

Personal Data Protection Bulletin

2023

Third Quarter

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

Recent Updates from Türkiye

Personal Data Protection Board Amended the Exception Criteria for The Obligation to Register With the Data Controllers Registry

With the decision of the Personal Data Protection Board (“Board”) dated 06.07.2023, the “annual financial balance sheet total” criterion considered in determining the companies within the scope of the Data Controllers Registry (“VERBIS”) registration obligation is updated. With the amendment, data controllers whose annual number of employees is less than 50 (fifty) and annual financial balance sheet total is less than 100 (one hundred) million Turkish Liras and whose main activity is not processing sensitive personal data are not obliged to register with VERBIS.

You may find the Board’s decision [here](#).

Key Actions:

- ✓ Data controller companies should periodically review the registration obligation and exception criteria and register with VERBIS within the legal period from the determination of the registration obligation.

Announcement on Letter of Commitment Application was Published

The application submitted by Google Reklamcılık ve Pazarlama Limited Şirketi regarding the transfer of personal data abroad was evaluated by the Board and the said data transfer was authorized on 17.08.2023.

It should be noted that this decision does not authorize a general data transfer from Türkiye to Google servers. The Board’s decision covers only the data transfers made by Google Reklamcılık ve Pazarlama Limited to the data recipient residing abroad specified in the relevant undertaking.

You may find the announcement [here](#).

Commercial Electronic Message Complaint System Was Renewed

The interface of the Commercial Electronic Message Complaint System, which allows consumers to complain about commercial electronic messages sent without their permission, has been renewed. It is now possible for consumers to complain about companies that send unauthorized commercial electronic messages via e-Government Gateway and <https://tiss.ticaret.gov.tr> and to execute permissions by directly connecting to the Message Management System. In addition, innovations such as the collective transfer of applications to the relevant units when necessary were also made available.

You may find the announcement [here](#).

Presidential Decree on The Approval of The Medium-Term Program (2024-2026) Was Published

The Presidential Decree dated 06.09.2023 and numbered 7597 on the Approval of the Medium-Term Program (2024-2026) was published in the Official Gazette dated 06.09.2023 and bis numbered 32301. The Medium-Term Program for the 2024 - 2026 period includes among the targets set by the Medium-Term Program, the completion of the works for the harmonization process of PDPL with the European Union ("EU") acquis, particularly the European Union General Data Protection Regulation ("GDPR"), by the last quarter. In order to increase data-based competitiveness, it was stated that a National Data Strategy will be prepared and put into practice by the third quarter of 2024.

You may find the presidential decree [here](#).

The Board's Decision Summaries

The Board published 2 (two) new decision summaries on 14.08.2023. We have compiled the decision summaries for you:

- **Summary of the Decision on the Condition of Explicit Consent for Health Services Provided By A Private Health Institution**

In the case subject to the decision, to make an appointment on the website of a private hospital, it is mandatory to consent to the processing of personal data and to be contacted for this purpose to be informed about services and announcements. The Board considered that the requirement of explicit consent for the service by the data controller would cripple the will of the data subjects. In the decision, it is stated that while it is possible to rely on different processing conditions for the processing of personal data in the appointment application form, obtaining explicit consent would be deceptive and an abuse of rights.

In the decision, it is also evaluated that the expression *"I give my consent"* in the option *"I have read the clarification text regarding the processing of my data. I consent to the processing of my data under the Law on the Protection of Personal Data"* on the appointment registration page creates the impression of consent to the clarification text. The Board recommends that a box be checked to indicate that the disclosure text has been read.

You may find the summary of the Board decision [here](#).

Key Actions:

- ✓ Explicit consent for transactions not directly linked to a service should not be a condition for the prestation of that service.
- ✓ Misleading statements that may imply consent to the clarification text should be avoided.
- ✓ Where other data processing requirements are applicable, the explicit consent requirement should not be relied upon.

- **Board Decision on A Hospital's Obtaining Explicit Consent From Patients Regarding the Processing Of Personal Data Within the Scope of Advertising and Promotional Activities**

In the case where the data controller hospital requested explicit consent from the patients for taking photographs and videos, the Board examined the posts on the social media accounts of the hospital in question; it was determined that information was given about the health problems of the patients and that the treating physician made statements about the diagnosis and the result of the treatment applied to the patients.

