse consequences as a result of the data protection authorities' decisions and who have an interest in having them set aside.

You may find the Belgian Constitutional Court's decision here *(in French)*.

The EDPB Published Report on the Use of Cloud Services by the Public Sector

On January 17, 2023, the EDPB has published a report on the use of cloud services by the public sector. Underlining sensitive nature and large amounts of data processed by public bodies, the EDBP recommended that public bodies, when using cloud-services, should (i) carry out an impact assessment, (ii) precisely define the roles of the involved parties in a contract, (iii) control whether the cloud service providers ("CSP") are following the instructions given to them, (iv) have control over the use of data subprocessors, (v) promote the involvement of a data protection officer, (vi) and cooperate with other public bodies when negotiating with the CSPs.

You may find the Report here.

Key Actions:

- ✔ Compliance with personal data protection legislation should be prioritized at all stages of cloud service implementation, and public institutions and cloud service providers should allocate the necessary resources and time to identify and analyze compliance issues that may arise before they start working.

Following the EDPB's Binding Decisions, Irish Data Protection Authority ("IE DPA") Rendered Decisions Regarding Facebook and Instagram

Following the EDPB's binding dispute resolution decisions, the IE DPA had finally adopted its decisions regarding Facebook and Instagram. These decisions are the result of complaint-based inquiries into Facebook's and Instagram's activities in particular concerning the lawfulness and transparency of processing for behavioral advertising. The EDPB, in its binding

decisions, had stated that behavioral advertising is not a core element of services provided by Meta Ireland and therefore had found unlawful for Meta Ireland to refer to the contract as the legal basis for processing personal data for behavioral advertising purposes as this was not a core element of the services. As a consequence, the EDPB instructed the IE DPA to amend its draft decisions.

The IE DPA accepted the majority of the EDPB's findings and fined Meta Ireland €210 million under the Facebook decision and €180 million under the Instagram decision. Meta Ireland has also been directed to bring its data processing operations into compliance with GDPR within a period of three months. You may find our announcement on EDPB's binding decisions in Personal Data Protection Bulletin - 2022 Fourth Quarter and the EDPB's press release here.

European Parliament Clarifies Its Stance on The Data Act

The European Parliament's Committee on Industry, Research and Energy voted in favor of the proposal for a regulation of the European Parliament and of the Council on harmonized rules on fair access to and use of data (Data Act Proposal) and publish a report ("Report") on the proposal. The proposal aims to promote a competitive data market, open up opportunities for data-driven innovation and make data more accessible. The main regulations of the Data Act Proposal could be briefly stated as regulations and obligations regarding B2B and B2C data sharing, access to data related to the Internet of Things, government access to data, data transfer and access restrictions to nonpersonal data, smart contract requirements and contractual relationships between data holders and data recipients, especially concerning the position of small and medium enterprises. The Report points out that Europe has a large amount of industrial data, but that its potential has not yet been sufficiently exploited. The Report also states that the proposal could be the key to economic growth if it can create a data resilient ecosystem that provides easy access to industrial data.

You may find the Report here.

Read our related Newsletter Article:
"Briefing for the Impact Assessment of the Data Act Has Been Published"
Sevgi Ünsal Özden / July 2022

On February 24, 2023, The EDPB Adopted Several Guidelines:

Guidelines on the interplay between the application of Article 3 and the provisions on international transfers as per Chapter V of the GDPR (05/2021)

With respect to data transfers abroad, the Guideline numbered 05/2021 sets out criteria to qualify a processing operation a processing operation as a transfer of personal data to a third country or to an international organization, consequences of data transfer and safeguards to be provided.

Guidelines on deceptive design patterns in social media platform interfaces: how to recognize and avoid them (03/2022)

Deceptive design patterns are defined as "interfaces and user journeys implemented on social media platforms that attempt to influence users into making unintended, unwilling and potentially harmful decisions, often toward a decision that is against the users' best interests and in favour of the social media platforms interests, regarding the processing of their personal data". The Guideline numbered 03/2022 gives examples of deceptive design patterns but also best practice recommendations, and includes also a checklist of deceptive design pattern categories.

Guidelines on certification as a tool for transfers (07/2022)

The Article 46 of the GDPR stipulates that *a controller or processor may transfer personal data to a third country or an international organization only if the controller or processor has provided appropriate safeguards* and that an approved certification mechanism will be deemed as an appropriate safeguard with this regard. The Guideline numbered 07/2022 clarifies certification as a data transfer mechanism.

You may find the Guidelines here.

The French Supervisory Authority's ("CNIL") Announcement on 2023's Investigation Priorities

On March 15, 2023, the CNIL made an announcement as regards to its four key priorities regarding its upcoming investigations for 2023 which are smart cameras by public actors, the use of the file on personal credit repayment incident, the management of health files and mobile apps.

You may find the CNIL's announcement here.

The California Privacy Rights Act: Expanding Consumer Privacy Protection and Business Obligations

The California Privacy Rights Act ("CPRA"), which was approved in November 2020, amending the California Consumer Privacy Act ("CCPA") and introducing additional privacy measures to ensure consumer protection, went into effect on January 1, 2023. The CPRA expands the scope of the CCPA provisions and imposes new obligations on businesses that process Californians' personal data.

You can access the provisions of the CPRA 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