In the decision, it is evaluated that the data controller violated the prohibition of advertising applied to private hospitals by processing health and other personal data for advertising purposes and that the advertising and promotional activities do not have a legitimate purpose since the explicit consent obtained from the data subjects will not eliminate the prohibition of advertising.

You may find the summary of the Board decision [here](#).

Key Actions:

- ✓ Data controllers should follow all legal regulations related to their field of activity. Explicit consent for transactions prohibited by law cannot be asserted as a condition for lawful data processing.

Recent Developments from the World



UK Announced Amendments to Data Protection Legislation

With its announcement dated 11.09.2023, the UK announced that it will amend its data protection legislation by updating the definition of fundamental rights and freedoms so that it will refer to rights under UK law instead of rights protected under EU law. Accordingly, the UK published the draft Data Protection (Fundamental Rights and Freedoms) Amendment Regulation 2023, which aims to amend the UK General Data Protection Regulation ("UK GDPR") and the Data Protection Act 2018 ("DPA 2018").

You may find the announcement [here](#).



Switzerland's New Federal Act of Data Protection Entered into Force On 1 September 2023

Adopted in 2020, the New Federal Act on Data Protection ("FADP"), which aims to harmonize Swiss data protection law with the GDPR, entered into force on 01.09.2023. The FADP, which is in most respects equivalent to the GDPR, partially deviates from the GDPR and regulates the provisions on the protection of personal data more strictly.

You can find detailed information on the Act [here](#).

Key Actions:

- ✓ Data controller companies should periodically review the registration obligation and exception criteria and register with VERBIS within the legal period from the determination of the registration obligation.



European Commission Publishes Adequacy Decision for EU-USA Data Privacy Framework

On 10.07.2023, the European Commission published its adequacy decision on the EU-USA Data Privacy Framework (“DPF”), declaring the United States of America (“USA”) a safe zone. Organizations that have certified their compliance with the DPF principles and have been added to the DPF list can now transfer data from the EU without the need for any additional measures, such as standard contractual clauses and binding corporate rules.

The adequacy decision is available [here](#).



UK-USA Data Bridge and Swiss-USA Data Privacy Framework Come into Force

On 21.09.2023, the UK Government announced its decision to establish the UK-USA Data Bridge (“Data Bridge”), also known as the UK Extension of the DPF. Effective 12.10.2023, transfers from the UK to US companies on the DPF list that have exercised the option to receive personal data under the Data Bridge will be possible.

At the same time, the Swiss-USA Data Privacy Framework (“Swiss-DPF”) entered into force on 17.07.2023 for data transfers from Switzerland to the USA. However, it is not possible to transfer data based on the Swiss-DPF until the Swiss-DPF compliance decision has entered into force.

You can find detailed information on the Data Bridge [here](#) and detailed information on the Swiss-DPF [here](#).



The European Data Protection Board Has Issued A Statement on the European Commission’s Review of the Japan Adequacy Arrangement

The European Data Protection Board (“EDPB”) issued a statement on 18.07.2023 regarding the European Commission’s 2019 adequacy decision that Japanese law provides equivalent protection to the EU for personal data to be transferred from the EU to Japan and that Japanese law is in line with the requirements of the GDPR. The EDPB’s statement is an important reminder that adequacy decisions for data transfers to third countries are regularly reviewed and changes in the laws of the countries concerned are closely monitored.

You may find the decision [here](#).



The Norway’s Data Protection Authority Has Published Guidance on Website Analytics and Tracking Tools

According to the Guidelines, website owners should not fully rely on the cookie management panel and should be aware that different rules and regulations apply to cookies and personal data. In this context, website owners should prevent third parties from obtaining personal data, take into account additional obligations regarding sensitive personal data, and not transfer data to unreliable third countries. In addition, the website should have disclosure texts on the processing of personal data that can be easily understood by visitors, and data subject rights should be respected.

You may find the detailed information on guidance [here](#).



UK Data Protection Authority Published Guide to Mass Communication by E-Mail

On 30.08.2023, the UK Data Protection Authority (“ICO”) published guidance on what to consider when sending e-mails to multiple recipients at the same time. Accordingly, when sending an e-mail containing sensitive personal information, it is recommended to use alternatives such as bulk e-mail services, mail merge, or secure data transfer services instead of the BCC feature.

You may find the guidance [here](#).



ICO Publishes Draft Guidance On Biometric Data and Biometric Technologies for Public Consultation

The ICO has published a draft guide on biometric data and biometric technologies for public consultation. The draft, published on the official website, discusses biometric recognition systems within the framework of personal data and explains the requirements under personal data protection law.

You may find the relevant guide [here](#).



Danish Data Protection Authority Publishes Guidance on Preventing Unauthorized Access to Personal Data by Employees

The Guidelines recommend that companies conduct a risk assessment of employee access to personal data and take appropriate control measures accordingly. Such measures may include authorizing employees to access data only when necessary, recording employees' use of personal data, and continuously monitoring the use of systems containing personal data.

You may find detailed information on the relevant guide [here](#).



The Irish Data Protection Authority Announced That It Has Fined Tiktok €345 Million

On 01.09.2023, the Irish Data Protection Authority issued its final decision regarding the investigation into the Chinese video-sharing site TikTok, which examined whether the GDPR obligations were complied with in the processing of personal data of child users. As a result of the investigation, it was determined that the account settings of child users are set to public by default and therefore the content of children can be viewed by anyone, due to the "Family Match" feature, adults who are not verified as the child's parents can access children's information, TikTok fails to provide information to children with sufficient transparency, dark commercial designs are used to manipulate user choices, and age verification measures are not taken adequately as part of the sign-up process.

The data protection authority imposed an administrative fine totaling EUR 345 Million against TikTok together with a reprimand. In addition, it was given time to comply with the GDPR within 3 (three) months from the date of notification.

You may find more detailed information about the judgement [here](#).

Key Actions:

- ✓ Convenient age verification systems shall be used when processing personal data relating to children.
- ✓ Children's data should be protected privately and account settings should not be made public by default.
- ✓ The custody relationship should be verified before opening the accounts of child users to parental access.



Draft Data Law Approved by the Committee of the Council of the EU

On 14.07.2023, the Committee of the Council of the EU announced that they had approved the draft Data Act. In the following process, the European Parliament is expected to take a final decision and adopt the draft in order to reach a provisional agreement. The Data Act broadly covers both personal and non-personal data and data generated together ("Internet of Things") and aims to maximize the value of data in the economy by making it available for innovative use. The Data Act is expected to contribute to the development of new services, especially in the field of artificial intelligence, where data sharing is important for algorithm training. Regulating business-to-business (B2B), business-to-consumer (B2C), and business-to-government (B2G) data sharing, the Data Act will be applicable to manufacturers of smart, connected products, and providers of related services, businesses, data recipients, and public sector bodies, as well as data processing service providers within the EU. It should also be noted that the Data Act has a cross-border scope of application. It will therefore apply to manufacturers who place their products on the market in the EU, as well as to data subjects who make their data available in the EU.

The text of the Data Act is available [here](#) and our Newsletter article on the Information Notice on the Impact Assessment of the Data Act is available [here](#).



Legislators Act to Protect Children Online

As children are becoming increasingly active online, action has been taken worldwide to protect children's rights, including their personal data. In this context, the US Senate approved the amendments to the US Online Privacy Protection Act (COPPA) and the Kids Online Safety Act (KOSA). These amendments aim to prevent the misuse of children's personal data and recognize that it is unlawful to process minors' data without their consent (verified parental consent).

At the same time, in the UK, on 19.09.2023, the Internet Safety Act, which includes provisions specifically on the protection of children online, was adopted by lawmakers to protect children in the online space. The Internet Safety Act is expected to enter into force shortly. In addition, the ICO announced the publication of a 10 (ten) step guide for information sharing to protect children and young people from physical, emotional or mental harm.

You can find the announcement on COPPA and KOSA [here](#), the announcement on the Internet Safety Act [here](#) and the ICO announcement [here](#).

Key Actions:

- ✓ The Data Act is a legal act that is directly applicable in the Member States without the need for additional regulation by national legislators and also has a cross-border application. Therefore, it is important for the parties covered by the Data Act to identify their obligations and start preparations without delay in order to harmonize with the legal regulations.



Digital Services Act Enters into Force for Major Online Platforms

The Digital Services Act ("DSA"), which provides a new and comprehensive set of rules for organizations offering Online Brokerage Services on how they should design their services and procedures, entered into force on 16.11.2022. On 25.04.2023, the European Commission adopted the first appointment decisions under the DSA, designating 17 (seventeen) major online platforms and two major online search engines with at least 45 (forty-five) million monthly active users. These include Facebook, Google, Amazon, and other well-known social

media platforms and marketplaces. The harmonization period of the designated operators expired on 25.08.2023, meaning that they must now comply with all new obligations under the law. Smaller platforms, which will be supervised by the local authorities of the Member States under the DSA, must comply with all obligations by 17.02.2024.

You can find the European Commission's announcement [here](#) and detailed information [here](#).



The Council of Europe Published the Model Contractual Clauses for the Transfer of Personal Data

On 27.06.2023, the Council of Europe announced the adoption of the first module of Model Contractual Clauses for cross-border data transfer based on the Convention for the Protection of Individuals about Automatic Processing of Personal Data ("Convention 108+"). The Model Convention Clauses aim to regulate data sharing between data controllers and are recommended for adoption by competent authorities.

The Model Convention Clauses are available [here](#).



Data Governance Act Becomes Binding as of 25.09.2023

The Data Governance Act ("DGA"), which entered into force on 23.06.2022, became binding for companies on 24.09.2023. The DGA aims to promote data sharing across the EU, facilitate the reuse of public sector data and assist undertakings in the development of new data-rich products and services, including data based on artificial intelligence. It is stated that the DGA will be a legal framework to establish a mechanism to ensure the secure re-use of certain categories of public sector data, such as trade secrets, personal data and data protected by intellectual property rights.

You can find detailed information [here](#).



“X” Announced That It Will Collect Users’ Biometric Data and Employment Data

X, formerly Twitter, announced that it has updated its privacy policy and increased the category of personal data it will collect from its users. According to the updated privacy policy, X may process users’ biometric data for security, safety, and identification purposes if users give explicit consent. In addition, personal data such as employment history and preference, education history, skills and abilities have been added to the data categories to be processed with the update in order to support users in the job and/or employee search process.

You can find detailed information about the updated privacy policy [here](#).



The Court of Justice of the European Union Ruled that Personal Data Protection Rules Can Be Applied to Competition Law

On 04.07.2023, the Court of Justice of the European Union (“CJEU”) ruled that national EU competition authorities may take into account a company’s compliance with relevant regulations, including EU data protection rules when assessing whether it has abused its dominant position. The CJEU stated that competition authorities may exercise their powers only for the purpose of detecting infringements of competition law and not by taking over the tasks of data protection authorities, and that the authorities must cooperate with other authorities in the exercise of their tasks.

You can access the relevant judgement [here](#) and our client announcement regarding the judgement [here](#).



European Commission Proposed a Regulation Laying down Additional Rules of Procedure to Improve the Implementation of the GDPR

On 04.07.2023, the European Commission proposed a new regulation setting out additional procedural rules for the implementation of the GDPR. This Regulation aims to facilitate cooperation between data protection authorities and to clarify and harmonize procedural rules for cross-border cases. If adopted, it will sit alongside the GDPR and complement the existing cooperation and consistency mechanisms set out in Chapter VII.

You can find relevant Regulation [here](#).



European Data Protection Supervisor Opinions on the European Commission's Proposals on Access to Financial Data and Payment Services

In its first opinion on the European Commission's proposal for the Financial Data Access Framework, the European Data Protection Supervisor ("EDPS") welcomed such a regulation and recommended that the definition of "customer data" be narrowed. In its second opinion, the EDPS analyzed the European Commission's proposed Regulation on Payment Services in the Internal Market and the proposed Directive on Payment Services and Electronic Money Services in the Internal Market. The EDPS generally endorsed the regulations and recommended defining the limits of what personal data is necessary to prevent fraud.

You can find the opinion on the proposal for the Access to Financial Data Framework [here](#) and the opinion on the proposed regulations on Payment Services and Electronic Money Services [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

AMSTERDAM

Office 4.31, Strawinskylaan 457,
1077 XX Amsterdam

+31 (0)20 747 1113

amsterdam@erdem-erdem.nl

www.erdem-erdem.av.tr